THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

FINANCIAL SERVICES TASK FORCE REPORT

April 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Security Telecommunications Advisory Committee (NSTAC) Financial Services Task Force (FSTF) recognizes the criticality of the payment, clearing, and settlement processes of the financial services sector to our national economy. Additionally, recent government policies and actions have concluded that the telecommunications infrastructure underlying the critical FS clearing, payment and settlement processes is a matter of National Security. The FSTF also acknowledges the sector's dependence on resilient and robust telecommunications services in support of these processes. The concept of resiliency and its components of diversity, redundancy, and recoverability are critical to understanding some of the national security and emergency preparedness (NS/EP) issues challenging the financial services and telecommunications industries today.

The financial services sector strongly emphasizes the need to maintain diversity as one of the components of resiliency. The primary challenges the financial services sector faces with respect to diversity are as follows:

- Failure of critical services due to the loss of diversity.
- The ability to ensure that diversity is predictable and continually maintained.
- The potential for lack of clear understanding of terms and conditions in telecommunications contracts or tariffs (and the potential for resulting confusion when financial services institutions establish business continuity plans).

Without a real-time process to guarantee that a circuit's path or route is static and stable, an NS/EP customer cannot be assured at all times that the diversity component of the resiliency plan retains its designed characteristics. The FSTF recognized that the telecommunications infrastructure was designed and engineered based on a business model directed at the general public. When necessary, networks have been modified or developed to meet specific needs at the customer level, except where limited by the available technology or a customers' willingness to pay for unique requirements. Continued advances in technology and network resiliency baselines within the telecommunications industry will benefit the financial services sector and other critical infrastructures; accordingly, the policies and recommendations presented in this report are bound by current technology capabilities.

Telecommunications companies recognize the importance of innovation and the need to develop next generation products and services that can be adopted by customers with NS/EP needs. However, many telecommunications networks would need considerable upgrades to support NS/EP functionality within their larger network frameworks. At the same time, the demand for such services is insufficient to allow the marketplace to support the specialized requirements of NS/EP functions on a wide-scale basis. Resiliency solutions, including diversity, will continue to evolve as the telecommunications sector continues research and development efforts, and as the Federal Government and critical infrastructure customers continue to encourage and participate in those efforts. All interested parties should support research and development

activities for improving managed network solutions and alternative technologies as a potential means for achieving high resiliency for the FS customer base.

Targeted capital incentives should also be considered as a tool to encourage critical infrastructure owners, including the financial services sector, to make the necessary investments to mitigate telecommunications resiliency risks to their business operations. Historically, capital incentives serve as a mechanism of national policy promoting the public good. Appropriately structured capital recovery incentives for critical business operations could be used to accelerate immediate investments to mitigate vulnerabilities to critical NS/EP operations.

It is important to note that when different business continuity strategies cannot fully guarantee operational sustainability, specifically engineered and managed efforts may be required. The degree of assurance that a business operation deems adequate to achieve a high level of resiliency will dictate the decisions and the appropriate approach to be pursued. To that end, cross-sector assessments, or customer-provider assessments, will remain a useful tool to facilitate better understanding of the need for resiliency.

During the NSTAC's cross-sector effort, FSTF members acknowledged the importance of promoting mutual understanding among the financial and telecommunications sectors to effectively address NS/EP-related issues. Both sectors should continue in their efforts to engage members of their communities, as well as the public sector, in a constructive dialogue to foster mutual understanding of their operations and unique needs. Furthermore, the framework that the FSTF developed to analyze the dependencies of the financial services sector on the telecommunications industry can be adapted to conduct risk assessments of other critical infrastructures.

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—

- Support the Alliance for Telecommunications Industry Solutions' National Diversity Assurance Initiative and develop a process to:
  - Examine diversity assurance capabilities, requirements, and best practices for critical NS/EP customers and, where needed,
  - Promote research and development to increase resiliency, circuit diversity, and alternative transport mechanisms.

- Support financial services sector initiatives examining:
  - The development of a feasible "circuit by circuit" solution to ensure telecommunications services resiliency, and

  - The benefits and complexities of aggregating sector-wide NS/EP telecommunications requirements into a common framework to protect national economic security.

- Coordinate and support relevant cross-sector activities (e.g., standards development, research and development, pilot initiatives, and exercises) in accordance with guidance provided in Homeland Security Presidential Directive 7.

- Provide statutory protection to remove liability and antitrust barriers to collaborative efforts when needed in the interest of national security.

- Continue to promote the Telecommunications Service Priority program as a component of the business resumption plans of financial services institutions.

- Promote research and development efforts to increase the resiliency and the reliability of alternative transport technologies.

- Examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions.

1.0 INTRODUCTION

The terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the United States' financial system.[1] In the days following the attacks, institutions in the affected areas implemented their business continuity plans (BCP), which proved vital to the rapid restoration and recovery of essential services in the New York City area. In relation, President George W. Bush emphasized that the prompt restoration of Wall Street's capabilities was critical to the economic welfare of the Nation; and, in doing so, he linked economic stability to national security. In addition to other financial services restoration efforts already under way, the telecommunications sector quickly responded to restore the capabilities that support financial markets, resulting in the reopening of the national financial markets within 5 days after the attacks.

In November 2002, the Federal Reserve Board (FRB) and BITS—a nonprofit industry consortium of the 100 largest financial institutions in the United States that focuses on issues related to security, crisis management, e-commerce, payments, and emerging technologies—briefed the Industry Executive Subcommittee (IES) of the President's National Security Telecommunications Advisory Committee (NSTAC) about the significant dependence of the financial services sector on the telecommunications infrastructure to support core payment, clearance, and settlement processes of financial institutions. As such, disruption of telecommunications services could hamper critical financial services processes, potentially affecting the national economy. To minimize operational risks and ensure the timely delivery of critical financial services, the FRB recommended that the NSTAC analyze telecommunications infrastructure issues pertaining to network redundancy and diversity. The NSTAC established the Financial Services Task Force (FSTF) to conduct the analysis. The FRB and BITS suggested that in performing this analysis, the FSTF solicit input from Federal, State, and local governments, as well as other critical infrastructure entities and build on the knowledge accrued over many years of studying network security and infrastructure vulnerabilities.

This report provides the findings and conclusions of the NSTAC analysis and highlights where the FSTF was unable to reach a consensus on key issues. It should be noted that the task force focused its analysis on the physical aspect of resiliency and did not address its cyber component. The recommendations provided herein are intended to address the numerous challenges facing the Nation's financial services providers and telecommunications industry in the current threat environment.

[1] James J. MacAndrews and Simmon M. Potter, "Liquidity Effects of the Events of September 11th, 2001", Federal Reserve Bank of New York Economic Policy Review, November 2002.

2.0 SPECIFIC TASKING

The NSTAC IES chartered the FSTF to undertake the following: (1) Define areas of critical concern to the financial services sector (e.g., resiliency, diversity, redundancy recoverability, and interdependency issues as well as the need for continual assessment of the status of the foregoing); (2) Determine whether or how the telecommunications industry meets or addresses these concerns; (3) Identify specific policy recommendations to address any deficiencies, including developing mechanisms to (a) enhance information sharing between the Government and among the financial services and telecommunications sectors to reduce operational risk, (b) facilitate national security risk assessments for geographic areas critical to the financial services sector to identify vulnerability mitigation options (based on susceptibility to a defined set of threats), and (c) identify industry practices that could impede addressing such concerns; (4) Identify areas of Federal, State, or local public policy or laws that might impede the industry from addressing identified concerns; (5) Identify issue commonalities with other sectors, and the applicability of findings/recommendations to those sectors.

