

**THE PRESIDENT'S  
NATIONAL SECURITY TELECOMMUNICATIONS  
ADVISORY COMMITTEE**



***OPERATIONS SUPPORT GROUP  
REPORT***

**JUNE 1999**

**OPERATIONS SUPPORT GROUP REPORT  
TABLE OF CONTENTS**

**EXECUTIVE SUMMARY ..... ES-1**

**1.0 INTRODUCTION ..... 1**

**2.0 CHARGE ..... 2**

**3.0 RESULTS ..... 2**

    3.1 PDD-39 and PDD-62 Implementation ..... 2

        3.1.1 Conclusion ..... 3

        3.1.2 NSTAC Direction to the IES ..... 3

    3.2 National Coordinating Center for Telecommunications ..... 3

        3.2.1 Conclusions ..... 6

        3.2.2 NSTAC Direction to the IES ..... 6

    3.3 Y2K Technology Problem ..... 6

        3.3.1 Conclusions ..... 10

        3.3.2 NSTAC Recommendation to the President ..... 11

        3.3.3 NSTAC Direction to the IES ..... 11

**OPERATIONS SUPPORT GROUP MEMBERS ..... ANNEX A**

**NCC VISION-OPERATIONS SUBGROUP MEMBERS ..... ANNEX B**

**YEAR 2000 SUBGROUP MEMBERS ..... ANNEX C**

**POTENTIAL CANDIDATES FOR NCC PARTICIPATION ..... ANNEX D**

**EXECUTIVE SUMMARY**

The President's National Security Telecommunications Advisory Committee's (NSTAC) Operations Support Group (OSG) evaluates the overall progress and direction of national security and emergency preparedness (NS/EP) telecommunications operational activities. Among its specific taskings, the OSG was charged to review the functions of the National Coordinating Center for Telecommunications (NCC) and recommend enhancements where required, and investigate Year 2000 (Y2K) readiness of the telecommunications infrastructure. Two OSG subgroups, the NCC Vision-Operations Subgroup and the Y2K Subgroup, respectively, addressed these actions. This report presents the charge, activities, conclusions, and recommendations of the OSG and its two subgroups since the last NSTAC meeting in September 1998.

In reviewing the functions of the NCC, the NCC Vision-Operations Subgroup considered revisions to electronic incident intrusion reporting criteria/process flow proposed by the NCC to guide NCC participants in reporting activities they identify as deviating from normal thresholds. The subgroup also assessed current participation in the NCC to see whether augmentation was needed for the NCC to fulfill its electronic indications, assessment, and warning (IAW) function. The subgroup agreed that broadening participation in the NCC would widen the scope of expertise and operational personnel available to fulfill the NCC's function and enable the NCC to grow as NS/EP telecommunications evolve. The subgroup developed, through consensus, a list of companies and Government departments and agencies for consideration by the National Communications System for participation in the NCC.

The Y2K Subgroup addressed the Y2K readiness of the critical products, services, and systems supporting the telecommunications infrastructure. The Y2K Subgroup facilitated meetings between industry and Government, helping to ensure that all aspects of the Y2K technology problem pertaining to NS/EP telecommunications were being considered and that appropriate contingency plans were being developed.

Throughout the current NSTAC cycle, the Y2K Subgroup collaborated with the NCC in their development of contingency plans to prepare for Y2K and improve intercarrier coordination for potential widespread outage recovery. The subgroup also initiated discussions with industry and Government entities that would be able to assist in creating an international early warning system for telecommunications outages attributable to Y2K.

Investigating the Y2K outreach efforts of the Federal Government, the Y2K Subgroup considered the importance of disseminating timely and accurate Y2K information to State and local levels. Additionally, the subgroup discussed the need for increased industry and Government interaction with the public to dispel prevalent misconceptions regarding the threat Y2K poses to all infrastructures, including telecommunications.

