THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP REPORT

SEPTEMBER 1998

NETWORK GROUP REPORT
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the last meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) in December 1997, the Network Group (NG) has directed its efforts to five activities. Two of these activities involve the NG's ongoing responsibilities: facilitating the exchange of network security research and development (R&D) information between Government and industry and overseeing the NSTAC Network Security Information Exchange (NSIE). Discussions at NSTAC XX resulted in two additional activities: examining how national security and emergency preparedness (NS/EP) operations might be affected by a severe disruption of Internet service and clarifying the findings in the Widespread Outage Subgroup's (WOS) report to NSTAC XX. The NG initiated a fifth activity□ a review of the status of efforts to prepare the telecommunications infrastructure for the millennium change□in response to a request from the Manager, National Communications System.

ACTIVITIES

- **R&D Exchange**: The NG's network security R&D exchange will take place in October 1998 in collaboration with Purdue University's Computer Operations, Audit, and Security Technology Laboratory (COAST), the Institute of Electrical and Electronics Engineers (IEEE), and the Office of Science and Technology Policy (OSTP). The R&D exchange will address the growing convergence of telecommunications and the Internet, and methods for improving the collaboration among Government, industry, and academia on R&D efforts.
- **NSIE**: In June 1998, the Government and NSTAC NSIEs sponsored a workshop on the insider threat to information systems. The workshop offered an overview of the emerging insider threat and suggested measures organizations could take to reduce their vulnerability to it. The NSIEs developed two white papers to provide background material for the workshop and are developing an after-action report reflecting the insights that emerged from the workshop discussion so this material can be shared with a broader audience.
- **Internet Issue**: Following discussion at NSTAC XX, the Industry Executive Subcommittee (IES) tasked the NG to examine how NS/EP operations might be affected by Internet failures over the next 3 years. The NG has approved an outline for its Internet report and is currently gathering data on the Internet's architecture, its vulnerabilities, and how the Internet will be used to support NS/EP operations. The report will be provided to NSTAC at its next meeting.
- **Widespread Outage Subgroup**: The WOS report was also a topic of discussion at NSTAC XX. The WOS was asked to reexamine the conditions that may contribute to a widespread telecommunications outage and subsequently developed conclusions to provide to NSTAC XXI.
- **Year 2000 Problem**: The NG examined the status of efforts to address the Year 2000 (Y2K) problem and prepare the telecommunications infrastructure for the millennium change, factors that may affect those efforts, and problems that may result if those efforts are not fully effective. The NG will continue to monitor the Y2K

readiness of the telecommunications infrastructure as test results become available, and provide its insight on this matter, through NSTAC, to the President.

The NG offers the recommendations below to enhance the Y2K readiness of the telecommunications infrastructure.

Recommendations to the President

- The President should direct appropriate departments and agencies to develop contingency plans to:
  - respond to Y2K-induced service impairments of the Government's NS/EP customer premises equipment, functions, and applications; and
  - fulfill mission-critical NS/EP responsibilities in the event of Y2K-induced public network (PN) service impairments.
- The President should direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

Recommendation to the IES

The IES should continue to provide coordination, as required, for National Coordinating Center for Telecommunications (NCC) processes and procedures as they are developed for response to potential Y2K outages.

1.0 INTRODUCTION/BACKGROUND

The Network Group (NG) serves as the focal point for the network security activities of the President's National Security Telecommunications Advisory Committee (NSTAC). The Industry Executive Subcommittee (IES) established the NG as a permanent body to guide NSTAC's ongoing network security activities, i.e., participating in the exchange of research and development (R&D) information between Government and industry and overseeing the NSTAC Network Security Information Exchange (NSIE). The NG also addresses new network security issues as they arise.

2.0 CHARGE

Since NSTAC XX in December 1997, the NG has continued its efforts to guide ongoing network security activities, responded to two additional tasks resulting from the NSTAC XX meeting, and initiated a task at the request of the Manager, National Communications System (NCS).

The two ongoing activities are as follows:

- **R&D Exchange**. Plan and conduct an R&D exchange and determine the feasibility of a long-term R&D consortium and
- **Information Exchange**. Promote the exchange of information between Government, industry, and academia regarding vulnerabilities and threats and network security.

The two tasks originating from the NSTAC XX meeting are:

- **Internet Issue**. Examine how NS/EP operations might be affected by a severe disruption of Internet service caused by the failure of network routing and control mechanisms and
- **Widespread Telecommunications Outage**. Respond to questions regarding the Widespread Outage Subgroup's (WOS) Report to NSTAC XX.

In response to a request from the Manager, NCS, the NG also addressed the following task:

- **Year 2000 (Y2K) Problem**. Examine Y2K issues associated with NS/EP telecommunications.

3.0 ACTIVITIES

3.1 R&D Exchange

In late 1996, the Deputy Manager, NCS, asked the NSTAC to assist the Defense Advanced Research Project Agency in its work to address intrusion detection R&D. The NSTAC's Intrusion Detection Subgroup (IDSG) subsequently provided a report to NSTAC XX in December 1997 detailing its findings and recommendations for the President to consider in promoting the R&D of intrusion detection technologies. As a follow-on to the IDSG's work, the NG decided to sponsor an R&D exchange in the fall of 1998 addressing two issues: the growing

convergence of telecommunications and the Internet, and how Government, industry, and academia can better collaborate on network security R&D.

3.1.1 Status

The Network Group plans to conduct the R&D Exchange in October 1998 in collaboration with activities sponsored by Purdue University's Computer Operations, Audit, and Security Technology (COAST) Laboratory[1] and the Institute of Electrical and Electronics Engineers (IEEE), and the Office of Science and Technology Policy (OSTP). The sponsors welcomed the opportunity to collaborate with NSTAC on this effort since their activities cover the same research topics the NG plans to address, and target the same audience.[2] The NG is currently working with Purdue, the IEEE, and the OSTP to finalize arrangements for the R&D exchange.

