THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

VULNERABILITIES TASK FORCE REPORT
TRUSTED ACCESS

January 27, 2003

Table of Contents

Executive Summary

This report addresses the Administration's concerns that the telecommunications infrastructure may be more vulnerable because trusted physical access (hereafter referred to as "access") is granted to individuals requiring entrance to sites where telecommunications assets are concentrated. For the purpose of this report, access control implies that the authority responsible for a specific building, site, or telecommunications asset has the ability to limit access to only those individuals it trusts. Categories of sites of primary concern include those controlled by incumbent local exchange carriers under Federal Communications Commission authority (e.g., collocation sites), sites controlled by other telecommunications and commercial enterprises (e.g., telecom hotels), sites controlled by customers of telecommunications providers, and sites where access is difficult to control (e.g., infrastructure assets that interconnect critical facilities).

A malicious act (such as tampering with or destroying telecommunications assets) committed against any single site that results in its damage or loss would not likely cause regional or national outages. The loss of such a site could, however, present local or last-mile impacts that might adversely affect national security and emergency preparedness (NS/EP) services. As such, it is necessary to identify and address factors that could affect the efficacy of access control procedures for critical telecommunications sites.

It is important to recognize that *any* one individual with malicious intent accessing *any* critical telecommunications facility could present a threat. At any given time and on a daily basis, numerous individuals access critical telecommunications facilities. The threat of insiders performing malicious acts also transcends each type of site discussed in this document. Legitimate employees with authorized access to critical facilities can have malicious intent for any number of reasons (e.g., a disgruntled or compromised employee). In relation to the threats posed by individuals, personal identification (ID) procedures can also be vulnerable. For instance, companies employ different picture ID requirements and processes for individual access to critical sites. A highly secure, standard type of certificate-based picture ID card is not available for wide-scale use. Individual-based threats, which are common across all sites, also highlight the need for industry to be able to conduct comprehensive national security background checks on key personnel accessing or working at critical sites. The absence of a national database with pertinent screening information prevents industry from performing an effective screening. Voluntary best practices regarding the physical security of, and access to, critical telecommunications assets have not been universally promulgated and employed. A foundation of voluntary procedures might help to reasonably secure facilities without stifling competition.

Different access control requirements and procedures will likely be necessary under normal conditions versus times of stress, such as a local, regional, or national emergency. Not only is the authority in control of access likely to change during emergency response situations, but also the perimeter of the controlled area may change. If the site is the focal point of an emergency, such as a hazardous material (hazmat) incident, fire, or criminal act, access control may transfer from the building owner to representatives of fire, police, State, or Federal authorities. When the authority devolves from the owner's control to others, access control procedures must be adapted to the new environment. The President's National Security

Telecommunications Advisory Committee (NSTAC) believes that the best procedure will incorporate representatives of the control authority and the site owner so that individuals seeking access are properly screened.

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies to—

- Coordinate with industry and State and local governments to develop guidance for:
  - creating national standards and capabilities for national security background checks, screening, and National Crime Information Center reviews
  - defining the criteria for inclusion in background checks
  - identifying who should be subject to background checks.

- Lead the research and development and standards bodies' efforts to make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of individuals at critical sites.

- Coordinate with industry to develop a national plan for controlling access at the perimeter of a disaster area, in coordination with State and local governments. This plan should be incorporated in the *Federal Response Plan*.

- Adopt telecommunications service procurement security policy guidelines that provide positive incentives to those companies that follow Network Reliability and Interoperability Council best practices for access control.

Vulnerabilities Task Force Report
Trusted Access to Telecommunications Facilities

1.0 Introduction

The Administration has expressed concern that the concentration of multiple entities' telecommunications assets in specific locations may have implications for the security and reliability of the telecommunications infrastructure. During the business and executive sessions of the National Security Telecommunications Advisory Committee (NSTAC) XXV meeting, concerns focused on telecom hotels, Internet peering points, trusted access to telecommunications facilities, equipment chain of control issues, and cable landings.

Following this meeting, the NSTAC Industry Executive Subcommittee (IES) chartered the Vulnerabilities Task Force (VTF) to examine these issues and vulnerabilities in common duct runs and rights of way, as well as the logical security issues associated with the Open Advanced Intelligent Network (AIN).