3.0 ANALYTICAL FRAMEWORK

To accomplish its tasking, including analyzing the dependencies of the financial services sector on the telecommunications industry, the FSTF developed an analytical framework based on a risk assessment and risk management methodology (represented in Figure 1, page 5). The framework can be adapted to conduct risk assessments of other critical infrastructures. As will be set forth more fully below, the concept of resiliency and its components of diversity, redundancy, and recoverability are integral parts of the FSTF analytical framework and are critical to understanding some of the national security and emergency preparedness (NS/EP) issues challenging the financial services and telecommunications industries today.

The FSTF examined resiliency in the telecommunications sector from the viewpoint that diversity, redundancy, and recoverability capabilities are indispensable to achieve resiliency. The FSTF acknowledged that resiliency, diversity, redundancy, and recoverability can be defined in several ways—for example, the FRB states in its *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* that "resilience of the U.S. financial system in the event of a 'wide scale disruption' rests on the rapid 'resumption' and 'recovery' of the 'clearing and settlement activities' that support 'critical financial markets.'"[2] For the purpose of this report, these terms were interpreted as follows:

Diversity
The financial services sector views diversity from a functional perspective: primary and backup telecommunications capabilities should not share common points of failure. More important, the financial services sector believes that diversity is a proactive component of resiliency and is required to ensure predictable recovery of financial services functions if primary

[2] The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, September 5, 2002, pg. 6.

telecommunications services are disrupted. At a technical level, however, the telecommunications industry recognizes that a single engineering definition of network diversity does not exist. Service providers define diversity solutions in contracts with each customer according to the customer's unique requirements. Diversity solutions can range from simple, relatively inexpensive measures, like dual dial tone sources, to comparatively costly network architectural solutions. Diversity management can ensure that redundant assets do not share common points of potential failure, thus protecting a network from catastrophic failure.

Diversity encompasses a multitude of factors, including technology, geography, facilities, and business continuity planning. Moreover, diversity can be achieved through a multitude of means:

- Media diversity provides alternative communications transport mechanisms (e.g., wireless, satellite);
- Entry diversity offers more than one cable entrance into a building;
- Pair and cable diversity provides a local loop connection through multiple, non-adjacent pairs in more than one cable;
- Path or route diversity provides end-to-end, physically or logically separate routes for a circuit;
- Central office diversity provides local loops that terminate in more than one central office;
- Site diversity provides alternative or backup locations;
- Service provider diversity involves services obtained from more than one telecommunications service provider;
- Supplier diversity provides more than one vendor for the underlying hardware and software utilized in the infrastructure.

The telecommunications infrastructure meets the needs of the general public because it evolved in response to market forces and regulatory requirements. However, service providers typically negotiate contract-specific diversity services to meet customers' NS/EP telecommunications requirements[3]. For additional information on terms associated with diversity, see Appendix B. For additional information on NS/EP telecommunications requirements, see Appendix C.

Redundancy

Redundancy provides alternative methods of telecommunications capabilities to sustain business operations and eliminate any single point of failure that could disrupt primary services. For telecommunications supporting critical financial services functions, redundancy includes, but is not limited to, dual sites where the function is performed, dual telecommunications offices serving each site, and dual routes between each site and the serving central offices. Other

[3] "National security and emergency preparedness telecommunications services" are the telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that does or could cause injury or harm to the population; cause damage or loss of property; or degrade or threaten the NS/EP posture of the United States. NCS, *Telecommunications Service Priority System for NS/EP Service User Manual* (NCS Manual 3-1-1).Washington, DC: NCS, March 1998.

redundancy measures include, but are not limited to, on-site and off-site backup equipment, multiple telecommunications circuits, or alternative communications technologies.

Recoverability

Recoverability is the reactive component of resiliency. Recoverability must be considered from the perspective of the critical financial services business function and the underlying telecommunications infrastructure. The procedures for recovery of critical functions are typically documented in business continuity plans, which must be regularly exercised.[4] Recovery capabilities ensure that methods are in place to quickly restore business operations if a partial or full interruption or failure occurs. Response time and recovery activities depend on the scale and scope of an incident, access control to damaged assets and customer premises, prevailing weather conditions, status of the electric power infrastructure, security and safety considerations, and regulatory demands.

From the perspective of the telecommunications service provider, recoverability of network services may include automatic and manual measures to recover (or restore) interrupted services. These measures could include network management controls, Synchronous Optical Network (SONET) technology, other automatic service recovery technologies, and manual transfer to alternate facility routes.

Resiliency

Resiliency can be enhanced by implementing telecommunications services capabilities that can withstand a shock or hazard with minimal interruption or failure. A resilient financial services operation and its critical telecommunications services must be able to endure hazards of nature, such as earthquakes, tornados, floods, and other natural disasters, as well as manmade hazards, such as bombings, cyber crimes, malicious destruction, and terrorist attacks. Critical infrastructures in the current threat environment face additional challenges because they must be able to withstand the effects of random events and potentially hazardous and sophisticated scenarios, which are often specifically designed to inflict long-term extended damage on critical infrastructures and economic stability.

The FSTF examined telecommunications services resiliency from the viewpoint that diversity, redundancy, and recoverability are necessary to achieve resiliency. Recovery and redundancy together cannot provide a sufficient level of resiliency if these measures can be disrupted by a single event; therefore, diversity is crucial. Industry best practices for diversity include separation of multiple circuit paths, decentralization of office facility connections, and alternative transmission technologies.[5] These three telecommunications resiliency measures are complementary and may coexist to provide a predictable level of business continuity for critical NS/EP services. The financial services sector relies on the telecommunications sector to ensure

---

4 "*Interagency Paper on Sound Practices*," pg. 8-17.

5 Network Reliability and Interoperability Council VI, *Homeland Security-Physical Security Prevention and Restoration Report*, March 14, 2003. http://www.nric.org/fg/charter_vi/fg1/RECOM_FG_1A_Homeland_Security_Physical_Security_Mar14.doc; Network Reliability and Interoperability Council VI, *Homeland Defense-Cyber Security Best Practices*, March 14, 2003. http://www.nric.org/fg/charter_vi/fg1/FG1B_front_matter_and_proposals_FINAL_3-13-03.doc

that these measures are applied end-to-end on critical connections when so specified by the customer. Even if it is possible to verify through testing that some recovery and redundancy measures are in place, financial services firms need to rely on other methods of due diligence to verify the engineering and recoverability of telecommunications services.

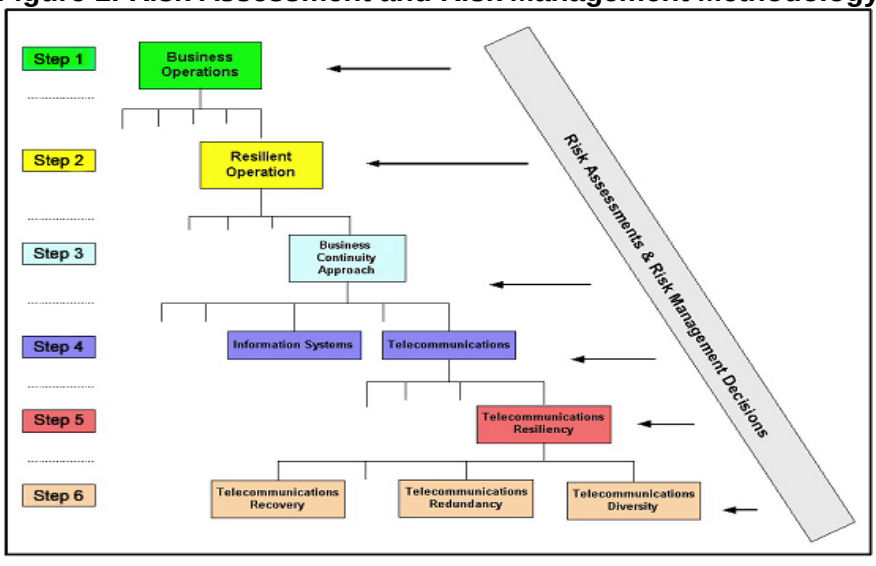
When performing resiliency assessments, it is important to consider a number of factors:

- Essential business functions
- Time sensitivity of each essential function
- Threats to the continuity of the functions and the services upon which they depend
- Threat mitigation options
- Cost/benefit analysis
- Mitigation strategy
- Implementation
- Testing
- Information sharing on all of the above.