## ***President's National Security Telecommunications Advisory Committee***

---

During the current NSTAC cycle, the OSG also kept abreast of Federal exercise activities that pertained to the implementation of two Presidential directives. Presidential Decision Directive (PDD) 39,<sup>1</sup> published on June 21, 1995, emphasizes interagency coordination to prevent and manage the consequences of terrorism in all its forms. In May 1998, the President released PDD-62,<sup>2</sup> a directive establishing a structure for overseeing a wide range of Government agency policies and programs to defeat terrorism. Most of the exercises designed to implement these directives were subsequently modified to be Y2K based. Therefore, the OSG concluded that no terrorism related exercises were appropriate for NSTAC participation during the current cycle.

### **NSTAC Recommendation to the President**

Recommend that the President direct the President's Council on Y2K Conversion and the Federal Government to continue providing timely, meaningful, and accurate Y2K readiness and contingency planning information related to the information and communications critical infrastructures to State and local governments, thereby enhancing the flow of information to the general public and community Y2K groups.

### **NSTAC Direction to the IES**

- The NSTAC directs the IES to be prepared to support Emergency Response Training seminars or other Federal exercises related to PDD-39 and PDD-62, as appropriate.
- The NSTAC directs the IES to continue to monitor the NCC's implementation of its IAW function and to help refine, in an evolutionary fashion, reporting criteria and guidelines that facilitate the performance of the IAW function in the NCC.
- The NSTAC directs the IES to continue to cooperate and assist with Government Y2K preparedness efforts during the next NSTAC cycle.

---

<sup>1</sup> Counterterrorism Policy: Presidential Decision Directive 39

<sup>2</sup> Combating Terrorism: Presidential Decision Directive 62

## ***President's National Security Telecommunications Advisory Committee***

---

### **1.0 INTRODUCTION**

The President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) created the Operations Support Group (OSG) to evaluate the overall progress and direction of national security and emergency preparedness (NS/EP) telecommunications operational activities. OSG members represent the telecommunications, information technology, and systems integration industries and provide unique perspectives on the challenges of NS/EP operations and planning. The NSTAC XXII OSG members are listed in Annex A.

In October 1996, the IES created the National Coordinating Center for Telecommunications (NCC) Vision Task Force to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. The OSG assumed oversight of the task force in April 1997, renaming it the NCC Vision Subgroup and later the NCC Vision-Operations Subgroup. The NCC Vision-Operations Subgroup members are listed in Annex B.

The IES formed the OSG Year 2000 (Y2K) Subgroup immediately after the September 1998 NSTAC XXI meeting, where discussion of the issue of Y2K preparedness was prevalent. Specifically, the IES noted at NSTAC XXI that neither the public sector nor the private sector was able to guarantee total eradication of the Y2K problem, nor the adequacy of Y2K interoperability internetwork testing. Several Y2K issues emerged at that meeting, including the need for Y2K outreach efforts and emphasis on contingency planning and potential restoration scenarios. In addition, speakers at the NSTAC XXI business and executive sessions expressed concerns about the potential for public overreaction to the Y2K technology problem and the lack of a coordinated global approach to handle Y2K problems that were international in scope.

Prior to NSTAC XXI, the NCC Vision-Operations Subgroup undertook some of the NSTAC's initial work regarding Y2K contingency planning, having accepted additional tasking to evaluate NCC resources and help determine its coordination requirements for potential outages caused by any Y2K problems. The Y2K Subgroup was formed to continue this tasking and also investigate the Y2K readiness of the information and telecommunications infrastructure, particularly as it pertains to NS/EP telecommunications functions. The Y2K Subgroup members are listed in Annex C.