The current environment, characterized by the consolidation, concentration, and collocation of telecommunications assets, is the result of regulatory obligations, business imperatives, and technology changes. This construct has created a more diverse network topology but also has heightened security concerns. Because the networks composing this topology, which are owned and operated by private industry, are the critical infrastructures upon which the Government and other sectors rely, the security of these networks is of utmost importance.

Each of the aforementioned security issues will be addressed in separate VTF reports. A final executive summary document will be created to highlight each topic and NSTAC recommendation.

2.0 Specific Tasking

This report addresses the Administration's concerns that the telecommunications infrastructure may be more vulnerable because trusted physical access (hereafter referred to as "access") is granted to individuals requiring entrance to sites where telecommunications assets are concentrated.

3.0 Scope of This Report

For the purpose of this report, access control implies that the authority responsible for a specific building, site, or telecommunications asset has the ability to limit access to only those individuals it trusts. This trust may be extended by the granting authority to organizations rather than to specific individuals, in which case, an additional means is needed to authenticate the individual as a trusted member of the organization to which access has been granted.

The five areas of access addressed in this report are as follows:

a) Categories of individuals who require access might include:
   - The facility owners'
     - Employees
     - Telecommunications equipment vendors
     - Other vendors (fuel, janitorial supplies, cafeteria workers, vending machine suppliers, security forces, etc.)
     - Building contractors (heating, air conditioning, plumbing, electrical, etc.)
     - Subcontractors to other vendors and contractors

   - The facility owners' tenants, including their tenants':
     - Employees
     - Contractors
     - Vendors
     - Subcontractors to other vendors and contractors

   - Other non-telecom related organizations or individuals requiring access
     - First responders (police, firefighters, etc.)
     - Other municipal workers (water department, sanitation department, etc.)

b) The authority granting access
   - Incumbent local exchange carrier (ILEC) that owns a central office operated as a collocation site
   - Commercial landlord operating a telecom hotel, Internet peering point, or other commercial site where telecommunications assets are concentrated
   - A customer who controls access to his own building, leased space, or telecommunications room where multiple telecommunications providers have placed their cables or equipment

c) The buildings, sites, and assets subject to access control procedures
   - ILEC central offices subject to collocation requirements imposed by the *Telecommunications Act of 1996*[1] (hereafter referred to as the *Telecommunications Reform Act*)
   - Other telecommunications equipment offices
   - Telecom hotels
   - Other commercial floor space conditioned for the support of telecom assets and/or related equipment
   - Outside plant locations, such as equipment cabinets and controlled environmental vaults (CEV).

d) Remote/distributed buildings, sites, and assets to which access is difficult to control
   - Buried cables, pedestals, neighborhood terminal boxes, etc.
   - Unmanned and unguarded towers and "huts"

[1] *Telecommunications Act of 1996*, Public Law No. 104-104, 110 Stat. 56 (1996).

- Other unguarded outside plant facilities
- Manholes, cable ducts, etc.

e) Practices, rules, regulations, and best practices applicable to access control
- Federal Communications Commission (FCC) regulations
- State public utilities commission/public service commission regulations
- Federal/State law
- Contracts
- Best practices.

4.0 Categories of Sites With a Concentration of Assets

This report addresses physical access that is authorized by some authority to a site where telecommunications assets have been concentrated.[2] Several types of these sites are considered. It is important to note that while there are a number of reasons for classifying the sites in the categories listed below, some providers might operate in one or more of these categories in different marketplaces. For example, a traditional ILEC that chooses to offer local access service in an area outside its historic territory will be a competitive local exchange carrier (CLEC) in that environment. Where ILECs gain access to the long distance market, they become an interexchange carrier (IXC). Likewise, a traditional IXC that chooses to offer local access service is operating as a CLEC. These distinctions will eventually disappear.

Categories of Sites:

a) Sites Controlled by ILECs Under FCC Authority or Regulation

The Telecommunications Reform Act, as implemented by the FCC, placed collocation[3] requirements on ILECs to enable CLEC access to elements of the local distribution network. One such arrangement is virtual collocation, in which the CLEC occupies building space it owns or leases somewhere near the ILEC central office. The ILEC, CLEC, or a third party connects the two facilities with copper cable, fiber cable, or some other transport medium. This arrangement allows for interconnection while both carriers continue to control access to their own buildings in accordance with their own access controls rules, regulations, and procedures.