3.1 Risk Assessment and Risk Management Methodology

Risk assessment and risk management methodologies are core competencies practiced by the critical infrastructure institutions as a means of establishing and maintaining sound business operations. The FSTF employed a 6-step risk assessment and management methodology (Figure 1) to structure its analysis of critical issues to the financial services sector (e.g., redundancy, resiliency, diversity).

Figure 1: Risk Assessment and Risk Management Methodology



3.1.1 Critical Business Operations

As a general sound business practice, institutions perform business impact analyses to document the critical business operations that must be resilient (step 1 of Figure 1). With regard to the financial services sector, critical business operations are defined, in part, through regulatory guidance.

The Interagency Paper, which was jointly issued by the Office of the Comptroller of the Currency (OCC), the FRB, and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most critical business operations at risk for financial markets.[6] Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.[7]

Moreover, in December 2002, the FRB revised its policy and procedures for NS/EP telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's NS/EP mission to maintain national liquidity.[8] The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption of "a few minutes to one day" occurred. These functions, which are listed below, require same-day recovery and are critical to the operation and liquidity of banks and the stability of financial markets:

- Large-value interbank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Automated clearinghouse (ACH) operators
- Key clearing and settlement utilities
- U.S. Department of Treasury automated auction and processing system
- Large-dollar participants of these systems and utilities.

The SEC and the Commodities Futures Trading Commission have also developed policies and procedures for applying NS/EP telecommunications programs to key market utilities and market participants. Collectively, these key utilities provide support for the provision of a wide range of financial services to businesses and consumers in the U. S. and are critical for national economic security. Together with the few key large-dollar participants, these systems maintain liquidity and support the implementation of monetary and fiscal policy. As an example, based on 2002

---

6 "*Interagency Paper on Sound Practices*," pg. 5

7 Systemic risk includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

8 *Federal Register*, vol. 67, no. 236, Monday, December 9, 2002. Notice, "Federal Reserve Board Sponsorship for Priority Telecommunication Services of Organizations That Are Important to National Security/ Emergency Preparedness," http://www.federalreserve.gov/boarddocs/press/other/2002/20021203/attachment.pdf.

statistics, the Federal Reserve's Fedwire and CHIPS payment system transferred the United States Gross Domestic Product of approximately $10.5 trillion every 4 days.[9] Clearly, these networks and systems are critical to the Nation's economy and require NS/EP-level treatment.

3.1.2 Resilient Operations

Resilient operations (step 2 of Figure 1) represent those critical business operations that must continue to function in the event of local or widespread disruptions. The scope of resiliency includes recovery and backup measures for primary operations, facilities, infrastructure systems, supplier services, interdependent business partners, and key staff. Best practices also include verification of resiliency levels for utilities, services, and business partner systems necessary for business continuity. Maintaining redundancy of key components at a primary site will insulate critical business operations from equipment failure or other disruptions and will help achieve resiliency. Maintaining recovery capabilities at a secondary site will enable the resumption of business operations if disruption occurs and will help reinforce resiliency levels. The recovery practices identified in the Interagency Paper cited in the preceding section emphasize that geographic diversity for primary and backup sites is paramount, and backup sites should not rely on the same infrastructure components (e.g., electric power, telecommunications, transportation, and water supply) used by the primary sites. These practices are core components for ensuring resilient operations.

3.1.3 Business Continuity Approach

Strong business continuity plans (step 3 of Figure 1) are important to owners and operators of critical infrastructures and to their customers, shareholders, and insurers. Understanding the hierarchical operational needs of an institution provides the necessary framework to make difficult business decisions about priorities and capital allocation. Furthermore, in the current threat environment, an institution can no longer exclusively examine its key operations and accurately determine acceptable levels of risk. Providers of critical infrastructure services must also consider that disruption of their key operations could affect the Nation's security, emergency preparedness, and economic stability.

Ensuring uninterrupted telecommunications services is a critical component of the business continuity plan of a financial institution. Moreover, ensuring continuity of NS/EP services through resilient, reliable, and secure telecommunications capabilities is paramount for financial institutions to ensure national economic security. However, the demands of regulators, the needs of businesses, and the expectations of the general public in times of crisis must all be balanced, presenting significant challenges for the financial services sector.

[9] Bank for International Settlement (BIS), Committee on Payment and Settlement Systems of the Group of Ten Countries, "Statistics on Payment and Settlement Systems in Selected Countries," (Figures for 2002), http://www.bis.org/cpss/cpsspubl.htm.

3.1.4 Telecommunications and Business Continuity

Identifying the logical and physical telecommunications assets of an institution and the locations of these assets (step 4 of Figure 1) is imperative to a business continuity strategy and risk assessment plan because telecommunications capabilities are necessary for operations. Fully understanding business operations, all of their potential points of failure, and the fault tolerance for each point of failure are imperative when determining the necessary level of telecommunications resiliency.

The events of September 11, 2001, taught both telecommunications and financial services institutions new lessons about critical infrastructure interdependencies. Cross-sector partnerships are necessary to understand the intricacies of infrastructure interdependencies and their potential consequences. Financial services institutions and telecommunications companies must partner to understand how telecommunications services support NS/EP financial functions. With that goal, the financial services industry and the telecommunications industry have engaged in a constructive dialogue on how best to mitigate risks. Dialogues facilitated by the NSTAC, the NCS, the telecommunications sector, BITS, and other financial services-related bodies have increased the focus and attention on the interrelationships between telecommunications and financial services critical functions. These discussions will lead to greater understanding, cooperation, and innovation, which will, in turn, achieve the ultimate goal of this task force: greater resiliency of critical financial services circuits.

3.1.5 Telecommunications Resiliency

When critical telecommunications assets have been identified, an institution must define the level of telecommunications resiliency (step 5 of Figure 1) necessary to support critical business operations and assets. The FRB estimates 6,000 "dedicated" circuits qualify for Telecommunications Service Priority (TSP) in support of financial services NS/EP functions in the United States today.[10] This relatively small number of NS/EP circuits makes resiliency more of a challenge. Those circuits are distributed across many networks, technological platforms, companies, and locations across the Nation; but they are often concentrated in easily identifiable metropolitan areas. Although the recent focus on these circuits is changing the perceptions of how companies contract for telecommunications services, in some instances, further advancements and enhancements are necessary to bring about an even higher level of certified resiliency. The following sections outline specific measures toward achieving a requisite level of telecommunications resiliency within the financial services industry.

4.0 ACHIEVING THE APPROPRIATE LEVEL OF RESILIENCY

The financial services sector recognizes the importance of resiliency and strongly emphasizes the need to maintain diversity as the most important aspect of resiliency. Although the financial services sector manages the resiliency of critical financial processes, it must depend on the

[10] Letter from the FRB Director Steve Malphrus to Mr. William Sweeney, Chair of the FSTF, January 21, 2004.

telecommunications sector to engineer and maintain the resiliency of the underlying telecommunications infrastructure. The primary challenges the financial services sector faces with respect to diversity are as follows:

- Failure of critical services due to the loss of diversity.
- The ability to ensure that diversity is predictable and continually maintained.
- The potential for lack of clear understanding of terms and conditions in telecommunications contracts or tariffs (and the potential for resulting confusion when financial services institutions establish business continuity plans).