## **2.0 CHARGE**

The IES charge to the OSG for the current cycle included the following:

- Evaluate and support Presidential Decision Directive (PDD) 39<sup>1</sup> and PDD-62<sup>2</sup> implementation for their impact on NS/EP telecommunications.
- Evaluate and balance the current functions of the NCC with evolutionary changes of NS/EP telecommunications and recommend enhancements where required. Areas for review include:
  - criteria for reporting/process flow,
  - identify and deal with roadblocks,
  - membership,
  - outreach, and
  - assist the NCC with ongoing enhancements.
- Investigate the Y2K readiness of the information and telecommunications infrastructure as it relates to an enduring continuity of Government.
  - Investigate international Y2K preparedness efforts with respect to operations in the United States and abroad.
  - Assist the NCC in its contingency planning efforts.
  - Investigate societal implications of potential Y2K outages.
  - Investigate the implications of PDD-63<sup>3</sup> with respect to Y2K.

## **3.0 RESULTS**

### **3.1 PDD-39 and PDD-62 Implementation**

PDD-39, published on June 21, 1995, emphasizes interagency coordination to prevent and manage the consequences of terrorism in all its forms, including matters related to nuclear, biological, and chemical (NBC) terrorism, or threats to the Nation's infrastructure. PDD-62, issued in May 1998, established a National Coordinator for Security, Infrastructure Protection,

---

<sup>1</sup> Counterterrorism Policy: Presidential Decision Directive 39

<sup>2</sup> Combating Terrorism: Presidential Decision Directive 62

<sup>3</sup> *Protecting America's Critical Infrastructures*: Presidential Decision Directive 63

## ***President's National Security Telecommunications Advisory Committee***

---

and Counterterrorism to oversee programs and policies of Government agencies to defeat terrorism.

During the current cycle, the OSG received a classified briefing on PDD-62 and kept abreast of Federal exercise activities that pertained to the implementation of both directives. Included in these Federal exercise activities were the nationwide series of Emergency Response Training (ERT) Seminars conducted by the National Communications System (NCS), in partnership with the General Services Administration and NCC industry representatives. The purpose of the seminar program is to provide information to Regional Emergency Response, Federal, State, and industry personnel, on how Federal assistance is provided under activation of the Federal Response Plan (FRP). Additionally, the seminars provide an opportunity for agency representatives to share information on emergency response tools and for industry to provide expert information on the advances in technology.

Two phases of ERT have been completed with over 1,500 attendees. Regional industry participation has accounted for approximately 40 percent of seminar participation. During Phase 3, the agenda will include a major section on the recently published Terrorism Annex to the FRP.

However, Phase 3, scheduled to start during January/February 1999, has been delayed as a result of the focus of the Federal and State response communities on Y2K contingency planning and exercise activities. In addition, the OSG received copies of the Terrorism Annex to the FRP.

### ***3.1.1 Conclusion***

The OSG concluded that no PDD-39 and PDD-62 related exercises were appropriate for NSTAC involvement during the current cycle as a number of the exercises were Federal Emergency Management Agency (FEMA) emergency preparedness exercises that had been modified to be Y2K-based, or were designed for local level training. Those Government exercises that might have been appropriate were cancelled.

### ***3.1.2 NSTAC Direction to the IES***

The NSTAC directs the IES to be prepared to support ERT seminars or other Federal exercises related to PDD-39 and PDD-62, as appropriate.

## **3.2 National Coordinating Center for Telecommunications**

Based on an NSTAC recommendation, the NCS established the NCC in 1984 to serve as a telecommunications industry/Government organization to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities. In September 1996, the Manager, NCS, requested the IES' assistance in developing an indications, assessment,

## ***President's National Security Telecommunications Advisory Committee***

---

and warning (IAW) response capability in the NCC. The OSG reviewed the NCC Charter to determine if an IAW function could be incorporated into the NCC's mission. The NCC Vision-Operations Subgroup of the OSG concluded that the reporting of electronic intrusion incident information was within the scope of the NCC Charter and was a reasonable expansion of the day-to-day activities of the NCC.

In December 1997, NSTAC endorsed the NCC's implementation of an initial intrusion incident information processing pilot program to develop the IAW function. The NCC Vision-Operations Subgroup worked closely with the NCC to develop intrusion incident reporting criteria/process flow and format guidelines to be used in the pilot. The NCC IAW Center Pilot began on June 15, 1998, and was conducted over a 120-day trial period.