Another arrangement, which is more pertinent to this report, is physical collocation. Under FCC rules, ILECs are required to allow CLECs to install equipment in ILEC central offices. Despite the perception that this mandated rule has increased vulnerability, in reality, it is one more manifestation of a longstanding problem discussed in Section 5.0.

[2] Access may also occur logically via electronic means in the operations, administration, and management (OA&M) space. Logical access will be discussed in a separate report on the AIN.

[3] The FCC defines collocation as, "The duty to provide, on rates, terms, and conditions that are just, reasonable, and nondiscriminatory, for physical collocation of equipment necessary for interconnection or access to unbundled network elements at the premises of the local exchange carrier, except that the carrier may provide for virtual collocation if the local exchange carrier demonstrates to the State commission that physical collocation is not practical for technical reasons or because of space limitations." *Telecommunications Act of 1996,* 47 U.S.C. § 251 (c) (6).

b) Sites Controlled by Other Telecommunications Enterprises

While not mandated to do so by the FCC, other telecommunications enterprises, such as IXCs, CLECs, Internet service providers (ISP), and Web-hosting operators, have opened their buildings and other sites to tenants with whom they wish to interconnect. Some of the access control issues pertinent to ILEC central offices are also relevant at these sites.

c) Sites Controlled by Other Commercial Entities

A commercial entity, foreign or domestic, could own or lease and then sublet space to telecommunications service providers for installing equipment used in the telecommunications infrastructure. Types of facilities where this occurs include telecom hotels, Internet peering points, and Web-hosting sites. Space utilized in telecom hotels and collocation facilities could include the entire building, floors within a building, or a portion of a single floor or floors. Separate floors, rooms, or cages are usually made available to the individual tenants.

Overall building access control to such sites is at the discretion of the landlord subject to any applicable Federal, State, and municipal requirements. Tenants also have some control of access to their own spaces and equipment.

d) Sites Controlled by Customers of Telecommunications Providers

Customers also control access to some locations where multiple carriers' assets have been concentrated. For example, a multistory building owned and operated by a commercial enterprise might fully occupy the building or lease some space to other tenants. Typically, commercial buildings have a common cable entrance and telecommunications equipment room for the use of all telecommunications service providers serving customers in the building. Additional equipment may also be located in the space that the customer occupies.

In the case of the common entrance and equipment room, the building owner or management firm usually controls access. The individual tenants control access to the spaces they occupy. Building services personnel, such as janitors and security employees, also have access, although they may not be allowed in the locked equipment spaces.

e) Sites Where Access Is Difficult To Control

Authorized and unauthorized access to telecommunications infrastructure assets that interconnect central offices, telecom hotels, collocation facilities, Internet peering points, and other concentration nodes cannot be controlled in the manner that access to buildings, floors, and rooms can be controlled. There are thousands of miles of underground and buried cable, and any number of controlled environmental vaults, huts, radio towers, equipment cabinets, and pedestals throughout the infrastructure. Such facilities are secured to the extent possible with electronic locks, padlocks, fences, alarms, security cameras, and the like; but in remote sites, unauthorized access can be achieved and mischief and escape completed before authorities can respond to any alarm.

The deployment of such assets in the infrastructure is far too extensive to control access to prevent tampering. Since the terrorist attacks of September 11, 2001, many Federal and State organizations have requested lists of such assets for the stated purpose of helping industry protect those sites. However, it should be noted that initiatives by the Department of Defense under the U.S. Key Asset Protection Program and Critical Infrastructure Protection Program have concluded that not even the U.S. military resources would be adequate to protect the nationwide web of telecommunications assets.

While the outside plant interconnections between infrastructure nodes may be most at risk due to their accessibility and lack of direct access control, the evolution in networks has significantly changed the way these paths are used to carry network traffic. What was once a fixed backbone structure is today vastly more dynamic and less structured. Alternate spare capacity is built into the architecture; routes may be automatically restored both electronically and optically; and competition in the industry has resulted in separate networks and redundant cable routes. Fiber rings and self-healing networks are becoming more ubiquitous, and the effect of a cable cut in the "backbone" of the infrastructure rarely causes a loss of any service for more than a few minutes. In the local distribution plant where there is normally only one pathway to the customer premises, cable cuts are more disruptive but to a much smaller universe of users. It is important to note that the number one threat to the outside plant infrastructure continues to be the construction backhoes, as evidenced in outage reporting to the FCC by the carriers.