3.1.2 Next Steps

Following the R&D exchange in October, the NG will report its findings regarding collaboration among Government, industry, and academia on network security R&D.

3.2 Network Security Information Exchange (NSIE)

3.2.1 Status

The Government and NSTAC NSIEs have continued to exchange information and views on threats and vulnerabilities affecting information and software elements of the public networks (PN), remedies, and consequent risks. The NSIEs have a history of sharing "lessons learned" within the information exchange process with a broader audience. This year, NSIE representatives addressed the insider threat to information systems and sponsored a workshop on this topic. The workshop offered an overview of the emerging insider threat and suggested measures that organizations could take to reduce their vulnerability to it. The workshop was designed to address the needs of mid-level managers responsible for negotiating business agreements with vendors, contractors, customers, and business partners; developing and implementing computer security policies, procedures, and practices; or developing and implementing Human Resources policies, procedures, and practices.

The workshop was held in June 1998 and was attended by 101 individuals representing 52 organizations. In addition to NSTAC member companies and NCS member departments and agencies, the audience included representatives from other critical infrastructures (e.g., the financial services and electrical power industries), as well as contractors, vendors, and professional recruiters who serve the telecommunications industry. As part of this initiative, the NSIEs developed two white papers on the insider threat:

[1] The COAST Laboratory is a multiple-project, multiple-investigator laboratory in computer security research. It functions with close ties to researchers and engineers in major companies and government agencies. Its research focuses on real-world needs and limitations, with a special focus on security for legacy computing systems.
[2] In October 1998, COAST is sponsoring a Workshop on Security in Large-Scale Distributed Systems, which will be held in conjunction with the IEEE Symposium on Reliable Distributed Systems.

- *The Insider Threat: Legal and Practical Human Resources Issues: An NSIE White Paper*, April 1998.
- *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment*, June 1998.

3.2.2 Next Steps

The NSIEs are developing an after-action report to capture workshop-generated information and insights on the insider threat to share their findings with a broader audience.

3.3 Internet Issue

Much like the private sector, the Government is using the Internet more extensively for day-to-day functions such as e-mail and procurement. As the Government extends its Internet use to more critical applications, such as supporting national security and emergency preparedness (NS/EP) functions, there are concerns about how a severe disruption of Internet service might affect NS/EP operations. This issue arose during discussion at the NSTAC XX meeting in December 1997, and the IES subsequently tasked the NG to examine how NS/EP operations might be affected by Internet failures over the next 3 years.

For the purposes of the report, a severe disruption is described as a sustained interruption or severe degradation of Internet service that could have potential strategic and/or service integrity significance to Government, industry, and the general public. Such an event would likely affect Internet service in at least one region of the country including at least one major metropolitan area. It would involve multiple Internet service providers and significantly degrade the ability of other essential infrastructures to function and would have an impact on the availability and integrity of Internet service for at least a significant portion of a business day.

3.3.1 Status

The NG has taken the following approach to the tasking:

- examine the extent to which NS/EP operations will depend on the Internet over the next 3 years,
- identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the PN, and
- examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

The NG has approved an outline for the Internet report and is currently gathering data for use in developing the initial sections. The NG has begun to gather information on the Internet's architecture, its vulnerabilities, and how the Internet will be used to support NS/EP operations. Sources for this information include both industry and Government subject matter experts, augmented by a research of open-source literature.

3.3.2 Next Steps

Over the next several months the NG will continue to gather and analyze information on these topics and develop the report. The report will be provided to NSTAC at its next meeting, in the summer of 1999.

3.4 Widespread Outage Subgroup

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, requested that Mr. Charles Lee, Chairman of the NSTAC, provide NSTAC's forward-looking views on the possibility of a widespread service outage in the public telecommunications network. The WOS was established in July 1997 to address Dr. Gibbons' letter. The WOS subsequently presented its findings to the NSTAC principals at NSTAC XX in December 1997.[3] At that time, the WOS was asked to reexamine the conditions that may contribute to a widespread telecommunications outage.

3.4.1 Conclusions

The WOS offers the following conclusions regarding the NSTAC XX WOS report clarification task:

- The dynamic nature and complexity of the public telecommunications network precludes a mathematical determination of the probability of a widespread outage. Despite the rapid changes occurring in the industry, a widespread outage remains unlikely.
- The greatest opportunity for ensuring the continued reliability of the PN will ensue as both established entities and newer entrants adhere to and help develop industry standards and best practices.
- The Alliance for Telecommunications Industry Solutions (ATIS) is positioned to address issues of technology-related vulnerabilities (e.g., software integrity, SONET operations control, and Signaling System 7 (SS7) gateway screening).
- The focal point for Government industry coordination has been and should remain at the National Coordinating Center for Telecommunications (NCC). The NCC has initiated an effort to expand the National Telecommunications Coordinating Network (NTCN) to improve communications capabilities with critical entities during network outage conditions.
- IES subgroups are currently seeking input from the NCS and the Federal Communications Commission Defense Commissioner's staff in outlining procedures for resolving regulatory issues during emergency telecommunications disruptions.

[3] *Report on the Likelihood of a Widespread Telecommunications Outage*, The President's National Security Telecommunications Advisory Committee, December 1997.

3.5 Year 2000 Problem

The NG report on the Year 2000 (Y2K) problem focuses on the current status of efforts to prepare the telecommunications infrastructure for Y2K, factors that may affect those efforts, and problems that may result if Y2K efforts are not fully effective. Because the telecommunications infrastructure is essential to maintaining the national security posture and responding to man-made and natural disasters, this report gives particular attention to NS/EP communications. The report recommends actions to the President to enhance the Y2K readiness of NS/EP telecommunications and mitigate the impact of Y2K-induced service disruptions on the Nation's NS/EP posture. In addition, the report recommends action the IES might take to help the Government respond to Y2K-induced service disruptions.