Following the conclusion of the NCC IAW Center Pilot on October 15, 1998, the Manager, NCC, briefed the subgroup on lessons learned from the pilot and proposed revisions to the reporting criteria/process flow and format guidelines. The proposed revisions were considered by the subgroup during the current cycle.

Under the revised criteria, NCC participants would report activities that they identified as deviating from their company's or agency's normal thresholds of operational activity. Subgroup members also agreed that mandatory format requirements might inhibit the reporting of intrusion incident information and, as a result, concluded that NCC participants should report information on such anomalous activities in the format of their choosing. The Manager, NCC, expressed the NCC's willingness to accept any information or report that entities are willing to provide. Based upon the experience of the NCC IAW Center Pilot, the NCC decided to fully incorporate the IAW function into its operations.

Potential roadblocks that might inhibit the reporting of information to the NCC were reviewed by the subgroup. The possibility that nondisclosure agreements would be needed to participate in the NCC was addressed along with the need to change the NCC Charter should such agreements be required. It was determined that at present, nondisclosure agreements would not be necessary. Therefore, no further review of the NCC Charter was warranted by the subgroup.

During the current cycle, the subgroup also assessed participation in the NCC to see if augmentation was needed for the NCC to fulfill the IAW mission. The subgroup agreed that broadening participation in the NCC would help the NCC fulfill its expanded mission. This action would widen the scope of expertise and operational personnel available to fulfill the NCC's function. Broader participation would enhance the technical base enabling the NCC to grow as technology and NS/EP telecommunications requirements evolve. To develop a list of possible participants, the subgroup first defined categories from which potential NCC participants might be drawn. The categories included system integrators, software and hardware providers, vendors, carriers, Internet service providers, gateway service providers, industry trade associations, and the



## ***President's National Security Telecommunications Advisory Committee***

---

lead Government agencies representing the critical infrastructures as identified in PDD-63.<sup>4</sup> Following that activity, the subgroup developed a list of companies and Government agencies and departments that the subgroup felt should be invited to participate in the NCC. Consideration of whether the company's product or service could contribute to or induce a widespread outage was a major criterion applied in identifying possible new NCC participants. The list of potential candidates for NCC participation is attached as Annex D.

The subgroup recognized that the primary responsibility of these new participants would be operational response, and that representatives would need to be available and willing to respond during incidents. Representatives also would be expected to participate in weekly staff meetings and other meetings or related exercises as necessary either in person or via teleconferencing.

The OSG concluded at the end of the NSTAC XXI cycle (September 1998) that the NCC provided a model for all infrastructures by which information could be gathered, analyzed, sanitized, and provided to the Government. During the current cycle, members of the OSG briefed Government agencies and departments on the role of the NCC and its growing ability to conduct cyber IAW as a means of assisting the NCC in outreach efforts. Outreach efforts have helped to raise awareness about the NCC, its mission, and its capabilities.

As a result of outreach activities, the NCC has been able to begin the process of sharing intrusion incident information with the National Infrastructure Protection Center (NIPC). The NIPC was created in February 1998 as a national critical infrastructure threat assessment, warning, vulnerability, law enforcement investigation, and response entity. The NIPC's mission is to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and cyber, that threaten or target the Nation's critical infrastructures. This mission allows the NIPC to collect information that may be useful to the NCC in fulfilling its mission, while intrusion incident information reported to the NCC may help the NIPC fulfill its mission.