A 2003 Government Accounting Office (GAO) report noted:

> *Ensuring that service providers actually maintain physically redundant and diverse telecommunications services has been a long-standing concern within the financial industry. For example, in December 1997, the President's National Security Telecommunications Advisory Committee reported, "despite assurances about diverse networks from the service provider, a consistent concern among the financial services industry was the trustworthiness of their telecommunications diversity arrangements."* [11]

4.1 Achieving Resiliency Today

Within the financial services sector, key financial markets are concentrated in the New York City, Boston, Chicago, and San Francisco metropolitan areas. Areas of physical concentration can introduce significant challenges for achieving telecommunications resiliency because multiple key utilities or large-dollar organizations share telecommunications facilities and circuit paths.[12] Consequently, telecommunications resiliency must often be approached as a shared solution that can benefit utilities and participants within an area of concentration.

The telecommunications industry and the financial services industry agree that the process of ensuring resiliency can be clarified. Existing resiliency services include network redundancy, and diversity features tailored to a customer's specific requirements, usually through a process of intense customer and provider negotiations. Telecommunications service providers and financial institutions agree that improvements can and should be made to make the process of achieving higher resiliency and diversity easier, more transparent, and less costly. Financial services institutions, which have specific telecommunications resiliency requirements, must spend significant time and resources collaborating with service providers to design services to meet those requirements. It may be that one or more resiliency components are needed to achieve the specific requirements. Innovation, collaboration, and partnership will make it easier for financial services institutions to meet the restoration and recovery timelines established by financial regulators. The objective is to meet the resiliency requirements, not necessarily to require that

[11] United States General Accounting Office (GAO) Report to the Committee on Financial Services, House of Representatives, GAO-03-414, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, February 2003. The GAO is currently undertaking a follow-up review of steps taken by the financial services industry to improve its operational resiliency. http://www.gao.gov/new.items/d03414.pdf

[12] *Interagency Paper on Sound Practices*, pg. 3.

financial services applications employ all resiliency components in their designs. The financial services sector seeks to simplify the negotiation and solution design process, and the telecommunications sector agrees the process should be simplified for NS/EP purposes. Many challenges that are related to this negotiation process are set forth below.

4.1.1 The "Loss of Diversity" Challenge

Financial services participants in the task force emphasized a compelling need for "true diversity assurance" for customers' critical circuits. Diversity can be defined in many ways, and the level of diversity required by a customer is a contractual issue typically negotiated between parties. Generally, diversity is the ability for circuits to traverse separately routed physical paths, such that if one route experiences an interruption, another circuit is not impacted. The financial services sector is concerned about diversity measures in support of resiliency capabilities for both telecommunications circuits and fiber optic cable routes, such as SONET ring implementations. Geographic diversity is also an important consideration for the financial services industry. As the FRB, SEC, and OCC recognized, "Firms that establish geographically dispersed facilities can achieve additional diversity in their telecommunications and other infrastructure services, which will provide additional resilience in ensuring recovery of critical operations."[13] While understanding the many facets of diversity is important, the process to achieve and maintain absolute diversity requires deeper analysis.

The events of September 11, 2001, heightened the focus on business continuity for many critical customers and focused dialogue on the needs of the NS/EP customer, rather than the traditional home, small business, or commercial customer. Telecommunications and financial services entities must collaborate to meet NS/EP demands. Telecommunications companies recognize the importance of innovation and the need to develop next generation products and services that can be adopted by customers with NS/EP needs. Diversity solutions will continue to evolve if the telecommunications sector continues research and development efforts, and if the Federal Government and critical infrastructure customers continue to encourage and participate in those efforts.

In cooperation with the telecommunications industry, the financial services sector has adopted a number of best practices to ensure resiliency in its communications networks. In addition, financial services organizations have been early adopters and strong proponents of new services and technologies that further improve telecommunications resiliency. As the 2003 GAO Report to the Committee on Financial Services indicated, most of the financial industry's key data processing centers were operational and prepared to meet the processing needs of the financial industry.[14] However, insufficient telecommunications diversity, which augments redundancy

[13] Ibid., pg. 9.

[14] GAO-03-414, *Potential Terrorist Attacks: Additional Actions Needed*. The GAO is currently undertaking a follow-up review of steps taken by the financial services industry to improve its operational resiliency http://www.gao.gov/new.items/d03414.pdf

and recovery measures, did impact financial firms; and that topic must be considered when developing telecommunications resiliency plans.[15]

4.1.2 Ensuring "Static Routes" or Service Availability

In today's marketplace, customers seeking a "guarantee" of diversity typically contract for a specific level of service or a particular type of service. A customer can purchase a dedicated, point-to-point circuit, which will have a static route and is easily identifiable for a customer's business risk analysis purpose. While such routes are identifiable, certain, and static, the circuits lose the benefit of the dynamic nature of today's networks and many of the self-healing aspects that are built into telecommunications networks.

Without a real-time process to guarantee that a circuit's path or route is static and stable, an NS/EP customer cannot be assured at all times that its diversity plan is being met. However, this discussion about a "real-time" certification process for static routes is new and novel to the telecommunications industry. For example, the Federal Aviation Administration (FAA) Leased Interfacility National Air Space Communications System (LINCS) network (discussed in Section 5.2) requires a certification on route diversity only once a month. The FAA business case appears to accept a monthly certification as the appropriate frequency of assurance of resiliency. Monthly certification does not imply 30/31 days of uncontaminated diversity. With the monthly process, however, the customer is being assured that no grooming error is sustained for longer than a month before the service provider takes corrective action.

Some FSTF participants have argued that "manual certification" is not adequate because a manual process is labor intensive, time consuming, and not scalable as a general solution. In the view of the task force, real-time processes and certifications are required to ensure resiliency and diversity of time-critical circuits, such as those supporting financial sector national security requirements. The telecommunications sector's initial response to this statement was to point out that financial services customers are not currently requesting this type of manual certification process in any commercial context, nor has this level of service been requested for any other circuit or service.

Before September 11, 2001, the financial services sector assumed that in requesting diversely engineered services, the telecommunications industry had systems to provide assurance that this property was retained and verifiable. In the aftermath of those attacks, and in light of the current threats faced by our Nation, the financial services sector is responding to its experiences and analyses that have emphasized the need for verifiable assurances for NS/EP services. Achieving an understanding of the telecommunications industry's diversity capabilities is a key component of this response.

15 The Network Reliability and Interoperability Council (NRIC) identifies diversity as a best practice, most recently as part of NRIC VI, Focus Group 1A Physical Security: http://www.nric.org/fg/index.html

The telecommunications sector, through the Alliance for Telecommunications Industry Solutions (ATIS), is sponsoring a National Diversity Assurance Initiative to examine the processes and procedures that would be required to provide a level of diversity assurance certification of routing in a more timely manner. Diversity may be more achievable for customers who keep their circuits on the same network, but challenges ensue when a customer uses multiple service providers (or when a service provider uses circuits leased from another service provider) to provide an end-to-end circuit. This work has just begun and includes many technical hurdles. Foremost of these is that many databases that contain circuit information are not specifically used for national security level needs but are engineered to maximize efficiency for all customers. Thus, special modifications would be needed to isolate the very small number of circuits that have an NS/EP purpose. Second, telecommunications companies must develop a common lexicon so that processes/capabilities can be adopted across companies. Third, this work must be done with the understanding that, as in the financial services sector, telecommunications companies are competitors; and sharing specific information about customers' services in an automated database is unprecedented, and is contrary to many business practices in existence today. The "real time routing certification" option is a highly technical and expensive process and the ATIS initiative may or may not achieve the solution that the financial services sector seeks—service that remains resilient and able to withstand significant events or incidents with minimal to no impact yet remains within acceptable cost parameters. Therefore, the task force recommends that the President support the ATIS National Diversity Assurance Initiative and the development of a process to examine diversity assurance capabilities, requirements, and best practices for critical NS/EP customers and, where needed, promote research and development to increase resiliency, circuit diversity, and alternative transport mechanisms. In addition, major conclusions and findings from this initiative should be shared with the telecommunications industry and financial services sector communities.

