THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

VULNERABILITIES TASK FORCE REPORT
INTERNET PEERING SECURITY

March 27, 2003

TABLE OF CONTENTS

Executive Summary

During the evolution of the Internet, it became clear that centralized locations were needed to facilitate the exchange of traffic among the various operators' interconnected networks. This led to the development of the first public peering points, hereafter referred to as network access points (NAP), and later to direct or private peering points between network operators.

If a physical attack were the method of choice, only a well-coordinated attack on numerous NAPs and private peering points distributed across the United States could impair overall Internet operations. Such a substantial attack would be very difficult to plan and implement and require a large amount of resources. According to a previous report by the National Security Telecommunications Advisory Committee (NSTAC), the loss of assets in a potential single point of failure would not cause a nationwide disruption of the critical telecommunications infrastructure.[1]

Specifically, the physical destruction of a NAP, or even several NAPs would not impair Internet functionality because of the number and geographic diversity of NAPs and the multiple means of interconnection available to Internet service providers (ISP). Even if a major peering point were lost, peering of ISPs would continue to occur at other private peering points and other NAPs. Moreover, if multiple NAPs were lost, traffic flow across the Internet could be impacted but not completely disrupted because of the multiple routing options.

The loss of a private peering point would probably affect only Internet traffic flow for customers of those ISPs exchanging traffic at that peering point and only for customers' facilities located within the immediate area of the peering point. An attack on multiple private peering points used by the same ISP could have greater impact on that ISP's service and consequently its customers' operations. However, even in this case, overall Internet functionality would not likely be impaired and, as noted previously, an attack on multiple, dispersed facilities would be difficult to perpetrate.

It is important to note that some smaller ISPs might rely on a single NAP or private peering point to connect to the Internet. These ISPs typically provide services to localized areas, and might support State and local government organizations. In such cases, damage or loss of the ISP's single peering point could affect an organization's mission-critical operations and communications.

Despite inherent network redundancy and resiliency, it is important for the Government to consider possible impacts of the loss of a specific site, such as a NAP or private peering point, on mission-critical national security and emergency preparedness (NS/EP) services. Vulnerabilities could be identified through site-specific mission-critical risk analyses undertaken in coordination with service providers and other business continuity organizations in the private sector.[2] In addition, the Government must consider certain security factors when contracting for network services. For instance, the Government should provide greater consideration to

[1] See the "Single Point of Failure Exercise" section from the NSTAC *Convergence Task Force Report*, June 2001, pp. 13-15.

[2] Ibid.

providers adhering to high levels of security standards and best practices, including those developed by the Network Reliability and Interoperability Council (NRIC).

The VTF is not presenting any new recommendations specific to this report. The NSTAC previously analyzed NS/EP issues related to the concentration of telecommunications assets in the *Vulnerabilities Task Force Report on Telecom Hotels*.[3] The following recommendations from the *Report on Telecom Hotels* are particularly applicable to this report. The Government should undertake these actions to mitigate possible risks to mission-critical NS/EP services:

- "*Undertake site-specific mission-critical risk assessments in coordination with service providers and other business continuity organizations in the private sector to identify possible vulnerabilities that could affect NS/EP communications and operations. If vulnerabilities are identified, adequate funding and resources should be provided to mitigate and remediate vulnerabilities affecting individual mission-critical functions.*

- *Adopt telecommunications services procurement security policy guidelines that provide incentives to companies that follow NRIC best practices, high levels of security standards, and other recognized business contingency principles.*"[4]

[3] See *Vulnerabilities Task Force Report on Telecom Hotels,* April 2003.

[4] See *Vulnerabilities Task Force Report on Telecom Hotels,* April 2003, Section 6.0, "Recommendations to the President."

Vulnerabilities Task Force Report
Internet Peering Security

1.0 Introduction

The Administration has expressed concern that 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 as well as vulnerabilities in common duct runs, rights of way, and 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. Since the networks comprising 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 recommendations.

