THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

VULNERABILITIES TASK FORCE REPORT
CONCENTRATION OF ASSETS:
TELECOM HOTELS

February 12, 2003

Table of Contents

Executive Summary

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. The President's National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee chartered the Vulnerabilities Task Force (VTF) to examine these issues. This report addresses the Administration's concerns about the concentration of telecommunications assets in telecom hotels.

Like any other building, a telecom hotel can be threatened due to its location, by inherently dangerous activities of its neighbors, through the interruption of other underlying infrastructures, or because a neighboring facility might be a terrorist target. The telecommunications industry and Government entities have conducted analyses regarding implications of the loss of telecom hotel assets. The telecommunications industry analysis has shown it is unlikely that the loss of assets in a telecom hotel would cause a nationwide disruption of the critical telecommunications infrastructure.[1] It is also important to note that the existence of telecom hotels has helped to disperse telecommunications assets over multiple locations, thereby reducing service impacts caused by a loss of any one facility. From a Government user perspective, the Joint Program Office for Special Technology Countermeasures (JPO-STC) has performed various analyses evaluating the Government's dependencies on infrastructures, including telecommunications assets/facilities, for specific sites and regions across the United States. Results from the JPO-STC analyses have revealed that loss of service of specific telecommunications nodes could adversely affect certain Government entities and their corresponding missions.

To help mitigate risks, each entity choosing to install equipment in a telecom hotel must determine if the proposed building complies with the carrier's business continuity policies. If all tenants would conduct an analysis based on sound business continuity practices, security concerns could be significantly minimized. Consistent evaluation of facilities can be achieved with a set of industry "best practices." The Federal Communications Commission's Network Reliability and Interoperability Council (NRIC) has completed significant work in this regard, and it continues to be an appropriate forum for developing physical security best practices related to the telecommunications industry. For the purpose of physical diversity for individual services within a specific carrier's network, a user may request and contract for such service from that carrier. In that case, it is that carrier's responsibility to provide such diversity within its network. Should the user choose multiple carriers for the purpose of providing diversity, the assurance of such diversity would be the user's responsibility.

The Government's role in mitigating risks involves carefully considering how it contracts for services and providing greater consideration to providers adhering to high levels of security standards and best practices. It is also important to consider possible impacts of the loss of a telecom hotel or other specific sites on critical-mission national security/emergency preparedness (NS/EP) services. Risk assessment organizations should be provided adequate funding to undertake such critical-mission risk analyses in coordination with service providers

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

and other business continuity organizations in the private sector. If vulnerabilities are identified, it is important that adequate funding and resources be provided to mitigate and remediate vulnerabilities affecting individual critical-mission functions.

Federal, State, and local governments request infrastructure data from the information and communications sector to assist in critical mission continuity assurance efforts. These requests can often be duplicative and require substantial resources from industry to respond. To facilitate a more efficient process for industry to respond to such requests, a central mechanism should be established to coordinate all government infrastructure data requests. The Government can strengthen industry's ability to protect assets from known threats by implementing a cross-functional threat warning system that has well-defined parameters and can be incorporated into industry's and the Government's internal threat warning and response procedures.

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 fund and undertake the following—

- Work with risk assessment organizations and service providers,to conduct site-by-site critical-mission risk analyses to identify vulnerabilities that could affect NS/EP communications and operations; provide adequate funding and resources for departments and agencies to identify, mitigate, and remediate vulnerabilities that could affect individual critical-mission functions.

- Establish a mechanism to coordinate infrastructure data requests from Federal, State, and local governments to the information and communications sector.

- Work with industry to develop and implement a cross-functional threat warning system that both carriers and the Government could adopt as part of their internal threat warning and response procedures. Also, coordinate with industry to develop a process for sanitizing threat information for distribution.

- 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.

Vulnerabilities Task Force Report
Concentration of Assets:
Telecom Hotels

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 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 heightens security concerns. 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. Therefore, security of these networks is of utmost importance.

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

2.0 Specific Tasking

This report addresses the Administration's concerns about the concentration of telecommunications assets in telecom hotels. Because the definitions for telecom hotels and collocation sites are often confused, this report will distinguish the two.

3.0 Definitions

Equipment concentration occurs when two or more telecommunications carriers install equipment in the same building. There are two general categories of sites where equipment concentration occurs:

a. **Collocation Site:** a building or telephone company central office, owned and operated by an incumbent local exchange carrier (ILEC) and also providing interconnection for competitive exchange service providers as set forth in the

regulations established by the Federal Communications Commission (FCC) in accordance with the *Telecommunications Act of 1996*.

b. **Telecom Hotel:** Conditioned floor space owned and operated by a commercial landlord for the purpose of hosting multiple service providers. Tenants may include the incumbent ILEC, competitive local exchange carriers (CLEC), Internet service providers (ISP), competitive access providers (CAP), Web hosting operations, or any other non-telecommunications commercial enterprises in need of floor space to support their electronic equipment.