5.0 Access Control Vulnerabilities

NSTAC has stated in previous reports that a scenario cannot be envisioned in which a single point of failure could cause a widespread public network disruption.[4] A malicious act (such as tampering with or destroying telecommunications assets) committed against any single site that results in its damage or loss would not likely cause regional or national outages.[5] The loss of such a site could, however, have local or last-mile impacts[6] that might adversely affect national security and emergency preparedness (NS/EP) services. The possibility of NS/EP impacts from site loss or damage highlights why access control is a valid concern. It also emphasizes the need to identify and address factors that could limit the efficacy of access control procedures for critical telecommunications sites. Primary factors analyzed below include individuals with malicious intent, the omnipresent insider threat, the lack of a standard personal identification process, and the lack of universally applied access control procedures and best practices.

Notwithstanding the differences in sites highlighted in Section 4.0, *any* one individual with malicious intent accessing *any* critical telecommunications facility could present a threat. At any given point in time, and on a daily basis, numerous individuals access critical telecommunications facilities. Examples of types of individuals accessing sites include telecommunications equipment vendors, fuel suppliers, janitorial services, cafeteria workers, vending machine suppliers, security forces, and heating, air conditioning, plumbing, electrical

[4] See NSTAC *Convergence Task Force Report*, June 2001; *Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies*, June 1999; and *Widespread Outage Subgroup Report*, December 1997.

[5] See NSTAC *Widespread Outage Subgroup Report*, December 1997; and the "Single Point of Failure Exercise" section of the NSTAC *Convergence Task Force Report*, June 2001, pp. 13-15.

[6] NSTAC emphasized in its *Convergence Task Force Report* (p. 13) that, "…single points of network failure, such as a telecom hotel or specific local switches, would likely only have local or last-mile impacts rather than regional or national consequence."

contractors, and their subcontractors. Other personnel who are granted access occasionally include police officers, firefighters, and municipal workers, such as the water department and the sanitation department. These individuals may be granted unescorted access from day to day until their work in the facility is completed.

The authority controlling the facility will typically grant access to another organization with the requirement that the organization certify it has conducted the appropriate background checks on its employees and contractors. Therefore, the integrity of access control becomes a matter of trust.

The threat of insiders performing malicious acts also transcends each type of site discussed in this document. Legitimate employees with authorized access to critical facilities can have malicious intent for any number of reasons (e.g., disgruntled or compromised employee). The insider threat might be hard to recognize and difficult to defend against.

In relation to the threats posed by individuals, personal identification (ID) procedures can also be vulnerable. For instance, companies employ different picture ID requirements and processes for individual access to critical sites. These requirements have varying degrees of effectiveness for certifying that the person shown on the picture ID card is, in fact, the person presenting that card. A highly secure, standard type of certificate-based picture ID card is not available for wide-scale use. If made available, such a card used voluntarily by companies would augment existing access control procedures.

The aforementioned individual-based threats, which are common across all sites, highlight the need for industry to be able to conduct comprehensive national security background checks on key personnel accessing or working at critical sites. However, there are no standard guidelines or capabilities for conducting robust national security background checks available to industry. Telecommunications companies typically employ private firms to perform background checks on personnel. These firms do not follow standard requirements and have limited investigative powers. Typical screenings include only checks of State or local police records, and in some cases, are limited to the county in which the employee currently resides. The absence of a national database with pertinent screening information prevents industry from performing an effective screening. The only exceptions are the formal Government-sponsored investigations performed on employees whose jobs require them to have access to sensitive or classified information. Those investigations are lengthy and may last up to 24 months. Some union/management agreements do not contain language stating that employment is contingent upon passing such screenings. Incumbent carriers cannot verify the validity of the background investigations undertaken by CLECs on their employees and have to accept their findings in good faith. As a result, diligent screening procedures might not be applied to key personnel across industry. In addition, non-telephone company personnel (e.g., contractors, vendors) accessing critical sites might not be subject to rigorous screening procedures by their individual companies.

An additional concern is that voluntary best practices regarding the physical security of and access to critical telecommunications assets have not been universally promulgated and employed. A foundation of voluntary procedures might help to reasonably secure facilities without stifling competition.

6.0 Key Initiatives for Mitigating Access Control Vulnerabilities

Because the Nation relies on public telecommunications infrastructure for critical NS/EP communications and operations, vulnerabilities related to access control procedures for critical sites must be addressed. Key initiatives for mitigating vulnerabilities include developing guidance for standard national security background checks, developing and implementing physical security best practices, and conducting internal company risk assessments related to housing equipment at specific sites.