3.5.1 Analysis

The NG conducted a broad-based review of the telecommunications industry by soliciting briefings on Y2K status and initiatives from interexchange carriers, local exchange carriers, switching system vendors, large-scale system integrators, and Y2K risk assessment and remediation solution providers. This allowed the NG to assess the current state of the major telecommunications service providers and equipment vendors regarding their Y2K readiness. In addition, the Telco Year 2000 Forum, the ATIS, and the General Services Administration briefed the NG on their Y2K remediation initiative.

3.5.2 Conclusions

- The Y2K problem is receiving a high level of visibility within the management chains of the Government and the telecommunications industry (e.g., service providers and vendors).
- The millennium change is not a January 1, 2000, problem; it is a long-term problem that will begin before, and extend well beyond, January 1, 2000.
- The work required to address the Y2K problem (e.g., auditing and upgrading systems) will have some positive results for both providers and vendors in such areas as documenting systems and networks and updating hardware and software inventories.
- Extensive interoperability testing between service providers, both interexchange and local exchange carriers, is critical to preparing the telecommunications infrastructure for the millennium change.
- No organization, either private or Government, that briefed the NSTAC's NG offered a *guarantee* on total eradication of Y2K problems from their networks, services, or systems. Additionally, these organizations could not offer a guarantee of the adequacy of Y2K internetwork interoperability testing.
- Y2K contingency planning is crucial to minimizing the impact of the millennium change.
- Efforts to respond to multiple demands for status reports on Y2K initiatives are impeding companies' efforts to address the Y2K problem itself.

- Industry and Government will both have a better assessment of Y2K readiness in early 1999.

3.5.3 Recommendations

The NG proposed three recommendations for NSTAC's approval.

3.5.3.1 Recommendations to the President

- The President should direct appropriate departments and agencies to develop contingency plans to:
  - respond to Y2K-induced service impairments of the Government's NS/EP customer premises equipment, functions, and applications; and
  - fulfill mission-critical NS/EP responsibilities in the event of Y2K-induced PN service impairments.
- The President should direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

3.5.3.2 Recommendation to the IES

The IES should continue to provide coordination, as required, on NCC processes and procedures as they are developed for response to potential Y2K outages.

3.5.4 Next Steps

The NG will continue to monitor the Y2K readiness of the telecommunications infrastructure as test results become available and provide its insight on the matter, through the NSTAC, to the President.

4.0 SUMMARY OF RECOMMENDATIONS

4.1 Recommendations to the President

- The President should direct appropriate departments and agencies to develop contingency plans to:
  - respond to Y2K-induced service impairments of the Government's NS/EP customer premises equipment, functions, and applications; and
  - fulfill mission-critical NS/EP responsibilities in the event of Y2K-induced PN service impairments.

- The President should direct his Y2K single focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

4.2 Recommendation to the IES

The IES should continue to provide coordination, as required, on NCC processes and procedures as they are developed for response to potential Y2K outages.

ANNEX A

NETWORK GROUP MEMBERS

NETWORK GROUP MEMBERS

Nortel	Dr. Jack Edwards, Chair
GTE	Mr. Jim Bean, Vice-Chair
SAIC	Mr. Hank Kluepfel, Vice-Chair
AT&T	Mr. Dave Bush
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
ITT	Mr. Peter Steensma
MCI	Mr. Don Frick
NTA	Mr. Bob Burns
Raytheon	Mr. John Grimes
Sprint	Dr. Sushil Munshi
TRW	Ms. Ann Marmor-Squires
Unisys	Mr. Fred Tompkins
USTA	Dr. Vern Junkmann

OTHER CONTRIBUTORS

ITT	Mr. Dave Kelly
Lockheed Martin	Dr. Chris Feudo
MCI	Mr. Mike McPadden
U S WEST	Mr. Jon Lofstedt

ANNEX B

WHITE PAPER ON THE CLARIFICATION TASKING ON THE WIDESPREAD OUTAGE SUBGROUP REPORT (DECEMBER 1997)

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP

White Paper on the Clarification Tasking on the Widespread Outage Subgroup Report (December 1997)

SEPTEMBER 1998

WHITE PAPER ON THE CLARIFICATION TASKING ON THE WIDESPREAD OUTAGE SUBGROUP REPORT (DECEMBER 1997)
TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Background

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, requested that Mr. Charles Lee, Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), provide NSTAC's forward-looking views on the possibility of a widespread service outage in the public telecommunications network. The Widespread Outage Subgroup (WOS) was established in July 1997 to address Dr. Gibbons' letter. The WOS subsequently presented its findings to the NSTAC principals at NSTAC XX in December 1997.[1] At that time, the WOS was asked to further clarify several findings presented in its report. This white paper is the response to that request.

1.2 Scope

This white paper clarifies the findings presented in the NSTAC XX WOS Report. Specifically, this white paper will respond to questions regarding:

- how low is "low" for the likelihood of a widespread telecommunications outage occurring,
- the ability of technology-related vulnerabilities to cause or influence a widespread telecommunications outage, and
- plans/mechanisms for intercarrier and industry□Government response to a widespread telecommunications outage.

1.3 Widespread Outage Definition

A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day.

2.0 LIKELIHOOD OF A WIDESPREAD TELECOMMUNICATIONS OUTAGE

The dynamic nature and complexity of the public telecommunications network precludes a mathematical determination of the probability of a widespread outage. However, an outage involving multiple carriers, affecting a wide region of the country and, in particular, significantly degrading other critical infrastructures, remains unlikely. Recent network events have provided additional lessons, including: increased awareness, business continuity planning, and improved ability to respond to public network (PN) outages. In its 1997 Annual Report, *Prepared for the*

[1] *Report on the Likelihood of a Widespread Telecommunications Outage*, The President's National Security Telecommunications Advisory Committee, December 1997.