Both types of locations can provide a variety of telecommunications functions, e.g., interconnection; Internet peering; and operational, administrative, and management interfaces. Typically, telecom hotels are established to enable telecommunications service providers to interconnect with one another to exchange information and traffic.

These locations exist, in part, as a result of the *Telecommunications Act of 1996*, which requires incumbent carriers to provide interconnection for competitive carriers. As interconnection implementation progressed, many incumbent carriers exhausted collocation space available to competitive carriers.

"Virtual" collocation became another arrangement by which the incumbent carrier could extend facilities to a "meet point" in another location. The telecom hotel is one such meet point.

The functions of telecom hotels have expanded beyond a meet point for carriers. Many service providers have installed network elements typically found in a central office environment. The telecom hotel site then becomes the equivalent of several collocated central offices with equipment that serves a variety of functions. The nature of these functions may not be known to anyone other than the companies owning and operating the installed equipment.

4.0 Discussion

Telecom hotel facilities are a result, in part, of the deregulatory and competitive business climate of the telecommunications marketplace wherein commercial enterprises saw a business opportunity to provide such facilities. Likewise, incumbent carriers view the telecom hotel as one of the available means to satisfy their regulatory and business requirements. For these reasons, telecom hotels will likely be a part of the telecommunications infrastructure for the foreseeable future. Therefore, telecom hotels may affect the overall risk environment of the telecommunications infrastructure; and the appropriate roles for industry and Government in evaluating that risk must be explored. Such an evaluation must take into account available relevant Government data (data from the Joint Program Office for Special Technology Countermeasures [JPO-STC]), the advantages of telecom hotels (such as providing more diversity of network facilities and interconnection points), and the associated threats and vulnerabilities. Furthermore, in addition to infrastructure implications, user implications must be considered. The evaluation results will help identify mitigation measures that can be taken, consistent with the threat environment, to diminish any additional risk caused by introducing telecom hotels into the communications infrastructure.

4.1 Threat Environment

Like any other building, a telecom hotel can be threatened due to its location, by inherently dangerous activities of its neighbors, through the interruption of other underlying infrastructures, or because a neighboring facility might be a terrorist target. To date, there is little evidence that the telecommunications infrastructure has been the direct target of terrorism, but collateral damage has occurred as a result of attacks directed elsewhere.

4.2 Potential Implications of the Loss of a Telecom Hotel

It is important to differentiate how the Administration, telecom industry, and users look at the impact of the loss of assets in a telecom hotel. The Administration is concerned with a single point of failure impacting the overall infrastructure. The telecom industry is concerned about the overall impact of a loss of any asset on its infrastructure and customer services. Users are concerned about the impact on specific mission-supporting services.

Every telecom hotel is likely to have a variety of tenants who have installed diverse and complex equipment. The equipment could support local, regional, or nationwide services, or any combination thereof. The functionality of the tenants' equipment installed in the facility will determine the extent of loss. Therefore, assessing the potential impact of the loss of each individual telecom hotel facility is difficult.

The telecommunications industry and Government entities have conducted analyses regarding implications of the loss of telecom hotel assets. The telecommunications industry has shown it is unlikely that the loss of assets in a telecom hotel would cause a nationwide disruption of the critical telecommunications infrastructure.[2] It is also important to note that the existence of telecom hotels has helped to disperse telecommunications assets over multiple locations, thereby reducing service impacts caused by a loss of any one facility.

From a Government user perspective, the JPO-STC has performed various analyses evaluating the Government's dependencies on infrastructures, including telecommunications assets/facilities, for specific sites and regions across the United States. Results from the JPO-STC analyses have revealed that loss of service of specific telecommunications nodes could adversely affect certain Government entities and their corresponding missions. Specific assets studied include both local and regional telecommunications nodes as well as collocation sites. Up until this VTF effort, no distinction was made between telecommunication hotels and collocation sites; therefore, the analysis results may include some telecom hotels.

Although no analyses performed to date have shown that the entire communications architecture would be adversely affected through the loss of a single telecom facility, according to JPO-STC, loss of specific telecommunications nodes can cause disruption to national missions under certain circumstances. As a result of these analyses, the JPO-STC not only has shown the dependencies of Department of Defense (DoD) missions on telecommunications, but

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

also reports that there are further and more far-reaching implications to other national infrastructure sectors.

4.3 Industry Responsibilities for Mitigating Risks

Many carriers place a high priority on service reliability by building networks with alternative routes, backup facilities, and other service assurance capabilities. Such carriers will also employ business contingency planning procedures entailing the identification of critical functions, the supporting assets, potential threats, options for mitigating threats, costs incurred from damage to assets, and costs incurred to implement mitigation strategies. Each carrier choosing to install equipment in a telecom hotel must determine if the proposed building complies with the carrier's business continuity policies. If all tenants would conduct an analysis based on sound business continuity practices, security concerns could be significantly minimized.