The Information Sharing and Analysis Center (ISAC) concept was established under PDD-63. PDD-63 envisioned that an ISAC would be a private sector entity that would gather, analyze, sanitize, and disseminate to industry private sector information related to vulnerabilities, threats, intrusions, and anomalies affecting the critical infrastructures. Both industry and Government have recognized the NCC as an entity that currently performs most of these functions. A memorandum of understanding (MOU) is being drafted to position the NCC as an ISAC for the

---

<sup>4</sup> The lead agencies/departments are the Department of Commerce, the Department of the Treasury, the Environmental Protection Agency, the Department of Transportation, the Department of Justice/Federal Bureau of Investigation, the Federal Emergency Management Agency, the Department of Health and Human Services, the Department of Energy, the Central Intelligence Agency, the Department of State, and the Department of Defense. With the exception of the Environmental Protection Agency, all are represented in the NCS. Five of the eleven lead agencies participate in the NCC.

## ***President's National Security Telecommunications Advisory Committee***

---

telecommunications sector. The subgroup stands ready to assist in developing this MOU and fully supports the NCC in its role as an ISAC.

In addition, the NCC has briefed the subgroup on ongoing enhancements. Members received a briefing on the NCC's development of a network that will be available to connect companies and Government departments and agencies to the NCC. If that network is built, companies and Government departments and agencies will be able to report information on cyber incidents directly to the NCC by any appropriate means. The subgroup supports the concept presented by the NCC.

### ***3.2.1 Conclusions***

- The NCC IAW Center revised reporting criteria/process flow and their use as guidelines were found to be appropriate.
- To fulfill the NCC's enhanced mission, the Manager, NCS, should consider expanding participation in the NCC and invite additional participation as it deems necessary. Annex D provides a list, developed through subgroup consensus, of companies and Government agencies and departments recommended for consideration by the Manager, NCS, as potential new NCC participants.
- The NCC today performs the primary functions of an ISAC for the telecommunications sector and the Manager, NCS, should complete the MOU establishing it as such.

### ***3.2.2 NSTAC Direction to the IES***

The NSTAC directs the IES to continue to monitor the NCC's implementation of its IAW function and to help refine, in an evolutionary fashion, reporting criteria and guidelines that facilitate the performance of the IAW function in the NCC.

## **3.3 Y2K Technology Problem**

Both industry and Government have concerns regarding the Y2K readiness of the critical products, services and systems that support the public network (PN).<sup>5</sup> Should these components fail to process the Y2K date change, there is the possibility of disruptions to the operation of the PN, placing the Nation's security, economic vitality, and general public welfare at risk.

---

<sup>5</sup> The public network is defined as any switching system or voice, data, or video transmission system that is used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signalling networks).

## ***President's National Security Telecommunications Advisory Committee***

---

Although efforts to make the telecommunications infrastructure Y2K ready were well under way, discussions at NSTAC XXI identified some areas that needed to be addressed further. Those areas included Y2K outreach and awareness efforts, monitoring the readiness and interoperability testing of telecommunications networks, examining international Y2K preparedness efforts, and industry and Government contingency planning. As a result, the IES established the Y2K Subgroup to address these issues.

To address its charge, the Y2K Subgroup scheduled meetings with industry and Government entities responsible for Y2K preparation and contingency planning efforts. These meetings facilitated discussions between the subgroup and industry and Government representatives, helping to ensure that all aspects of the Y2K technology problem pertaining to NS/EP telecommunications were being considered. In addition to monitoring efforts to ensure the availability of NS/EP telecommunications in the event of potential outages or disruptions attributable to the Y2K problem, the subgroup examined the continuing dialogue between industry and Government on the subject of developing appropriate contingency plans. These meetings provided the subgroup with the basis for discussing the issues further with the President's Council on Y2K Conversion. The Council informed the subgroup that a meeting of Y2K national coordinators was scheduled at the United Nations on December 11, 1998, and suggested that the Y2K Subgroup identify telecommunications issues and concerns which the Council's chair could address at that meeting. Noting that the International Telecommunications Union (ITU) would be represented at that meeting, the Y2K Subgroup made the following suggestions to the Council for their consideration:

- The President's Council should encourage the ITU to become a repository and disseminator of Y2K information. The NCC, which is functioning as the central point of coordination for the telecommunications contingency plans of the U.S. Government and network providers, should be consulted by ITU members for information on available nonpublic, network-based systems and resources.
- The ITU has been compiling a database of telecommunications systems and gateways around the world. Ideally, this information should be made available to the NCC, allowing it to anticipate potential international network problems and match U.S. assets accordingly.