Change, the Network Reliability Steering Committee (NRSC) reported its findings on network performance, derived from its analysis of major outage reports filed with the Federal Communications Commission (FCC).[2] The NRSC's analysis revealed that overall network performance remained stable, while the frequency of outages and the impact on customers was the lowest it had been in the last 5 years. This performance is especially noteworthy since the Nation's networks have been undergoing rapid technological changes while experiencing significant growth over the last 5 years—a 27 percent increase in the number of lines and a 20 percent increase in the number of calls.

The industry continually develops and refines standards and best practices to maintain the reliability and interoperability of the PN. The greatest opportunity for ensuring the continued reliability of the PN will ensue as both established entities and newer entrants adhere to and help evolve these standards and best practices.

3.0 TECHNOLOGY-RELATED VULNERABILITIES

The WOS report identified the following technology-related vulnerabilities:

- **Software Integrity.** PN software, like all software, is vulnerable to design flaws, implementation errors, and other problems that could cause it to fail or not function as desired, despite its designers' best efforts. Finding and mitigating software mistakes is often a difficult and imperfect process. Security analysis of software, in general, is not practiced at a sufficient level to maintain software integrity throughout the PN.[3]
- **SONET Operations Control.** Synchronous Optical Network (SONET) serves as the transport medium of choice for trunks, data communications lines, asynchronous transfer mode, and common channel signaling (CCS) links. SONET's address resolution functions support almost no security measures that could prevent an intruder from subverting it.
- **CCS (SS7) Gateway Screening.** Public networks depend on CCS, a packet-switched data network employing Signaling System 7 (SS7) protocols, to set up and terminate calls as well as transmit advanced feature data such as Caller ID. Gateway screening is one of a very limited set of SS7 security tools and is implemented at the interface between service providers' networks. Presently, there is no industry-wide understanding of how gateway screening should be extended into the new competitive network environment.
- **Physical Design.** The U.S. public networks have been designed to preclude single points of failure above the local switching level. This has been accomplished through substantial investment in both physical and logical diversity. Networks are utilizing

[2] FCC 94-189 Docket No. 91-273, Second Report and Order, Adopted July 14, 1994, specifies the outage reporting criteria: carriers should report outages lasting 30 minutes or more and potentially affecting 30,000 or more customers. Carriers must also report outages lasting 30 minutes or more and affecting special facilities (e.g., 911 tandems, major airports, major military installations, key government facilities, and nuclear power plants) regardless of the number of customers affected.

[3] It should be noted that the telecommunications infrastructure is not unique in this regard; this is also the case with respect to software employed in the other critical infrastructures.

dynamically controlled routing, with nonhierarchical network architectures capable of routing traffic around damaged or congested portions of the network in real time. Economic tradeoffs, enabled by technological advances, continue to cause some carriers to consolidate and collocate both facilities and network operation functions. Although somewhat decreasing the physical diversity of the PN, it has enabled the rapid introduction of advanced network management technologies into consolidated control centers. With this consolidation of operational functions, the technical complexity of these consolidated control centers becomes a vulnerability concern. If one of these consolidated control centers were to suffer a full or partial service disruption, the impact on the portion of the PN under the control of the affected center would be significant.

- **Introduction of New Technologies or Services.** New technologies, by their nature, are often more complex and sometimes create unintended consequences and unexpected interactions among subsystems. Because new technologies cannot be tested for and against every conceivable set of events or network conditions, unforeseen vulnerabilities may be introduced into the network.

Although vulnerabilities above could conceivably cause or influence a widespread telecommunications outage, none taken alone is a likely cause of a widespread or other large-scale service outage. The ATIS is positioned to address these technology-related vulnerabilities. NSTAC should continue to provide support when national security and emergency preparedness (NS/EP) issues arise.

4.0 PLANS/COORDINATING MECHANISMS FOR INTERCARRIER AND INDUSTRY□GOVERNMENT RESPONSE TO A WIDESPREAD TELECOMMUNICATIONS OUTAGE

As reported during NSTAC XX, there is no industry-wide plan for coordination within the telecommunications industry and with Government during a widespread outage affecting NS/EP telecommunications. However, progress has been made since the December 1997 NSTAC XX meeting. The focal point for industry□Government coordination has been and should remain at the National Coordinating Center for Telecommunications (NCC). To address outages when normal telecommunications may be inadequate, the NCC has initiated an effort to expand the National Telecommunications Coordinating Network (NTCN)[4] to enable intercarrier and industry□government communications. The proposed expanded NTCN will likely include key telecommunications service providers, equipment vendors, large-scale systems integrators, and Government organizations to better respond to network outages.

In addition, IES subgroups are currently seeking input from the National Communications System (NCS) and the FCC Defense Commissioner's staff in outlining procedures for resolving regulatory issues during emergency telecommunications disruptions.

[4] The conference bridging of the NTCN interconnects sites regardless of the communication means they use, e.g., a telephone call can be bridged to a site with only an operational high frequency (HF) radio capability.

5.0 CONCLUSIONS

The WOS offers the following conclusions regarding the NSTAC XX WOS report clarification tasking:

- The dynamic nature and complexity of the public telecommunications network precludes a mathematical determination of the probability of a widespread outage. Despite the rapid changes occurring in the industry, a widespread outage remains unlikely.
- The greatest opportunity for ensuring the continued reliability of the PN will ensue as both established entities and newer entrants adhere to and help develop industry standards and best practices.
- ATIS is positioned to address issues of technology-related vulnerabilities (e.g., software integrity, SONET operations control, and SS7 gateway screening).
- The focal point for industry Government coordination has been and should remain at the NCC. The NCC has initiated an effort to expand the NTCN to improve communications capabilities with critical entities during network outage conditions.
- IES subgroups are currently seeking input from the NCS and the FCC Defense Commissioner's staff in outlining procedures for resolving regulatory issues during emergency telecommunications disruptions.