Consistent evaluation of facilities can be achieved with a set of industry "best practices". The Federal Communications Commission's Network Reliability and Interoperability Council (NRIC) has completed significant work in this regard, and it continues to be an appropriate forum for developing physical security best practices related to the telecommunications industry.[3]

For the purpose of physical diversity for individual services within a specific carrier's network, a user may request and contract for such service from that carrier. In that case, it is that carrier's responsibility to provide such diversity within its network. Should the user choose multiple carriers for the purpose of providing diversity, the assurance of such diversity would be the user's responsibility.

4.4 Government Responsibilities for Mitigating Risks

It is the Government's responsibility to carefully consider how it contracts for services and to provide greater consideration to providers adhering to high levels of security standards and best practices. 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.

It is also important to consider possible impacts of the loss of a telecom hotel or other specific sites on critical-mission national security and emergency preparedness (NS/EP) services. Risk assessment organizations should be provided adequate funding to undertake such critical-mission risk analyses in coordination with service providers and other business continuity organizations in the private sector. If vulnerabilities are found, it is important that adequate funding and resources be provided to mitigate and remediate vulnerabilities affecting individual critical-mission functions.

[3] Please see the various NRIC *Reports to the Nation* and *Focus Group Reports* available on the NRIC Web site at http://www.nric.org/pubs/index.html. NRIC VI Focus Group 1, Subcommittee 1.A, is currently investigating physical security best practices. Information on the Focus Group's progress will be posted on the NRIC Web site.

The Federal, State, and local governments frequently request infrastructure data from the information and communications sector to assist in critical-mission continuity assurance efforts. These requests can often be duplicative, and require substantial resources from industry to respond. To facilitate a more efficient process for industry to respond to such requests, a central mechanism should be established to coordinate all government infrastructure data requests.

Furthermore, the responsibility of the Government in protecting domestic facilities from aggression and acts of violence must be clearly established. The Government can strengthen industry's ability to protect assets from known threats by implementing a cross-functional threat warning system that has well-defined parameters and can be incorporated into industry's and Government's internal threat warning and response procedures. Explicit threats need to be communicated to the telecommunications industry in a timely manner so specific countermeasures can be implemented. The Government recognizes the importance of this process in its *National Strategy for Homeland Security*, stating that it "…can create venues to share information on infrastructure vulnerabilities and best practice solutions, or create a more effective means of providing specific and useful threat information to non-federal entities in a timely fashion."[4] To facilitate efficient communication of threats, the Government should coordinate with industry to develop a process for sanitizing threat information for distribution.

5.0 Conclusions

- For the foreseeable future, telecom hotels will be a part of the telecom infrastructure.
- Although the service impact of loss of any one telecom hotel is difficult to assess because each site is likely to have a variety of tenants with diverse and complex equipment, it is unlikely that the loss of telecom hotel assets would cause a nationwide disruption of the Nation's critical telecommunications infrastructure.
- The JPO-STC has stated that the loss of specific telecommunications nodes could affect certain Government entities and their corresponding missions.
- The concentration of telecommunications assets within telecom hotels may present a vulnerability; however, their existence has dispersed telecom assets, thereby reducing the service impact caused by a loss.
- NRIC is an appropriate forum to develop physical security best practices related to the telecommunications infrastructure.
- To achieve physical diversity for individual services within a specific carrier's network, a user may request and contract for such service from that carrier. In these cases, it is that carrier's responsibility to provide such diversity within its network.

[4] *The National Strategy for Homeland Security*, Office of Homeland Security, July 2002, p. 30.

- The Government must recognize that purchasing services from multiple carriers does not guarantee physical diversity. If a user chooses multiple carriers for providing diversity, the assurance of such diversity would be the user's responsibility.

- Site-by-site critical-mission risk analyses should be undertaken by organizations to identify possible vulnerabilities that could affect NS/EP communications and operations. Appropriate funding and resources should be allocated to support such efforts.

- A central mechanism should be established to coordinate infrastructure data requests from Federal, State, and local governments to the information and communications sector.

- The Government should work with industry to develop and implement a cross-functional threat warning system that both parties could adopt as part of their internal threat warning and response procedures. A process to sanitize Government threat information for distribution should also be developed in cooperation with industry.

- The Government should 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.

6.0 NSTAC Recommendations to the President

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 fund and undertake the following—

- Work with risk assessment organizations and service providers to conduct site-by-site critical-mission risk analyses to identify vulnerabilities that could affect NS/EP communications and operations; provide adequate funding and resources for departments and agencies to identify, mitigate, and remediate vulnerabilities that could affect individual critical-mission functions.

- Establish a mechanism to coordinate infrastructure data requests from Federal, State, and local governments to the information and communications sector.

- Work with industry to develop and implement a cross-functional threat warning system that both carriers and the Government could adopt as part of their internal threat warning and response procedures. Also, coordinate with industry to develop a process for sanitizing threat information for distribution.

- 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.

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
NSWCDD-J22	Mr. Michael Shanahan
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