It is important for the telecommunications industry to have access to a standard system of national security background checks and identity verification to help ensure only rigorously vetted and authorized personnel are granted access to critical facilities. Therefore, the Federal Government could work in conjunction with State and local governments and industry to develop guidance for the creation of national standards for national security background checks, including screenings and National Crime Information Center (NCIC) reviews. The Government could also assist industry in identifying the criteria and verification procedures for inclusion in national security background checks and indicate who should be subject to the checks.

Availability of an interoperable standard for "tamper-proof," certificate-based picture ID cards could also help enhance access control at critical sites. The Government could support research and development and standards bodies activities concerning the feasibility of creating such an ID card. If found to be feasible, companies could voluntarily adopt and implement the cards to augment their own access security procedures and requirements. Certificate-based cards could enable stronger vetting processes and help to prevent fraudulent or unauthorized access by individuals at critical sites.

Voluntary best practices regarding physical security of and access to critical telecommunications assets should also be identified and adopted by all concerned parties. The Network Reliability and Interoperability Council (NRIC) is establishing a set of voluntary physical security and access control best practices. Even though implementing robust access control mechanisms might not be possible for every element of the telecommunications infrastructure (see Section 4e.), voluntarily applied NRIC best practices for access control could offer a framework for companies to reduce vulnerabilities. Therefore, the Federal Government should encourage industry adoption of NRIC best practices by establishing telecommunications service procurement security policy guidelines that provide positive incentives to those companies employing the best practices.

Each enterprise choosing to occupy facilities discussed in Section 4.0 must determine if available access control measures comply with their business continuity policies. The effect of unauthorized tampering with telecommunications equipment in such a facility would likely be limited to only those business functions and operations conducted or supported by assets in the building. Therefore, if all tenants would conduct an analysis of the risk to their critical business functions based on sound business continuity practices, security concerns could be identified and mitigated.

6.1 Procedures for Access Control and Authenticating Personnel During Emergencies

Different access control requirements and procedures will likely be necessary under normal conditions versus times of stress, such as a local, regional, or national emergency. Not only is the authority in control of access likely to change during emergency response situations, but also the perimeter of the controlled area may change. Under either condition, access control procedures will require a minimum of two steps to authenticate an individual for access to a building or other site. The authority granting access must be able to (1) determine that the individual requesting access is who he or she claims to be, and (2) verify that the individual is authorized to have access.

Under normal conditions, the site owner or a security firm operating on behalf of the owner will most likely control access to the site. In the event that the site is the focal point of an emergency, such as a hazardous material (hazmat) incident, fire, or criminal act, access control may transfer from the building owner to representatives of the fire, police, State, or Federal authorities. When the authority devolves from the owner's control to others, access control procedures must by adapted to the new environment. The NSTAC believes that the best procedure for properly screening persons seeking access will include utilizing representatives of both the control authority and the site owner. Screening will verify that personnel are who they claim to be, that they are members of an organization authorized to have access under the existing conditions, and that they have a legitimate need to enter the site. This can be accomplished only if the controlling governmental authority will rely upon the site owner, perhaps with assistance of the owner's tenants, to make the final decision that access is necessary.

In major emergencies, the perimeter under control may extend to several city blocks or even to several counties. In such events, perimeter control is likely to transfer from the first responders to State authorities and, perhaps, Federal authorities. To avoid impeding legitimate access, it is important that each governmental authority that controls access follows a standardized process. The need for a standardized access control process was documented in our findings and recommendation to the President,[7] following the response to the terrorist attacks of September 11, 2001. Once adopted, such procedures could be included in the *Federal Response Plan* for reference by all appropriate parties. By working together and following a national standard, access can be appropriately controlled; and procedures can transition smoothly from one authority to the next as perimeter control changes hands.

The ability to determine an individual's need for access to a disaster site, or any location during an abnormal condition, should be decided by the corporation responding to the disaster or incident. Access control will require coordination between the Government agency controlling the site and the corporation requesting access for the employee. The controlling authority should be responsible for allowing access, while the corporation's representative is responsible for ensuring the identity of the employee and ensuring the individual needs access to that site at that instance. A method of identification could be achieved through use of a "tamper-proof" certificate-based picture ID that is widely acknowledged as a means of identification. The NSTAC cautions against the issuance of any ID card intended only for emergency responders requiring access to disaster sites following a Presidential disaster declaration. The NSTAC

[7] See NSTAC letter dated December 17, 2001.

contends that it will be impossible for the telecommunications industry to ensure that the cards are in the hands of those individuals needed to respond to any event that may occur anywhere in the United States.