APPENDIX A

WIDESPREAD OUTAGE SUBGROUP MEMBERS

WIDESPREAD OUTAGE SUBGROUP MEMBERS

NTA	Mr. Bob Burns, Chair
AT&T	Mr. Dave Bush
Bellcore	Ms. Louise Tucker
GTE	Mr. Ernie Gormsen
Lockheed-Martin	Dr. Chris Feudo
MCI	Mr. Don Frick
OMNCS	Mr. Bernie Farrell
SAIC	Mr. Hank Kluepfel
USTA	Dr. Vern Junkmann
U S WEST	Mr. Jon Lofstedt

ANNEX C

YEAR 2000 PROBLEM STATUS REPORT

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP

Year 2000 Problem Status Report

SEPTEMBER 1998

YEAR 2000 PROBLEM STATUS REPORT
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

In January 1998, the Manager, National Communications System (NCS), requested the President's National Security Telecommunications Advisory Committee (NSTAC) to provide an update to the President on actions under way throughout the telecommunications industry to ensure continuity of service through the millennium change. In response to this request, the NSTAC's Industry Executive Subcommittee (IES) directed its Network Group (NG) to address the Year 2000 (Y2K) issue. The NG's review of Y2K readiness addresses national security and emergency preparedness (NS/EP) and the national telecommunications infrastructure.

Scope

This report focuses on the current status of efforts to prepare the telecommunications infrastructure for Y2K, factors that may affect those efforts, and problems that may result if Y2K efforts are not fully effective. Because the telecommunications infrastructure is essential to maintaining the national security posture and responding to man-made and natural disasters, this report gives particular attention to NS/EP communications. The report recommends actions to the President to enhance the Y2K readiness of NS/EP telecommunications and mitigate the impact of Y2K-induced service disruptions on the Nation's NS/EP posture. In addition, the report recommends action the IES might take to help the Government respond to Y2K-induced service disruptions.

Conclusions

The NG reached the following conclusions:

- The Y2K problem is receiving a high level of visibility within the management chains of the Government and the telecommunications industry (e.g., service providers and vendors).
- The millennium change is not a January 1, 2000, problem; it is a long-term problem that will begin before, and extend well beyond, January 1, 2000.
- The work required to address the Y2K problem (e.g., auditing and upgrading systems) will have some positive results for both providers and vendors in areas such as documenting systems and networks and updating hardware and software inventories.
- Extensive interoperability testing between service providers, both interexchange and local exchange carriers, is critical to preparing the telecommunications infrastructure for the millennium change.
- No organization, either private or Government, that briefed the NSTAC's NG offered a guarantee of total Y2K problem eradication from their networks, services, or systems. Additionally, these organizations could not offer a guarantee of the adequacy of Y2K internetwork interoperability testing.

- Y2K contingency planning is crucial to minimizing the impact of the millennium change.
- Efforts to respond to multiple demands for status reports on Y2K initiatives are impeding companies' efforts to address the Y2K problem itself.
- Industry and Government will both have a better assessment of Y2K readiness in early 1999.

Recommendations

The NG offers the recommendations below to enhance the Y2K readiness of the telecommunications infrastructure.

Recommendations to the President

- The President should direct appropriate departments and agencies to develop contingency plans to:
  - respond to Y2K-induced service impairments of the Government's NS/EP customer premises equipment, functions, and applications; and
  - fulfill mission-critical NS/EP responsibilities in the event of Y2K-induced public network service impairments.
- The President should direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

Recommendation to the IES

The IES should continue to provide coordination, as required, for National Coordinating Center for Telecommunications (NCC) processes and procedures as they are developed for response to potential Y2K outages.

Next Steps

A majority of operational Y2K compliance testing will not be completed until late 1998 or early 1999. By NSTAC XXII, the Y2K readiness of the national telecommunications infrastructure should be clearer, as by that time both industry and Government should have completed most systems and interoperability tests. The NG will continue to monitor the Y2K readiness of the telecommunications infrastructure as test results become available and provide its insight on this matter, through NSTAC, to the President.

1.0 INTRODUCTION

1.1 Background

In January 1998, the Manager, National Communications System (NCS), requested the President's National Security Telecommunications Advisory Committee (NSTAC) to provide an update to the President on actions under way throughout the telecommunications industry to ensure continuity of service through the millennium change. In response to this request, the NSTAC's Industry Executive Subcommittee (IES) directed its Network Group (NG) to address the Year 2000 (Y2K) issue. The NG's review of Y2K readiness addresses national security and emergency preparedness (NS/EP) and the national telecommunications infrastructure.

1.2 Scope

This report focuses on the current status of efforts to prepare the telecommunications infrastructure for Y2K, factors that may affect those efforts, and problems that may result if Y2K efforts are not fully effective. Because the telecommunications infrastructure is essential to maintaining the national security posture and responding to man-made and natural disasters, this report gives particular attention to NS/EP communications. Finally, the report recommends actions to the President to enhance the Y2K readiness of NS/EP telecommunications and mitigate the impact of Y2K-induced service disruptions on the Nation's NS/EP posture. In addition, the report recommends action the IES might take to help the Government respond to Y2K-induced service disruptions.

2.0 SURVEY OF TELECOMMUNICATIONS INDUSTRY Y2K ACTIVITIES

The NG conducted a broad-based review of the telecommunications industry by soliciting briefings on Y2K status and initiatives from interexchange carriers, local exchange carriers, switching system vendors, large-scale system integrators, and Y2K risk assessment and remediation solution providers. Several NSTAC member companies described their companies' Y2K initiatives and provided their perspectives on the Y2K problem. In addition, the NG heard briefings from the Telco Year 2000 Forum and the Alliance for Telecommunications Industry Solutions (ATIS) on their respective, cross-industry Y2K initiatives. This allowed the NG to assess the current state of the major telecommunications service providers and equipment vendors regarding their Y2K readiness.