Throughout the current cycle, the subgroup collaborated with the NCC in their development of contingency plans to prepare for Y2K and improve intercarrier coordination for potential widespread outage recovery. These efforts include enhancement of the National Telecommunications Coordinating Network (NTCN), a Y2K compliant, multipath communications network supporting coordination among Federal Government and telecommunications industry centers during times of degraded PN operation. The NCC also is taking the appropriate steps to link the NTCN, via the NCC conference bridge, with the Alerting

## ***President's National Security Telecommunications Advisory Committee***

---

and Coordinating Network, a nationwide network of private lines that is separate from the PN and which connects major telecommunications providers, vendors, and suppliers. In addition, the Y2K Subgroup has been working with the NCC to establish a tracking mechanism to monitor domestic Y2K outages. This tracking mechanism is being considered for international application.

In examining international Y2K preparedness efforts, the Y2K Subgroup analyzed efforts to establish an international Y2K early warning system for telecommunications. The early warning system would collect information on Y2K experiences as they occurred in countries west of the International Date Line. The subgroup initiated discussions with industry and Government entities that would have a need for an early warning system and possessed the ability to assist in creating an early warning system, focusing particularly on potential telecommunications outages.

The subgroup noted that the NCC would play a central role in the early warning system, coordinating the distribution of information from telecommunications service providers or Government entity abroad regarding Y2K related problems. The subgroup has been working with the OMNCS in its efforts to establish an international Y2K early warning system for telecommunications, actively seeking information and testing results from industry international sites and ITU members, as well as field reports from Department of Defense (DOD), Department of State (DOS), and NSTAC companies with international offices. In addition, subgroup members met with members of the ITU Y2K Task Force; and as a result, negotiations are taking place for the coordination of Y2K information. It is anticipated that meaningful exchange of Y2K information will occur as a result of these meetings.

The subgroup also collaborated in developing other OMNCS contingency planning efforts and monitored the network testing being conducted by the Y2K Telco Forum and the Alliance for Telecommunications Industry Solutions as well as the compilation of the latest Y2K compliance data from all telecommunications companies. The OMNCS will use this information to assess the effects of potential disruptions on NS/EP functions.

In addition, the subgroup considered the importance of the State and local Y2K outreach efforts of the Federal Government. Through these efforts, the Federal Government has been providing information to State and local governments, local emergency management personnel, and the U.S. public in general regarding potential Y2K related problems and contingency plans to be initiated. Examples of these outreach initiatives include the work of the President's Council on Y2K Conversion to establish a toll-free Y2K telephone line that will provide consumers with timely and accurate information, and FEMA's Y2K Consequence Management workshops for local emergency management services offices.

Investigating the Y2K outreach efforts of the Federal Government, the subgroup considered how the Y2K problem is perceived at the community level and how such information is being

## ***President's National Security Telecommunications Advisory Committee***

---

promulgated by the growing number of local and regional Y2K citizen's groups. In examining the issue, the subgroup met with representatives of and researched community and grassroots groups who, through community forums and Internet communications, are able to provide citizens with extensive Y2K-related information. Of particular concern to the subgroup was the promulgation of misinformation about the potential effects of the Y2K technology problem. Moreover, the subgroup noted the lack of direct coordination between the initiatives of community-level Y2K groups and the Y2K outreach efforts of the Federal Government.

To counter the misinformation being promulgated by some community and grassroots groups, the subgroup discussed the need for increased industry and Government interaction with the public detailing Y2K compliance and contingency planning efforts. This information would aid in alleviating public skepticism and dispel prevalent myths regarding the threat Y2K poses to all infrastructures, including telecommunications. In addition, industry and Government need to understand that local and regional Y2K focus groups have the potential to amplify public fears and undermine Y2K preparation efforts by spreading misinformation regarding Y2K. By coordinating their efforts with all levels of Government, these groups can instead function as an important link in a public Y2K education campaign.