4.1.3 Mutual Understanding, Contract Terms, and Tariffs

A common theme in many task force discussions centered on the perceived lack of understanding of contractual terms between the financial services sector and the telecommunications sector. Financial services sector participants cited difficulty in understanding how service providers define diversity, as a general term, and how contracts interrelate with tariffs. This paper sets forth some of the ways in which diversity can be defined and illustrates how the definition can be tailored to fit specific customer needs.

Additionally, the interrelationship of tariffs to contracts is a topic that financial services sector members should consider when gaining an understanding of how diversity is defined. Often, telecommunications companies have a definition of diversity in their tariff, but no standard definitions exist across tariffs. Within the task force, there was disagreement over whether reevaluating tariffed offerings is necessary. The FSTF was not able to reach resolution on that issue but raise the concern for those engaged in regulatory functions to analyze.

It should also be noted that general contract terms are often in conflict with the objectives of maintaining continuous service of NS/EP critical circuits during a significant event or crisis. In

fact, *force majeure* or "acts of God" clauses can nullify a party's obligations under a contract.[16] The parties should understand force majeure clauses in contracts related to NS/EP circuits or critical functions. Care should be taken to ensure that critical functions will not be left unsupported if the "unforeseeable" becomes reality. In the post September 11, 2001, environment, resiliency should be contemplated and understood in terms of potential interruption from events considered outside the control of either party.

4.1.4 The Centralized Network Approach for Enhancing Security and Resiliency of Critical FS Circuits

The FRB estimates that there are approximately 6,000 NS/EP-level circuits that qualify for TSP within the financial services sector. By contrast, the Nation's networks currently support more than 183 million wireline circuits alone.[17] Given the configuration, size, and scope of our Nation's telecommunications service providers and the number of circuits they support, the number of *critical* circuits, even estimated at a total of 150,000 across the U. S. for all sectors, is on a small scale.

Consolidating the critical circuits of the financial services institutions into a single managed network may prove effective to enhance scale, network management, and security, and to control costs. Managed networks provide a consistent solution across the board allowing for greater service levels and support, as opposed to addressing needs on a circuit-by-circuit basis. For example, some managed networks can be designed to use Internet Protocol based solutions to enable dynamic routing (an "always on" solution, without as stringent diversity requirements as static routing) approaches. Managed networks have better ability to ensure consistent security and authentication, within parameters and requirements agreed upon by all parties and within acceptable risk limits.

In a competitive marketplace, it may be difficult for financial services institutions to agree on a single solution. Moreover, the centralized network approach raises concerns about security, control, and confidentiality for the financial services customers. The financial services participants of the task force agree that the centralized network option is not an appropriate solution or approach for everyone in the sector. Therefore, the FSTF recommends the financial services sector to continue examining ways to develop a feasible "circuit by circuit" solution to ensure telecommunications services resiliency. Where feasible, the task force recommends supporting research and development initiatives examining the benefits of aggregating NS/EP sector-wide telecommunications requirements into a common framework to protect national economic security.

Two Managed Network Approaches

---

[16] *Force majeure* is defined as a clause "to protect the parties in the event that a part of the contract cannot be performed due to causes which are outside the control of the parties and could not be avoided by the exercise of due care." *Black's Law Dictionary*, 6th ed., 1990.

[17] *FCC's Local Telephone Competition: Status June 2003*, report released December 22, 2003. http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/lcom1203.pdf

The task force received detailed briefings on two large, existing managed network efforts designed in one case for assured redundancy and diversity, and in the other case for high reliability. The two networks are customized to meet specific and very high-level resiliency and security requirements, and were built at a high cost. These two network offerings are discussed as examples of highly resilient or robust networks; their inclusion does not constitute FSTF endorsement. They are, however, examples of the levels of coordination, communication, engineering, and capital that must be committed to attain the highest possible levels of resiliency commercially available today.

Secure Financial Transaction Infrastructure

The Secure Financial Transaction Infrastructure (SFTI$^{SM)}$ is a financial industry network solution that combines recovery, redundancy, and diversity solutions to provide continuous telecommunications resiliency. SFTI^{SM} is a result of a telecommunications strategy employed to achieve assurance of redundancy and diversity for a critical financial industry function provided by the Securities Industry Automation Corporation (SIAC). SIAC designed SFTI^{SM} to be a robust, resilient infrastructure with no single point of failure, and very low end-to-end latency and skew. This solution consists of a dynamic configuration with remote management and testability capabilities, and an effective event monitoring and reporting structure that relies on several key elements: migration to IP and elimination of legacy protocols, consolidation of traffic onto fewer, larger pipes by replacing multiple special purpose circuits, and location of SIAC "demarcs" away from data centers. Primary SFTI^{SM} customers include the New York Stock Exchange, the American Stock Exchange, other U.S. market centers, market data providers, and clearance and settlement institutions.

SFTI^{SM} follows stringent data communications architecture requirements; it provides bandwidth guarantees per internal network and guaranteed bandwidth per application. SFTI^{SM} also ensures customers' presence at a minimum of two access centers and protects one customer from another through route and filter management. Its access centers rely on several service providers' services and extranets to support multiple applications and offer easy capacity reallocation and expansion. Network operations centers provide customers two remote, out-of-band management teams that can take over all operations if one of them is destroyed and ensure continuous operation. These two centers have been engineered and equipped to be fully self-sufficient and sustain operations for several consecutive days in the event of a natural or manmade disaster. In addition, SIAC audits its circuit routing on a set schedule to ensure the regular grooming that telecommunications service providers perform does not compromise diversity. Recently, the Securities Industry Association (SIA) and Securities and Exchange Commission (SEC) recognized SFTI^{SM} as an industry-wide solution.

Federal Aviation Administration Leased Interfacility National Air Space Communications System

The FAA LINCS is a highly diverse private network constructed to meet specific requirements of a customer with critical mission requirements.

The FAA LINCS is the most "available" private line network in the world with an off-backbone availability requirement of 99.8 percent. More than 21,000 circuits serve the entire network.[18] Over 200 circuits form the LINCS backbone and satisfy diversity requirements of 99.999 percent availability. Such diversity requirements allow for a maximum total of 5 minutes of network outage time per year. Every routing change on the FAA LINCS network must be tracked through a manual feed to maintain diversity, and any diversity violations are rectified and reported to the FAA monthly. Emergency maintenance that forces diversity violations is flagged accordingly and resolved as soon as possible. Therefore, diversity maintenance is a very labor intensive and expensive process. Despite natural disasters, major failures of public infrastructures, and the 2001 terrorist attacks, the FAA LINCS survived as designed, keeping the line of communication open between air traffic controllers and airplanes. Developing and maintaining additional networks with similar availability requirements would require many years of engineering and employment of a large number of dedicated staff.

In July 2002, the FAA initiated a substantial modernization of its telecommunications networks to meet its growing operational and mission support requirements and to provide enhanced security features. The new FAA Telecommunications Infrastructure (FTI) Program is an integrated suite of products, services, and business practices that provide a common infrastructure supporting the National Airspace System (NAS) requirements for voice, data, and video services; improve visibility into network operations, service delivery status, and cost of services; and integrate new technologies as soon as they emerge. The phased transition to FTI is expected to take approximately 5 years and, once implemented, FTI will continue relying on a manual certification process of diverse circuits.