3.0 CURRENT STATUS OF Y2K READINESS WITHIN THE TELECOMMUNICATIONS INDUSTRY

Efforts to make the telecommunications infrastructure Y2K-ready are well under way. The major service providers and their vendors have been working on these issues for several years. The Telco Year 2000 Forum and others (e.g., the General Services Administration [GSA] and ATIS) are planning interoperability testing for critical products, networks, services, and systems. Those who briefed the NG on their Y2K initiatives expect the majority of critical products and networking to be Y2K-ready between late 1998 and early 1999.

The Telco Year 2000 Forum is a group of eight telecommunications service providers working together to deal with common Y2K issues.[1] Its major goals are to share information and "lessons learned"[2] and conduct Y2K interoperability testing. The objective of the forum's network interoperability testing is to minimize the risk of network and service failures and ensure that functionality of date/time sensitive operations is not adversely affected. The forum also serves to provide a common view to telecommunications hardware/software suppliers regarding Y2K solutions, and encourages hardware/software providers to adhere to product and service implementation schedules. The forum's test of Y2K compliant products/services, scheduled for third to fourth quarter of 1998, is designed to address the interoperability of components *within* discrete networks, rather than *between* networks. This intranetwork interoperability testing will include the major North American suite of equipment and will cover: emergency services; basic, enhanced and intelligent services; network management and operations, administration, maintenance, and provisioning (OAM&P) operations support systems; data networks; and customer premises equipment (CPE).

The interexchange carriers are not participating in the Telco Year 2000 Forum's intranetwork interoperability test but are conducting their own intranetwork tests of their products and services. They are also participating in ATIS's internetwork interoperability testing initiatives, described below.

ATIS[3] is planning to conduct internetwork interoperability Y2K readiness testing to verify that there are no adverse effects on interconnected networks.[4] The pretest and setup work to support the testing is currently under way, with an anticipated completion date in 4Q98. This testing will be conducted during January and February 1999. The items identified for testing include mass calling events on December 31, 1999; potential congestion; cross-network services; rollover to Y2K in the Local Number Portability (LNP) environment; impact of time zones; and key dates in an LNP environment (December 31, 1999, February 29, 2000, and December 31, 2000). Although ATIS plans to test the effects of mass calling events on the switching networks, it does not plan to test network management controls within network management operations support systems.

Service providers and vendors recognize that their companies' futures depend on how effectively they address their Y2K problems. Consequently, they are devoting substantial resources to achieving Y2K readiness. Their initiatives include taking comprehensive inventories of their systems, prioritizing them, assessing the extent to which they are date sensitive, and then implementing and testing solutions. The telecommunications industry has been able to sustain its high level of reliability, in part, because it has traditionally conducted extensive regression testing. This should minimize the likelihood that efforts to correct Y2K problems will adversely

[1] Members include Ameritech, Bell Atlantic, Bell-South, Cincinnati Bell, GTE, SBC Communications Inc. (SBC), Southern New England Telecommunications (SNET), and U.S. West.

[2] Although Telco Year 2000 Forum shares general information regarding the status of its activities, detailed information on testing is limited to the forum's members.

[3] The ATIS groups addressing Y2K testing are the Internetwork Interoperability Test Coordination Committee and the Network Testing Committee (NTC) of the Carrier Liaison Committee's Network Interconnection/Interoperability Forum. Testing participants include Ameritech, AT&T, and Sprint.

[4] It should be noted that ATIS's internetwork interoperability testing will be conducted between the test laboratories of the participating carriers, as it is not feasible to conduct these tests on the live network.

affect the reliability of the public network (PN). However, as with any software implementation, it is not possible to foresee, and test for, every possible adverse interaction. Because Y2K readiness preparation is a massive, diverse, pervasive, and complex software augmentation, even the most thorough, exhaustive efforts may fail to achieve 100 percent success.

Bellcore offered the following information to provide a sense of perspective on the magnitude of the Y2K problem for the telecommunications industry.[5]

- A telecommunications company is generally a "large enterprise." For example, there may be 1,400 to 1,600 switches, 30 to 50 signal transfer points (STP), 5 to 60 service control points, thousands of transport component systems, and many element management systems and operations systems, any one of which could have multiple date-sensitive functions.
- 75 percent of voice networking devices are date sensitive.
- 25 percent of data networking devices are date-sensitive (25 to 35 percent for intelligent devices).
- 100 percent of network management devices are Y2K affected.

No organization, either private or Government, that briefed the NSTAC's NG offered a *guarantee* of total Y2K problem eradication from its networks, services, or systems. Additionally, these organizations could not offer guarantees of the adequacy of Y2K internetwork interoperability testing.

4.0 GENERAL SERVICES ADMINISTRATION Y2K TELECOMMUNICATIONS COMPLIANCE PROGRAM REVIEW

The GSA has taken an active role in addressing the Y2K readiness of the Government's telecommunications services. Its Y2K Telecommunications Compliance Program was established to serve as a focal point for Y2K telecommunications compliance activities and information across the Federal Government, with the following goals:

- facilitate Government industry partnership to address Y2K telecommunications challenges,
- encourage Governmentwide sharing of Y2K telecommunications assessment and implementation approaches,
- create a Government repository and directory for product and service compliance information, and
- support the development and dissemination of methods and processes for agency testing of telecommunications systems.

[5] Information provided by Judy List, Vice President/General Manager, Bellcore, at a NSTAC Network Group meeting held on April 21, 1998.

The GSA Y2K Compliance Office developed the following evaluation and testing strategies:

- Work with vendors to understand Y2K vulnerabilities.
- Conduct hardware/software equipment testing at vendors' facilities.
- Partner with telecommunications service providers for testing of large switches.
- Conduct additional independent compliance testing (in the field on agency equipment and at independent agency and contractor laboratories).
- Disseminate evaluation and testing plans and results to Government organizations through the GSA Web site (http://y2k.fts.gsa.gov).