7.0 Conclusions/Findings

- The ability to effectively control access to critical telecommunications assets in buildings and other sites where such assets are concentrated is a valid concern.

- Access is a matter of trust even in the presence of contractual obligations.

- A scenario cannot be envisioned wherein a single point of failure could cause a widespread public network disruption. However, access control remains an important issue because the loss of, or damage to, a site housing numerous critical telecommunications assets could have local or last mile impacts and adversely affect NS/EP services.

- Primary factors influencing the efficacy of access control procedures include individuals with malicious intent, the omnipresent insider threat, the lack of standard personal identification and background check capabilities, and a lack of universally applied access control procedures and best practices.

- At any given point in time, numerous individuals are accessing critical telecommunications facilities. Any one individual with malicious intent could present a threat. The insider threat also transcends each type of critical site and is difficult to defend against.

- Currently there is neither a national standard nor capability available for companies to conduct background checks, screening, criminal investigations, and identity verification procedures for key personnel requiring access to critical telecommunications facilities or critical job categories.

- Because of the lack of national background check standards, it may be more difficult to mitigate the insider threat.

- The Federal Government, in conjunction with State and local governments and industry, could develop guidance for the creation of national standards for national security background checks and identity verification procedures for key personnel.

- Industry's voluntary implementation of best practices for access control to critical telecommunications assets could help secure such facilities without stifling competition.

- Even though robust access control is not possible for every element of the infrastructure, voluntary NRIC best practices for access control could provide a framework for companies to reduce access vulnerabilities.

- Access control of the perimeter of a disaster site can be enhanced by the adoption of standardized access control procedures across Federal, State, and local government jurisdictions.

- Personal ID capabilities can be enhanced through use of a "tamper-proof" certificate-based picture ID that is widely acknowledged as a secure means of identification.

- The issuance of national identification cards for use during disaster response activities may not be viable because telecommunications companies cannot guarantee *all* required response personnel for each unique emergency would possess these cards.

8.0 Recommendations

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies to—

- Coordinate with industry and State and local governments to develop guidance for:
  - creating national standards and capabilities for national security background checks, screening, and National Crime Information Center reviews
  - defining the criteria for inclusion in background checks
  - identifying who should be subject to background checks.

- Lead the research and development and standards' bodies efforts to make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of individuals at critical sites.

- Coordinate with industry to develop a national plan for controlling access at the perimeter of a disaster area, in coordination with State and local governments. This plan should be incorporated in the *Federal Response Plan*.

- Adopt telecommunications service procurement security policy guidelines that provide positive incentives to those companies that follow NRIC best practices for access control.

APPENDIX A—TASK FORCE MEMBERS AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

BellSouth Corporation	Mr. Shawn Cochran, Chair
Electronic Data Systems	Mr. Dale Fincke, Vice-Chair
Nortel Networks	Dr. Jack Edwards, Vice-Chair
AT&T Corporation	Mr. Harry Underhill
Bank of America Corporation	Mr. Roger Callahan
The Boeing Company	Mr. Robert Steele
Computer Sciences Corporation	Mr. Guy Copeland
Lucent Technologies	Mr. Karl Rauscher
Qwest	Mr. Jon Lofstedt
Raytheon Company	Mr. Robert Tolhurst
Rockwell Collins, Inc.	Mr. Ken Kato
Science Applications International Corporation	Mr. Hank Kluepfel
SBC Communications, Inc.	Ms. Rosemary Leffler
United States Telecom Association	Mr. David Kanupke
Verizon Communications	Mr. Jim Bean
WorldCom, Inc.	Ms. Joan Grewe

OTHER PARTICIPANTS

George Washington University	Dr. Jack Oslund
Lucent Technologies	Mr. Greg Shannon
National Security Council	Mr. Marcus Sachs
Qwest	Mr. Tom Snee
SBC Communications, Inc.	Mr. Paul Hart
SBC Communications, Inc.	Ms. Suzy Henderson
WorldCom, Inc.	Ms. Cristin Flynn