Members of the subgroup visited the Whidbey Telephone Company (WTC), a small local exchange carrier whose area included the City of Langley on Whidbey Island, Washington State, to further investigate the societal impact of Y2K and the ability of critical infrastructure managers to assist the community in alleviating these impacts.

The WTC, working with the Island County Department of Emergency Services, the City of Langley, and other concerned public and private organizations, has demonstrated the community level impact that entrepreneurial support for disaster contingency planning in general can have on Y2K preparations. WTC management has emphasized contingency planning which includes:

- establishing multiple, geographically diverse connections outside their service area;
- establishing connections to more than one other carrier;
- having significant battery and generator backup power;
- having basically only lines underground;
- establishing geographically diverse switch deployment;
- retaining and regularly using older manual switches as backup to computer driven switches to ensure an available emergency alternative; and

## ***President's National Security Telecommunications Advisory Committee***

---

- establishing connections to more than one Internet backbone service for the customers of the Internet Service Provider (ISP).

Beyond steps taken to enhance their survivability, WTC management is active in disaster planning in the local community. They offer alternate command post capabilities for the community to coordinate emergency services, and can support emergency services for areas outside their service area. Their willingness to help has included providing water for community members whose supplies have been cut off temporarily. This level of community involvement extends to Y2K contingency preparations. The involvement of the WTC in all these areas demonstrates the ability of critical infrastructure managers to assist their communities with emergency planning.

In addition, the subgroup investigated the implications of PDD-63 with respect to Y2K and agreed that Y2K may provide an example of a cyber-related incident of global scope. Y2K can serve as a test case and provide lessons learned for additional preparations required to protect the Nation's critical infrastructures. The subgroup found that the Government recognizes this and is incorporating Y2K efforts into critical infrastructure protection efforts.

### ***3.3.1 Conclusions***

- The OSG agrees that it is prudent to establish an international Y2K early warning system for telecommunications recognizing that the 17-hour advance notice will afford the United States a very short time frame in which to initiate response or remediation efforts. In addition, disruptions and outages attributable to Y2K could occur well before or after the actual date change.
- The OSG endorses the NCC's proposed domestic and international role as a national coordinating body in preparing for and responding to any Y2K telecommunications events, including NCC involvement in a Y2K early warning system. The OSG supports the continuing enhancement of the NTCN, the monitoring of network testing being conducted by various organizations, and the compiling of Y2K compliance data from all telecommunications companies.
- Initial efforts indicate that educational initiatives of the Federal Government to prepare emergency service personnel for Y2K-related events are helpful at the Federal, State, and local levels. However, in light of the considerable number of community-level Y2K focus groups with the potential to promulgate Y2K misinformation, the OSG agrees that there is a need for the Government to continue to be assiduous in disseminating accurate information and countering public skepticism.

## ***President's National Security Telecommunications Advisory Committee***

---

### ***3.3.2 NSTAC Recommendation to the President***

Recommend that the President direct the President's Council on Y2K Conversion and the Federal Government to continue providing timely, meaningful, and accurate Y2K readiness and contingency planning information related to the information and communications critical infrastructures to State and local governments, thereby enhancing the flow of information to the general public and community Y2K groups.

### ***3.3.3 NSTAC Direction to the IES***

The NSTAC directs the IES to continue to cooperate and assist with Government Y2K preparedness efforts during the next NSTAC cycle.