The NSTAC considers this a worthwhile effort and encourages its members to participate in GSA's efforts to collaborate with industry to address the Y2K challenges.

5.0 POTENTIAL TELECOMMUNICATIONS Y2K PROBLEMS

Failure to effectively achieve Y2K readiness has the potential to adversely affect components of the telecommunications infrastructure in several ways. Some cases are likely to be straightforward: the application may fail to recognize the date and report the error to the user, which would allow the error to be readily identified and corrected. In other cases, the application may fail to recognize the date, without reporting the error to the user, increasing the difficulty of diagnosing the problem. The third type of error may not affect the primary application but could cause failures in secondary applications or systems, making it even more difficult for users of those secondary applications to diagnose the source of the problem, particularly if multiple applications provide input into the secondary application.

Examples of how some of these problems may affect components of the telecommunications infrastructure at the platform/system level are listed below:

- **Platform operation (hardware).** Hardware clocks may not recognize the year 2000.
- **Operating system functionality.** Date functions may return the wrong year to applications.
- **Scheduling of events.** Errors in calendar dates can prevent scheduled events (e.g., reports, updates, testing, designing, provisioning, or billing) from running, and can result in incipient failures later.
- **Historical data.** Historical data may not be available from 1999, or 1999 may be re-ordered, with events occurring in 1999 sequenced after 2000.
- **Sorting and searching algorithms.** Dates *after* 1999 will be ordered *before* 1999; searching algorithms intended to *include* dates in 2000 (e.g., "Where date > 1997") will *exclude* them instead.
- **Password expiration.** All passwords may expire (which would prevent authorized users from performing legitimate functions), or they may never expire (which could diminish the protection offered by password aging).

- **Multiproduct time/date coordination.** Products that synchronize the date may roll to different dates.
- **OAM&P capabilities.** System tools may not recognize 00 or 2000 as a valid year.
- **Software integrity**. Even under the best circumstances, efforts to correct one software problem may inadvertently introduce another. In addition to the possibility of human error, work on the Y2K problem also provides an opportunity for those with bad intentions to introduce malicious code without being detected.

Y2K problems may also occur at the network level. For example, communications satellite links may suffer degradation from a variety of Y2K dependencies. Further, since our Nation's networks are interconnected with those of foreign telecommunications service providers, our telecommunications infrastructure may be adversely affected by their Y2K problems. Because the telecommunications infrastructure is so heavily dependent upon electrical power, Y2K-induced failures in the electrical power infrastructure could also affect telecommunications capabilities.

Any of the problems described above may combine to have a cascading affect on telecommunications service. For example, a mass calling event could cause different Y2K-induced problems to occur simultaneously in various network components (e.g., an operations platform, an operating system, and an operations support system). This could affect the ability of network management controls to properly respond to the system overloads caused by the mass calling event, disrupting or degrading service until all the problems can be diagnosed and corrected.

The Y2K problem can adversely affect the overall quality of telecommunications services in another, more subtle way: the time and money companies are spending on Y2K problem eradication can diminish the resources available to develop new products and enhancements to improve their networks' service and performance.

This list is by no means exhaustive; it merely suggests some of the issues facing the telecommunications industry. It is impossible to predict all the problems that may result if the Y2K problem is not completely eradicated. However, this problem can be mitigated with effective remediation efforts, operational testing, and contingency planning.

6.0 LEGAL CONCERNS REGARDING Y2K READINESS

The liability issues associated with Y2K readiness are another factor affecting the progress in addressing Y2K problems. Many law firms are exploring Y2K liability issues, in anticipation of the lawsuits they expect to result from Y2K problems. In fact, the lawsuits have already begun. Customers who assert that Y2K enhancements should be free are suing one software vendor who decided to charge for Y2K upgrades.[6] A grocery store is suing a cash register manufacturer because its machines cannot process transactions on credit cards that expire in 2000, and a computer company is suing an accounting software vendor.[7]

[6] *South Florida Business Journal*, Miami, FL, April 24, 1998.
[7] *The Washington Post*, page A-1, May 3, 1998.

The focus appears to be on fixing the blame and liability rather than accepting the fact that everyone owns the Y2K problem. In this adversarial environment, some organizations are reluctant to share information about their Y2K efforts because they cannot be certain how it might be used against them in court later. This situation impedes the cooperation among customers, providers, and vendors needed to effectively address the Y2K problem. Further, the focus on legal issues can reduce resources available to solve the Y2K problem. Companies may have to choose between augmenting their legal staff or their technical staff.

As the millennium approaches, customers as well as Government agencies are inundating companies with requests for status of their Y2K initiatives. For example, the Securities and Exchange Commission (SEC) requires companies to provide quarterly status reports on their Y2K problem eradication efforts. This is another drain on resources companies have allocated to solve their Y2K problems.

In addition, the Federal Communications Commission (FCC) is increasing its examination of the Y2K problem and recently sent a letter to the Chief Executive Officers of major local exchange carriers, interexchange carriers, and telecommunications equipment manufacturers to emphasize the FCC's interest in the Y2K problem. The letter also asked the carriers and equipment manufacturers for information on their Y2K initiatives and encouraged them to share their information with other companies by posting it on the FCC's Year 2000 home page (www.fcc.gov/year2000). In addition to serving as the point person for the FCC's Y2K efforts, the FCC Defense Commissioner represents the FCC on the President's Council on Year 2000 Conversion.

7.0 NS/EP IMPLICATIONS

Efforts to make the PN Y2K ready will go a long way toward making NS/EP telecommunications services Y2K ready, since the PN provides the basic transport and switching facilities for NS/EP telecommunications services. However, it is equally critical that the NS/EP-specific CPE and telecommunications services, such as the Government Emergency Telecommunications Service and the Telecommunications Service Priority System, are Y2K ready and tested. In addition, it is essential to develop contingency plans so the Government and industry will be ready to respond to Y2K-induced outages, should they occur.