2.0 Specific Tasking

The Administration has raised concerns about the concentration of critical telecommunications assets in single sites. This report addresses the possible national security and emergency preparedness (NS/EP) implications resulting from physical vulnerabilities of Internet peering point locations. Specifically, the report examines whether the loss of an Internet peering point through direct or indirect physical damage or destruction could have local or national impacts on NS/EP communications and missions. The Task Force did not address potential logical Internet peering point vulnerabilities in this report.

3.0 Brief History of Peering Points

In 1969, the United States Government funded a Department of Defense research project called the Advanced Research Projects Agency NETwork (ARPANET). The network was designed as a distributed rather than centralized network, wherein data flowed in packets and over varying paths before reaching its final destination. As packet network technologies matured, more disparate networks were connected, and the ARPANnet became known as "the Internet." Eventually, the National Science Foundation's data NETwork (NSFNet), a faster and further advanced network, took the ARPANet's place as the Internet backbone. In 1993, the NSF decided to leave the management of the backbone entirely to competing, commercial backbone providers.[6]

As network operators interconnected their networks, it became clear that centralized locations were needed to facilitate the exchange of traffic between multiple networks. This led to the development of the first public peering points, hereafter referred to as network access points (NAP), and later to direct or private peering points between network operators. The NSF played a significant role in the establishment of the first NAPs. In February 1994, the NSF announced that it would establish four NAPs to pave the way for the development of a commercially operated distributed backbone system. The four locations selected were San Francisco, Chicago, New York, and Washington, DC. PacBell, Ameritech, SprintLink, and Metropolitan Fiber Systems (MFS) were selected as the respective NAP operators. These entities helped create the key exchange points of the public Internet in April 1995. MFS's first facility was known as MAE East®, and later MAE West® was added in San Jose. All four of the original NAPs are still in operation.

Peering Terminology

Network Access Point (NAP): A junction point where major Internet service providers interconnect with each other to exchange traffic. This process is known as "public peering."

Private Peering Point: A point where two or a consortium of ISPs agree to exchange traffic over dedicated circuits.

"The rapid growth in Internet traffic soon caused the original NAPs to become congested, which led to delayed and dropped packets. As a result, a number of new NAPs appeared to reduce the amount of traffic flowing through the original NAPs."[7] Today, there are over 40 NAPs dispersed throughout the United States. These NAPs provide key connectivity points to a large number of Internet service providers (ISPs), including the major providers, many of who maintain a presence at multiple locations.

Congestion at NAPs also spawned development of direct or private peering between backbone providers. Through private peering arrangements, two or a consortium of operators agree to exchange traffic via dedicated circuits. Private peering can be more cost-effective for backbone providers. If providers interconnected only at NAPs, traffic originating and terminating in the same city but on different backbones would have to travel to a NAP in a different city or even a different country for exchange; with private peering, in contrast, it can be exchanged within the same city.[8]

[6] Michael Kende, "The Digital Handshake: Connecting Internet Backbones," FCC Office of Plans and Policy, Sept. 2000, p. 5.

[7] Ibid., p. 6.

[8] Ibid.

3.1 Peering Characteristics

Michael Kende's description of peering characteristics from the FCC's "Digital Handshake" white paper in 2000 is a widely supported interpretation. Kende writes:

> Peering has a number of distinctive characteristics. First, peering partners only exchange traffic that originates with the customer of one backbone and terminates with the customer of the other peered backbone. …The second distinctive characteristic of peering is that peering partners exchange traffic on a settlements-free basis. … Additional characteristics of peering relate to the routing of information from one backbone to another. Peering partners generally meet in a number of geographically dispersed locations. ... A final characteristic of peering is that recipients of traffic only promise to undertake “best efforts” when terminating traffic, rather than guarantee any level of performance in delivering packets received from peering partners.[9]

A peering exchange commonly takes place on a settlement-free basis, but may also include payments from one ISP to another if the mutual benefit of the exchange is no longer equitable. In determining whether an ISP-to-ISP relationship is equitable, an ISP may consider whether they exchange comparable levels of traffic and whether the other ISP's networks have a comparable geographic reach.