4.1.5 Use of Sector Dependency Assessments

The members of the financial services industry, other sectors, and Government officials realize that the security and resilience of critical financial services functions are dependent on the telecommunications infrastructures and are fundamental to the health and well-being of the American public and the Nation's economy. Other critical infrastructure sectors have similar dependencies.

To assess possible areas for joint improvement in an area of high concentration of critical financial services functions, representatives of the financial services and telecommunications industries, with support from relevant Federal agencies, recently held a "Joint Pilot Recoverability Assessment Information Exchange." By joint agreement, the pilot effort and its contents are subject to a non-disclosure agreement. It can be said, however, that the exercise was the first known cross-sector exercise between the financial services and telecommunications sectors.

[18] FAA LINCS information was provided to the FSTF by Mr. Dan Smith, MCI, on April 22, 2003.

Dependency assessments among sectors will continue to evolve in utility and focus and are to be actively encouraged. When preparing cross-sector assessments, it is important to focus first on the NS/EP requirements of the sectors. The Federal Government leadership in coordinating such multiple-sector NS/EP assessments is essential due to the significant legal and competitive market safeguards issues that must be satisfactorily addressed for participants. Often, any solutions or next steps resulting from such assessments may require efforts by industries that far exceed market force capabilities or demands. Cost to participants in undertaking such important assessments is also a significant factor requiring Government assistance. Consistent with the Homeland Security Presidential Directive 7, the Department of Homeland Security should continue to coordinate and support relevant cross-sector activities (e.g., standards development, research and development, pilot initiatives, and exercises). In addition, the Federal Government should provide statutory protection to remove liability and antitrust barriers to collaborative efforts in the interest of national security.

It should be noted that many of the underlying challenges about security and infrastructure protection can be handled in a customer-to-provider context. Customers now, more than ever, are inquiring about the security and resiliency of their services, and the physical paths over which those services route. Customer inquiries will go a long way towards improving communications and understanding between service providers and financial services customers; and customer assessments derived from a common template of mutually acceptable assessment practices are recommended.

4.3 Telecommunications Service Priority (TSP) Program

Business continuity planning is critical for all institutions that play a role in the operation of critical infrastructures. An institution's restoration and recovery planning should include the TSP program as a key component. The TSP program was established by the Federal Communications Commission (FCC) Report and Order dated November 1988 and is the regulatory, administrative, and operational framework for priority restoration and provisioning of any qualified NS/EP telecommunications service. The financial services sector has been a strong adopter of TSP as a component of recoverability or restoration planning. The Financial and Banking Information Infrastructure Committee (FBIIC) has established policy for financial institutions' use of TSP, and information is available on its Web site (www.fbiic.gov) in the "policies" area.

Other sectors should reference the work of the financial services regulators for assistance in determining an appropriate framework to ascertain which circuits or services would qualify for TSP protection. A telecommunications service provider with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service. Currently, there are more than 52,000 total active TSP assignments in support of NS/EP telecommunications in the TSP program.

Accordingly, the FSTF supports the efforts of the financial services regulators and industry associations in promoting TSP and recommends that the financial services community continue to consider TSP as a part of its NS/EP restoration and recovery planning needs.

4.4 Alternative Transport Mechanisms for Resiliency

The task force recognized that in some cases, the use of different media and technologies could aid in diversity assurance and telecommunications service predictability. Technologies that provide for communications via non-terrestrial media are emerging options for creating independent transport mechanisms in a local environment, where redundancy and diversity are essential. Alternative technologies, such as satellite, laser, microwave, and spread spectrum wireless, have the capability to offer alternate routings for the most critical communications if reliance on more than the terrestrial transport is considered necessary. In addition, using these wireless technologies can often overcome hurdles imposed by local regulators reluctant to permit pavement to be torn up for new or alternative fiber conduits in and out of a municipality. These technologies are offered as options, not requirements, for financial services institutions to consider when developing business continuity plans and assessing appropriate levels of resiliency for a given function. The following are descriptions of sample alternative technologies for consideration.

Satellite Technology. The Department of Defense (DOD) has relied on satellite communications as part of its defense communications structure for several decades. Satellite communications links efficiently extend the reach of terrestrial communications systems to distant areas and provide an independent infrastructure for alternative routing of traffic in an emergency. Most important, because their principal assets are in space, satellite communication systems with diverse ground sites can continue to function during disasters (e.g., natural disasters or terrorist attacks), that might render other communication methods inoperable.

Aside from the obvious satellite benefits, which include large coverage area and the high-speed and high-quality of the transmission, satellites offer much needed operational flexibility. Satellite communication networks offer users the ability to change network size and traffic flows in addition to monitoring and controlling equipment in a timely manner. Presently, agencies across the U.S Government lease broadband circuits on a variety of commercial satellites in geostationary orbit (an altitude of 30,000km) for both operational and emergency communications. In addition, the U.S. Government owns a number of military-unique communications satellites in the same orbit that offer circuits with added protection, making them largely immune to jamming and other attacks.

Although these benefits are many of the more attractive and efficient reasons for considering satellite communications, it should be noted that satellite communications have a few drawbacks. Severely inclement weather (e.g., hurricanes) can temporarily interrupt satellite transmission in the affected area, and other transmission delays in satellite circuits may affect certain types of applications.

Laser Technology. Private sector companies use laser-based technologies to transfer data in metropolitan areas. These optical-based applications use a series of connectors to "beam" information between nodes. Laser transmissions are difficult to detect; however, the technology is not a viable option for rural areas because the maximum distance between transmission links is only 500 meters. In addition, natural disasters and weather phenomena hamper laser communications capabilities.

Microwave Technology. Narrowband microwave technology is similar to broadcasting from a radio station. Unlike laser technology, which requires a direct line-of-sight, microwave technology uses the portion of the electromagnetic spectrum that exists below infrared frequencies but above normal radio frequencies to transmit voice and date communications (18.82 to 19.205 GHz).

Microwave radio links are used to integrate a broad range of networks from fixed and mobile communication networks. At present, many of the data communications services offered by mobile cellular networks are supported by microwave technology. Microwave technology takes less time to install than wire alternatives and can provide greater flexibility. Although the cost of microwave technology may be higher than other options, the medium has proved highly resistant to outside interference. Possible drawbacks are that the broadcast range of microwave technology is roughly 5,000 square meters, and the transmissions cannot travel through steel or load-bearing walls.

Spread Spectrum Technology. Spread spectrum technology uses wideband, noise-like signals to spread a given radio signal over a wide spectrum of radio frequencies. In standard narrowband communications, each channel operates over a tiny segment of the radio spectrum; and the FCC regulates the spectrum by assigning or licensing segments. Spread spectrum technology allows multiple radio signals to operate in an open, unlicensed band with little or no interference. Spread spectrum and narrowband signals can share the same band simultaneously. The variance in spread spectrum signals makes the transmission difficult to detect, intercept, or demodulate.

Although these technologies hold promise, they cannot be universally applied as a solution for telecommunications diversity in the financial services sector. Experience within the financial services industry has demonstrated that bandwidth, data transmission latency, security, and reliability issues may limit the practical application of these technologies as near-term solutions. The FSTF recommends that the President support additional research and development initiatives around these technologies as, in the future, they could yield significant resiliency benefits for NS/EP needs.

4.5 Summary of Resiliency Considerations

Financial services institutions, and other organizations with NS/EP responsibilities, struggle to achieve predictable and reliable levels of telecommunications resiliency due in part to the inconsistent meaning of diversity. In the past, the financial services sector may have erroneously assumed that diversity was established simply by ordering two circuits from different service

providers. In addition, the financial services sector was not aware that, while diversity can be engineered and verified at its initial implementation, routine technical maintenance within the telecommunications service providers' networks may inadvertently reassign circuits or switch provisioning that reintroduce common points of failure. Clearly, the task force deliberations have indicated that far more is required to ensure diversity.