While it is not possible to conduct complete end-to-end testing of the entire PN, it is important for the Government to test the interoperability of NS/EP services as an integral part of the underlying telecommunications infrastructure to ensure these features are Y2K compliant. The Office of the Manager, NCS (OMNCS), is currently defining the scope and methodology for testing NS/EP telecommunications services interoperability. This testing is to be completed before January 1, 1999. Once this testing has been conducted, the OMNCS will have a better understanding of its Y2K status and the next steps it should take.

In an effort to respond to the consequences of possible Y2K-caused service disruptions, the NCS is also expanding its coordination base for the Y2K time frame. This expansion includes connecting to critical Government and industry operations centers that would play a role in responding to possible Y2K disruptions. As part of this effort, the National Coordinating Center for Telecommunications (NCC) is enhancing its current National Telecommunications

Coordinating Network (NTCN) to meet this requirement. The NTCN expansion is expected to be completed and tested by second quarter of 1999.

8.0 CONCLUSIONS, RECOMMENDATIONS, AND NEXT STEPS

8.1 Conclusions

The NG offers the following conclusions regarding the Y2K readiness of the telecommunications infrastructure:

- The Y2K problem is receiving a high level of visibility within the management chains of Government and the telecommunications industry (e.g., service providers and vendors).
- The millennium change is not a January 1, 2000, problem; it is a long-term problem that will begin before, and extend well beyond, January 1, 2000.
- The work required to address the Y2K problem (e.g., auditing and upgrading systems) will have some positive results. After Y2K conversion, service providers and vendors should have documented systems and networks; updated equipment inventories (hardware/software); streamlined applications and systems; improved configuration management baselines; a better understanding of systems functionality and performance; more extensive implementation of approved industry standards.
- Extensive interoperability testing between service providers, both interexchange and local exchange carriers, is critical to preparing the telecommunications infrastructure for the millennium change.
- No organization, either private or government, that briefed the NSTAC's NG offered a *guarantee* of total eradication of Y2K problems from its networks, services, or systems. Additionally, these organizations could not offer a guarantee of the adequacy of Y2K internetwork interoperability testing.
- Y2K contingency planning is crucial to minimizing the impact of the millennium change. Both Government and industry must develop contingency plans so they are prepared to respond to the problems they were unable to anticipate or prevent. Service providers and vendors plan to test individual components of the telecommunications infrastructure and conduct interoperability tests between and among many network elements. However, it is not possible to design test cases for every potential problem, nor is it possible to conduct complete end-to-end testing on the live PN. By developing comprehensive contingency plans, the telecommunications industry and the Government will be able to respond effectively to Y2K perturbations in the PN and keep the PN and Government services mission-ready.
- Efforts to respond to multiple demands for status reports on Y2K initiatives are impeding companies' efforts to address the Y2K problem itself.
- Industry and Government will both have a better assessment of Y2K readiness in early 1999.

8.2 Recommendations

The NG has identified actions the President and the NSTAC's IES could take to enhance the Y2K readiness of NS/EP telecommunications and mitigate the impact of Y2K-induced service impairments on the Nation's NS/EP posture.

8.2.1 Recommendations to the President

8.2.1.1 Develop Contingency Plans to Respond to Y2K-induced Service Impairments

Given the extent and complexity of the Y2K software augmentation, there can be no guarantees that Y2K remediation measures will anticipate, and prevent, every problem. Y2K readiness initiatives should encompass not only efforts to *prevent* problems, but also plans to *respond* to problems that may have been overlooked. Therefore,

- The President should direct appropriate departments and agencies to develop contingency plans to:
  - respond to Y2K-induced service impairments of the Government's NS/EP CPE, functions, and applications; and
  - fulfill mission-critical NS/EP responsibilities in the event of Y2K-induced PN service impairments.

8.2.1.2 Coordinate the Government's Requests forY2K Readiness Information

The Government recognizes the importance of resolving the Y2K problem and consequently has great interest in the status of industry's Y2K readiness. Some Government departments and agencies have demonstrated this interest by requiring companies to report on the status of their Y2K initiatives. For example, the SEC requires companies to provide Y2K status reports on a quarterly basis. The GSA has requested similar reports. The FCC has also requested specific information from certain carriers and manufacturers. While the Government's interest and concern are understandable, efforts to respond to multiple requests diminish the resources available to address the Y2K problem itself. In order to meet the Government's requirement for information on the status of industry's Y2K initiatives without burdening industry with requests from many different departments and agencies□

- The President should direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

8.2.2 Recommendation to the IES

As part of the OMNCS's Y2K initiative, the NCC is reviewing its current operational response procedures and the existing NTCN to identify any actions required to enhance the NCC's response capabilities in the event of Y2K-induced telecommunications outages. To assist the NCC in this effort□

The IES should continue to provide coordination, as required, on NCC processes and procedures as they are developed for response to potential Y2K outages.

8.3 Next Steps

In addition to conducting operational testing for its NS/EP telecommunications support functions, the NCC is expanding its coordination base. This increased coordination base will allow the NCC to better respond to any Y2K-induced telecommunications disruptions that may occur. The NCC Vision-Operations Subgroup can assist the NCC in identifying the additional technical support needed during this time.

A majority of the telecommunications industry's Y2K compliance testing will not be completed until late 1998 or early 1999. The Telco Year 2000 Forum intends to conduct its interoperability testing during third and fourth quarters of 1998. The ATIS Internetwork Interoperability Test Coordination Committee plans to complete its internetwork interoperability test by March 1999. The NSTAC will stay abreast of these activities. By NSTAC XXII, the Y2K readiness of the national telecommunications infrastructure should be clearer, as by that time both industry and Government should have completed most critical systems and interoperability tests. The NSTAC will continue to monitor the Y2K readiness of the telecommunications infrastructure, as test results become available, and provide its insight on this matter to the President.