3.2 Network Peering Today

In 1990, there were fewer than seven ISPs. Today, there are over seven thousand autonomous ISP networks in the domestic United States. The reach of the Internet has crossed borders and continents. In order to achieve almost total connectivity, the top 200 of these networks use a combination of peering and transit. Transit occurs when one backbone provider pays another backbone provider to deliver traffic between its customers and the customers of other backbones.[10] The backbone provider selling the transit services will route traffic from the transit customer to its peering partners.[11] The remaining ISPs buy their transit from upstream, or larger ISPs.

Among the numerous peering networks, a significant portion of the traffic is via legacy private peering. This means that ISPs entered into peering agreements during the initial growth period of the Internet that were designed only to expand a network's reach, and were not necessarily based on a mutual and balanced exchange of traffic, as is largely the case today. In general, while NAPs are widely used around the United States, direct or private peering points remain the most common method of ISP interconnection.

[9] Michael Kende, "The Digital Handshake: Connecting Internet Backbones," FCC Office of Plans and Policy, Sept. 2000.

[10] Ibid., p. 7.

[11] Ibid.

4.0 Implications of the Loss of Peering Points

If a physical attack were the method of choice, only a well-coordinated attack on numerous NAPs and private peering points distributed across the United States could impair overall Internet operations. Such a substantial attack would be very difficult to plan and implement and require a large amount of resources. According to a previous NSTAC report, the loss of assets in a potential single point of failure would not cause a nationwide disruption of the critical telecommunications infrastructure.[12]

Specifically, the physical destruction of a NAP, or even several NAPs, would not impair Internet functionality because of the number and geographic diversity of NAPs and the multiple means of interconnection available to ISPs. Even if a major NAP were lost, peering of ISPs would continue to occur at other private peering points and other NAPs. Moreover, if multiple NAPs were lost, traffic flow across the Internet could be impacted but not completely disrupted because of the multiple routing options.

The loss of a private peering point would probably affect only Internet traffic flow for customers of those ISPs exchanging traffic at that peering point. Only ISPs with limited connectivity will suffer loss of transport, regardless of whether that connectivity is by public peering, private peering or upstream provider links. Some customers of the ISPs may be affected by degraded performance due to the downstream provider architecture of the Internet. An attack on multiple private peering points used by the same ISP could have greater impact on that ISP's service and consequently its customers' operations. Even in this case, overall Internet functionality would not likely be impaired and, as noted previously, an attack on multiple, dispersed facilities would be difficult to execute.

It is important to note that some smaller ISPs might rely on a single NAP or private peering point to connect to the Internet. These ISPs typically provide services to localized areas and might support State and local government organizations. In such cases, damage or loss of the ISP's single peering point could affect an organization's mission-critical operations and communications.

Marketplace demand since the September 11, 2001, terrorist attacks has worked to further increase geographic and contractual diversity. This has resulted in greater network redundancy and more robust physical security practices for peering points. This point is exemplified by MAE East® through its dispersion of infrastructure assets over multiple locations.

4.1 Logical Attacks

Overall Internet functionality is probably much more vulnerable to a logical attack than to a large-scale, coordinated physical attack on NAPs or private peering points. Physical attacks typically result in localized impacts, although it can take a long time to repair the damaged infrastructure. However, a logical attack could have an immediate and widespread impact. For example, if a hacker were to hijack the Border Gateway Protocol or other essential Internet routing protocols, the effects could be witnessed across the entire Internet. However, if

[12] See the "Single Point of Failure Exercise" section from the NSTAC *Convergence Task Force Report*, June 2001, pp. 13-15.

compared with damage due to physical attacks, logical attacks can be quickly remediated once a fix is promulgated.

To date, logical attacks have not specifically focused on peering points, but peering points have been indirectly affected by such attacks. For instance, the October 2002 broadcast storm involved the London Internet Exchange (LINX), which handles approximately 90% of all European peering.[13] In this case, the Internet experienced a slowdown in traffic but its overall operations were not impaired.