Diversity can be appropriately engineered either by the service provider, the customer, or both in collaboration. If the customer decides to undertake the engineering, the customer must be prepared to fully understand the telecommunications universe, including the terms of art (definition of diversity, resilience, availability, etc.) and technology. Conversely, if the service provider is to deliver a turnkey solution, the service provider must fully understand its customer's business environment and how that drives the criticality of any given circuit. As noted with the FAA LINCS and SFTI^{SM} networks, no longer can customers just purchase a few circuits and assume that they will meet their critical business needs. For a successful engineering of telecommunications services, mutual understanding of each party's business operations is key to maintaining the resiliency of critical functions.

5.0 FINANCIAL CONSIDERATIONS AND INCENTIVES FOR ENHANCING RESILIENCY OF NS/EP BUSINESS OPERATIONS

The telecommunications industry's experience has demonstrated that implementing high levels of network redundancy and diversity assurance measures proves extremely costly. As such, market demands must justify the costs for these requirements to be included in the broader network framework. As noted in this report, the NS/EP telecommunications needs of the financial services sector do not provide sufficient market leverage because the number of critical circuits is a very small commercial requirement. To ensure NS/EP functionalities are integrated into a large network, a network operator needs a guaranteed cost recovery model that is independent from the general public base. Therefore, from a public policy perspective, it is most important that options to address appropriate mechanisms to stimulate market investments be further examined. Mandates for such services are ineffective without appropriate funding mechanisms.

5.1 Capital Incentives

As core financial NS/EP processes are vulnerable to disruption, it is not advisable to rely exclusively on market forces and voluntary guidelines to create the necessary mechanisms to protect the national economy. As a solution, targeted capital incentives would encourage critical infrastructure owners, including the financial services sector, to make the necessary investments to mitigate telecommunications resiliency risks to their business operations. Historically, capital incentives serve as a mechanism of national policy promoting the public good. Appropriately structured capital recovery incentives for critical business operations could be used to accelerate immediate investments to mitigate vulnerabilities to critical NS/EP operations.

The required economic analysis and design of the most feasible capital recovery investment model is beyond the expertise of the FSTF participants. Therefore, the task force recommends that the President direct the appropriate departments and agencies to examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions.

6.0 FINDINGS

In analyzing the dependencies between the telecommunications and financial services sectors within the telecommunications risk methodology outlined in section 3.1, the FSTF developed a generic set of findings. Note that these findings, though examined in the context of the financial services sector, are applicable to other sectors that support NS/EP functions.

- **Comprehensive business continuity planning and practices are essential.** Neither the Federal Government nor a critical infrastructure can respond to a national-level crisis without critical infrastructure sectors employing strong business continuity and disaster response planning practices. Financial services entities that focus on the importance of resiliency in the context of their business continuity planning are better situated to partner with telecommunications companies to ensure that their needs are met.

- **The Nation needs telecommunications networks that operate in a resilient manner.** Networks should be resilient enough to provide maximum continuity of services with minimum functional disruption.

- **NS/EP functions should acquire the highest levels of telecommunications resiliency assurances available.** The continuity of the payment, clearing, and settlement processes of the financial services sector is critical to the overall economic security of the Nation.

- **Ensuring uncontaminated network resiliency and diversity is costly.** Financial services entities that have achieved high levels of network resiliency and diversity have done so only with significant levels of effort and expense.

- **A clear understanding between contracting parties is critical.** A clear contractual understanding between telecommunications service providers and financial services institutions is required to ensure resilient services. Contractual provisions can include requirements from customers that engineered redundancy and diversity will be maintained independently from grooming.

- **Public policy options are needed to stimulate investments.** From a public policy perspective, appropriate mechanisms to stimulate market investments to enhance NS/EP telecommunications resiliency capabilities should be identified.

- **Cross-sector understanding needs to be promoted.** Both telecommunications and financial services sectors should continue in their efforts to engage members of their

communities, as well as the public sector, in a constructive dialogue that will help foster mutual understanding of their operations and unique needs.

7.0 CONCLUSIONS

- Diversity, redundancy, and recoverability capabilities are indispensable to achieve resiliency.

- Telecommunications service providers define diversity solutions in contracts with each customer according to the customer's unique requirements. Diversity solutions can range from simple, relatively inexpensive measures, like dual dial tone sources, to comparatively costly network architectural solutions.

- Recovery and redundancy together cannot provide a sufficient level of resiliency if these measures can be disrupted by a single event; therefore, diversity is crucial. Industry best practices for diversity include separation of multiple circuit paths, decentralization of office facility connections, and alternative transmission technologies.

- A resilient financial services operation and its critical telecommunications services must be able to endure hazards of nature, such as earthquakes, tornados, floods, and other natural disasters, as well as manmade hazards, such as bombings, cyber crimes, malicious destruction, and terrorist attacks.

- Diversity solutions will continue to evolve if the telecommunications sector continues research and development efforts, and if the Federal Government and critical infrastructure customers continue to encourage and participate in those efforts.

- Without a real-time process to guarantee that a circuit's path or route is static and stable, an NS/EP customer cannot be assured at all times that its diversity plan is being met.

- Statutory protection to remove liability and antitrust barriers to collaborative efforts is needed in the interest of national security.

- An institution's restoration and recovery plan should include the TSP program as a key component.

- Technologies, such as satellite, laser, microwave, and spread spectrum wireless, have the capability to offer alternate routings for the most critical communications if reliance on more than the terrestrial transport is considered necessary.

- The telecommunications industry's experience has demonstrated that implementing high levels of network redundancy and diversity assurance measures prove extremely costly. As such, market demands must justify the costs for NS/EP requirements to be included in the broader network framework.

- Targeted capital incentives would encourage critical infrastructure owners, including the financial services sector, to make the necessary investments to mitigate telecommunications resiliency risks to their NS/EP operations.

- Diversity can be engineered either by the service provider, the customer, or both in collaboration. Therefore, mutual understanding of each party's business operations is key to maintaining the resiliency of critical functions.

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—

- Support the Alliance for Telecommunications Industry Solutions' National Diversity Assurance Initiative and development of a process to:
  - Examine diversity assurance capabilities, requirements, and best practices for critical NS/EP customers and, where needed,
  - Promote research and development to increase resiliency, circuit diversity, and alternative transport mechanisms.

- Support financial services sector initiatives examining:
  - The development of a feasible "circuit by circuit" solution to ensure telecommunications services resiliency, and
  - The benefits and complexities of aggregating sector-wide NS/EP telecommunications requirements into a common framework to protect national economic security.

- Coordinate and support relevant cross-sector activities (e.g., standards development, research and development, pilot initiatives, and exercises) in accordance with guidance provided in Homeland Security Presidential Directive 7.

- Provide statutory protection to remove liability and antitrust barriers to collaborative efforts is needed in the interest of national security.

- Continue to promote Telecommunications Service Priority program as a component of the business resumption plans of financial services institutions.

- Promote research and development efforts to increase the resiliency and the reliability of alternative transport technologies.

- Examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions.

