Financial Services Sector Coordinating Council

for Critical Infrastructure Protection and Homeland Security

FILED/ACCEPTED

SEP - 8 2010

Federal Communications Commission
Office of the Secretary

September 3, 2010

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission

Submitted Electronically

Re: FCC Notice of Inquiry, PS Docket No. 10-92: Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload

Dear Ms. Dortch:

The Financial Services Sector Coordinating Council (FSSCC)[1] welcomes the opportunity to comment on the FCC Notice of Inquiry regarding communications survivability and resiliency, cyber security certification, and network outage reporting. We have provided reports, comment letters, and best practices on this topic in the past that are relevant to our current comments.[2]

Technology advances over the last 25 years have fundamentally changed the way that our national economic activities and financial systems perform their essential functions. Broadband IP-based telecommunications capabilities, whether wired or wireless, are becoming the "common carrier" for performing the essential and vital business and personal processes and functions we all depend upon. This ever increasing dependency on telecommunications for all aspects of our national livelihood, necessitates the FCC and telecommunications industry assure beyond a "best efforts" basis, that the telecommunications infrastructure remains secure and available to the financial services sector and the other critical industries.

---

[1] The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), established in 2002, is the sector coordinator for Financial Services for the protection of critical infrastructure, focused on operational risks. Because the FSSCC fits into a larger network of industry / sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

[2] A sampling of and links to previous FSSCC documents and Association comment letters/best practices papers is included as an attachment to this comment letter.

No. of Copies rec'd 0
List ABCDE

To address risks in today's environment and to address regulatory requirements, financial institutions seek telecommunications providers that can offer:

- No single point of failure
- Resilient infrastructure
- Engineered diversity and methods for maintaining the engineered diversity over time
- Low end-to-end latency
- Services supporting high-bandwidth needs
- Remote, out-of-band, management and testability
- Strong network security

We believe that the financial service sector needs a factual basis for ensuring our essential telecommunications needs will be available at needed performance, reliability, resiliency and security. This includes:

- Being able to verify through standardized reporting, analysis and stress test that we our requirements are met
- Being provided timely notice of changes that would affect the characteristics being depended upon.
- Having the essential communications needs of critical industries, such as the financial services sector, be provided end-to-end priority in times of emergency. The priority should be commensurate with the relative priority of its critical functions it supports. This requires built-in capability to prioritize traffic in times of emergency, along with a plan and process for providing priorities services in times of emergency. This priority services should he verifiable and testable.
- Expanding the above to include similar treatment for emerging public cloud computing and storage services[3].

We would be happy to be part of a multi-industry task force to develop an implementation plan to achieve these needs.

Doug Johnson
Vice President, Risk Management Policy
American Bankers Association
Co-Chairman, Policy Committee
Financial Services Sector Coordinating
Council

---

[3] The trend to public clouds will only increase our dependency, not only on public telecommunications but on network connected public processing and storage utilities. Planning should start now to expand this notion of assurance, stress test and the availability of priority emergency services to critical industries of these minimum essential levels of redundancy, availability, resiliency and security of out nation's public telecommunications, computing and storage resources. Security and privacy concerns become even more essential when we are including, not only telecommunications, but computing and storage.

Financial Services Industry Efforts
Communications Survivability and Resiliency

1. FSSCC Statement on Telecommunications Resiliency (2004)
   https://www.fsscc.org/fsscc/reports/2004/FSSCC_Telecom_Statement.pdf
2. 2005 FSSCC Annual report (in particular the section on page 11 that deals with "addressing cross-sector dependencies")
   https://www.fsscc.org/fsscc/news/2006/annual_report.jsp
3. BITS Guide to Business Critical Telecommunications Services (2004)
   http://www.bitsinfo.org/downloads/Publications%20Page/bitstelecomguide.pdf
4. NSTAC Financial Institution Task Force Report (2004)
   http://www.ncs.gov/nstac/reports/2004/Financial%20Service%20Task%20Force%20Report%20(April%202004).pdf
5. ChicagoFIRST Telecommuting Test (2010)
   https://www.chicagofirst.org/press/2010/press_20100614.jsp
6. BITS Forum: "Securing Data in Web-Based Business Applications" (2008)
   http://www.bits.org/downloads/Events/SecurityForumAgenda.pdf
7. BITS Fraud and Identity Theft Prevention papers
8. BITS eMail Security Toolkit (2007)
   http://www.bitsinfo.org/downloads/Publications%20Page/BITSSecureEmailFINALAPRIL1507.pdf
9. BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information (2006)
   http://www.bitsinfo.org/downloads/Publications%20Page/BITSABADBNov06.pdf
10. Focus on Mobile financial services (and upcoming BITS-FSTC forum)
11. ABA-BITS-FSTC-FSISAC efforts on ICANN