**ANNEX A**

**OPERATIONS SUPPORT GROUP MEMBERS**



***President's National Security Telecommunications Advisory Committee***

---

**OPERATIONS SUPPORT GROUP MEMBERS**

COMSAT	Mr. Ernie Wallace, Chair
U S WEST	Mr. Jon Lofstedt, Vice Chair
AT&T	Mr. Harry Underhill
CSC	Mr. Guy Copeland
EDS	Mr. Bob Donahue
GTE	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
MCI WorldCom	Mr. Mike McPadden
Nortel Networks	Dr. Jack Edwards
NTA	Mr. Bob Burns
SAIC	Mr. Bob Rankin
Unisys	Dr. Dan Wiener
USTA	Dr. Vern Junkmann

**GOVERNMENT CONTRIBUTORS**

DOC	Dr. Jerry Gibbon
DOS	Ms. Kim Godwin
GSA	Mr. Tom Sellers
NTIA	Mr. Bill Belote
NCC	Mr. Bernie Farrell

**ANNEX B**

**NCC VISION-OPERATIONS SUBGROUP MEMBERS**

***President's National Security Telecommunications Advisory Committee***

---

**NCC VISION-OPERATIONS SUBGROUP MEMBERS**

U S WEST	Mr. Jon Lofstedt, Chair
ITT	Mr. Joe Gancie, Co-Chair
AT&T	Mr. Harry Underhill
COMSAT	Mr. Ernie Wallace
EDS	Mr. Bob Donahue
GTE	Ms. Ernie Gormsen
MCI WorldCom	Mr. Mike McPadden
Nortel Networks	Dr. Jack Edwards
NTA	Mr. Bob Burns
SAIC	Mr. George Murray
USTA	Dr. Vern Junkmann

**GOVERNMENT CONTRIBUTORS**

DOC	Dr. Jerry Gibbon
DOS	Mr. Jeff Meyers
GSA	Mr. Tom Sellers
NTIA	Mr. Bill Belote
NCC	Mr. Bernie Farrell

**ANNEX C**

**YEAR 2000 SUBGROUP MEMBERS**

***President's National Security Telecommunications Advisory Committee***

---

**YEAR 2000 SUBGROUP MEMBERS**

GTE	Mr. Lowell Thomas, Chair
NTA	Mr. Bob Burns, Co-Chair
COMSAT	Mr. Ernie Wallace
CSC	Ms. Sheila Andahazy
GTE	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
MCI WorldCom	Mr. Mike McPadden
Nortel Networks	Dr. Jack Edwards
USTA	Dr. Vern Junkmann
U S WEST	Mr. Jon Lofstedt

**GOVERNMENT CONTRIBUTORS**

NCC	Mr. Bernie Farrell
OMNCS	LTC Charles Fletcher

**ANNEX D**

**POTENTIAL CANDIDATES FOR NCC PARTICIPATION**

***President's National Security Telecommunications Advisory Committee***

---

**POTENTIAL CANDIDATES FOR NCC PARTICIPATION**

<b>Company</b>	<b>Reason Suggested</b>
America On-Line/Netscape	Internet service provider
Boeing	Network systems provider
Cisco	Telecommunications equipment and software provider
Computer Sciences Corporation	Systems integrator and end to end services provider
IBM	Systems integrator, and software, equipment, and end to end telecommunications services provider
Illuminet	Telecommunications services provider
Iridium	Satellite and mobile communications provider
Lockheed Martin	Systems integrator and end to end services provider
Lucent	Telecommunications equipment manufacturer and software provider
Microsoft	Software provider
Nortel Networks	Telecommunications switch manufacturer and software provider
Telcordia Technologies	Network operating platforms and operations support systems provider
Unisys	Systems integrator and end to end services provider

## ***President's National Security Telecommunications Advisory Committee***

---

### **Government Agencies**

The following Government agencies and departments, with the exception of the Department of Commerce's National Telecommunications and Information Administration, were suggested as possible new NCC participants as they were identified by PDD-63 as the lead agencies for critical infrastructure sector liaison or special function. The entities are not participants in the NCC at this time.

Central Intelligence Agency

Department of Commerce's National Telecommunications and Information Administration

Department of Health and Human Services

Department of Transportation

Department of Treasury

Environmental Protection Agency

Federal Emergency Management Agency