APPENDIX A

TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Electronic Data Systems	Mr. William Sweeney, Chair
Bank of America	Mr. Roger Callahan, Co-Vice Chair
BellSouth	Ms. Cristin Flynn, Co-Vice Chair
AT&T	Mr. Harry Underhill
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
Lucent Technologies	Mr. Karl Rauscher
MCI	Ms. Joan Grewe
Microsoft	Mr. Joel Greenberg
Nortel Networks	Dr. Jack Edwards
Northrop Grumman	Mr. Bill Gravell
Qwest Communications	Mr. Tom Snee
Raytheon	Ms. Heather Kowalski
SAIC	Mr. Hank Kluepfel
SBC Communications	Ms. Rosemary Leffler
Sprint	Mr. John Stogoski
USTA	Mr. David Kanupke
VeriSign	Mr. Michael Aisenberg
Verizon Communications	Ms. Ernie Gormsen

OTHER PARTICIPANTS

BellSouth	Mr. David Barron
BellSouth	Mr. Shawn Cochran
BellSouth	Mr. Doug Langley
BITS	Mr. John Carlson
BITS	Ms. Heather Wyson
Electronic Data Systems	Ms. Liesyl Franz
George Mason University	Dr. Kevin McCrohan
George Washington University	Dr. Jack Oslund
Qwest Communications	Mr. Jon Lofstedt
Raytheon	Mr. James Craft
SBC Communications	Ms. Suzy Henderson
SIAC	Mr. Andrew Bach
Sprint	Mr. Todd Colvin
Sprint	Ms. Laura Harper
The Clearinghouse	Mr. Al Wood
Verizon Communications	Mr. Lowell Thomas

GOVERNMENT PARTICIPANTS

DHS	Mr. Darrell Mak
GSA	Mr. Tom Sellers
FCC	Mr. Ken Moran
FRB	Mr. Ken Buckley
FRB	Mr. Chuck Madine

APPENDIX B

Terms of Reference Associated with Diversity

This appendix provides baseline terms of reference that can be used by communications managers to understand the various elements that need to be considered when contracting for diversity in telecommunications services. The lack of diversity in any of these elements does not obviate the service assurance, but merely increases the level of risk associated with that entire package of protection. By clearly understanding what is available, and what can or cannot be provided, telecommunications managers will be better empowered to make the risk analyses decisions necessary to protect the Nation's financial services and maintain liquidity. The items described below are typically not differentiated in tariffs; and given the tendency towards eliminating tariffs, some providers could consider offering these items, as well as others, as custom build offerings to provide increased diversity to key customers. It should be noted that customers also have a responsibility for ensuring that they request diversity for other aspects of their telecommunications needs that are beyond the scope of a service provider's responsibilities, e.g., multiple entrances into buildings, multiple risers. This type of coordination needs to take place between the customer and the building owner.

Terms of Reference

Power and Fusing: No components of a paired transmission path should share a common fuse or electrical load. (Manual verification.)

Cabling: There should be diverse cable routes between individual paths within the central office and within the customer locations. (Manual verification.)

Distributing Frames/Mounting Blocks: Termination of diverse circuits must be on separate distributing frame-mounting blocks. (Manual verification.)

ORB, DSX Panels: Diverse circuits should not traverse a single bay of these types.

Digital Cross-connect System: Where possible, diverse circuits should not traverse a single DCS system.

D4/D5 Bays: The channel bank equipment associated with each circuit should be located in separate bays.

Fiber Optic Terminals and Multiplexers: Diverse circuits should not transit common multiplex equipment when possible or technically feasible.

Test Access Equipment: Diverse circuits should not traverse a single active test access unit. (An element is considered active if it regenerates the signal and passive if there would be no adverse impact on signal transmission if the device failed.)

Timing/Synchronization Equipment: BITS clocks should utilize all diverse capabilities available. The timing feed to each type of diverse circuit should emanate from a different output card on the BITS or secondary clock in the office.

Note: It is recognized that for a service provider to ensure intra-office diversity, many of these common points must be checked manually, which will be difficult to accomplish. Ongoing maintenance activity and circuit management rearrangement opportunities should be used to verify that these components do not provide a single point of failure in the critical circuit path.

Requirements for physical cable diversity are summarized below.

Route Diversity

Route diversity is defined as having two physically or logically separate paths between the two ends of a circuit. Physically separate means separate cable sheaths and outside plant structures along different routes. The physical separation must exist from, at a minimum, the first splice access point (generally a manhole) out of one office to, at a minimum, the first splice access point (generally a manhole) before entering the next office.

Implementation schemes for interoffice route diversity include:

Split Circuit Routing
Two circuits are placed on separate service provider systems routed along different paths (one circuit on each path.) The service provider's systems should be diverse routed over separate cable sheaths and outside plant structures. This can be accomplished with fiber, copper, or radio facilities.

Fiber Systems with Alternate Path Protection
The protection channel (two fibers) of an asynchronous fiber system is routed in a separate cable sheath and outside plant structure. This is an example of a "self-healing" facility. This requires fiber facilities in both routes.

SONET or Asynchronous Fiber Ring Systems
In this configuration, two of the four fibers are routed in a separate cable sheath and outside plant structure. This is an example of a "self-healing" facility. Fiber facilities are required in both routes.

Structure Diversity

Structure diversity is an alternative method of providing diversity. It is defined as two physically separate sheaths and structure along the same path. The physical separation can be achieved in several ways:

Aerial/Buried
One cable is buried and one cable is aerial. This alternative should be considered when no underground facility is available.

Buried/Buried
Two cables are buried in separate trenches with maximum separation (e.g., opposite sides of a road or other public thoroughfare.)

Aerial/Aerial
Two aerial sheaths are affixed on separate pole lines with maximum separation (e.g., opposite sides of a road or other public thoroughfare.)

Underground/Underground
Two underground sheaths are placed in different ducts in either the same or different conduit runs. If the same conduit run is used, the maximum practical separation in the cross-section should be achieved. Vertical separation provides a greater degree of protection than horizontal separation. Two conduit runs in the same easement on the same side of the road will be considered as one run.

Aerial/Underground
This mode consists of one aerial sheath and one underground sheath. However, once conduit is placed along a route, it is generally considered to provide the greatest degree of protection and is usually used for the placement of all new cables and cables to replace buried and aerial cables. This type of diversity is preferable to underground/underground diversity only when a separate duct is unavailable and adequate pole space exists.

Buried/Underground
This mode uses one buried fiber sheath and one underground sheath. However, once conduit is placed along a route, it is generally considered to provide the greatest degree of protection and is usually used for the placement of all new cables and cables to replace buried and aerial cables. This type of diversity is preferable to underground/underground diversity only when a separate duct is unavailable and adequate pole space exists.

APPENDIX C

NS/EP communications functional requirements as defined by the NSTAC in its Convergence Report[19]

NS/EP Communications Functional Requirements

NS/EP Communications Functional Requirements	Description
Enhanced Priority Treatment	Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
Secure Networks	These services ensure the availability and survivability of the network, prevent corruption of or unauthorized access to the data, and provide for expanded encryption techniques and user authentication.
Restorability	Should a service disruption occur, voice and data services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
International Connectivity	Voice and data services must provide access to and egress from international carriers.
Interoperability	Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks.
Mobility	The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service [PCS], cellular, satellite, High Frequency [HF] radio).
Nationwide Coverage	Voice and data services must be readily available to support the National security leadership and inter- and intra- agency emergency operations, wherever they are located.
Survivability	Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential communications.
Scaleable Bandwidth	The ability of NS/EP users to manage the capacity of the communications services to support variable bandwidth requirements.
Addressability	The ability to easily route voice and data traffic to NS/EP users regardless of user location or deployment status. Means by which this may be accomplished include "follow me" or functional numbering, call forwarding, and functional directories.
Affordability	The service must leverage new public network (PN) capabilities to minimize cost. Means by which this may be accomplished favor the use of commercial off-the-shelf (COTS) technologies and services and existing infrastructure.

[19] The President's National Security Telecommunications Advisory Committee, Information Technology Progress Impact Task Force Report on Convergence, NSTAC XXIII, 2000.