5.0 Government's Role in Mitigating Risks

The Government can help to mitigate risks associated with peering points by undertaking site-specific risk analyses and adhering to strict contractual security requirements. Despite inherent network redundancy and resiliency, it is important for the Government to consider possible impacts on mission-critical NS/EP services from the loss of a specific site, such as a NAP or private peering point. Vulnerabilities could be identified through site-specific mission-critical risk analyses undertaken in coordination with service providers and other business continuity organizations in the private sector.[14] Similarly, State and local governments, relying on a single ISP for Internet services, should examine potential impacts on their mission-critical operations should ISP service be disrupted. Appropriate remedial actions should be undertaken if specific vulnerabilities are identified.

The Government must also consider certain security factors when contracting for network services. For instance, the Government should provide greater consideration to providers adhering to high levels of security standards and best practices, including those developed by the Network Reliability and Interoperability Council (NRIC). "The Government must recognize that requirements for premium levels of assurance against damage from any source will result in higher priced services. The Government also needs to address the fact that purchasing services from multiple carriers does not guarantee diversity."[15]

6.0 Findings

- Because of the number and geographic diversity of NAPs and the multiple means of interconnection available to ISPs, it is unlikely that the physical destruction of any single NAP, or even several NAPs, would impair Internet functionality.

- The loss of a private peering point would probably affect Internet traffic flow only for customers of those ISPs exchanging traffic at that peering point and impact only customers' facilities located within the immediate area of the peering point.

- If a physical attack were the method of choice, only a well-coordinated attack on numerous NAPs and private peering points distributed across the United States could impair overall Internet operations. Such a substantial attack would be very difficult to plan and implement and require a large amount of resources.

[13] James Middleton, "Linx Outage Slows UK Web," http://www.vnunet.com/News/1126232, accessed 02/19/03.

[14] NSTAC *Vulnerabilities Task Force Report on Telecom Hotels*, April 2003, p. 4.

[15] Ibid.

- An organization's Internet service is at higher risk of disruption if its ISP routes traffic exclusively through a single NAP or private peering point.

- Overall Internet functionality is probably much more vulnerable to a logical attack than to a large-scale, coordinated physical attack on NAPs or private peering points.

- Physical attacks on the Internet infrastructure would likely result in localized impacts to Internet traffic flow but would take longer to repair than logical attacks.

- Logical attacks could have a widespread impact on Internet operations but can be remediated in less time than a physical attack once a fix is promulgated.

7.0 Conclusions

- The Government can help to mitigate risks associated with peering points by adhering to strict contractual security requirements and undertaking site-specific risk analyses.

- Because the loss of a peering point could affect mission-critical NS/EP services at specific locations, vulnerabilities should be identified through site-specific mission-critical risk analyses undertaken in coordination with service providers and other business continuity organizations in the private sector.

- The Government should provide greater consideration to providers adhering to high levels of security standards and best practices, including those developed by NRIC.

8.0 Recommendations

The VTF is not presenting any new recommendations specific to this report. The NSTAC previously analyzed NS/EP issues related to the concentration of telecommunications assets in the *Vulnerabilities Task Force Report on Telecom Hotels*.[16] The following recommendations from the *Report on Telecom Hotels* are particularly applicable to the Internet peering issues discussed in this report. The Government should undertake these actions to mitigate possible risks to mission-critical NS/EP services:

- "*Undertake site-specific mission-critical risk assessments in coordination with service providers and other business continuity organizations in the private sector to identify possible vulnerabilities that could affect NS/EP communications and operations. If vulnerabilities are identified, adequate funding and resources should be provided to mitigate and remediate vulnerabilities affecting individual mission-critical functions.*

[16] See *Vulnerabilities Task Force Report on Telecom Hotels,* April 2003.

- *Adopt telecommunications services procurement security policy guidelines that provide incentives to companies that follow NRIC best practices, high levels of security standards, and other recognized business contingency principles*." [17]

[17] See *Vulnerabilities Task Force Report on Telecom Hotels,* April 2003, Section 6.0, "Recommendations to the President."

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

Lockheed Martin	Dr. Kathleen Cherry
WorldCom, Inc.	Ms. Cristin Flynn
GWU	Dr. Jack Oslund