Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr. Suite 230
Reston, VA 20191

July 17, 2018

Fiona Alexander
National Telecommunication and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, D.C. 20230

Submitted electronically to iipp2018@ntia.doc.gov

RE: Notice of Inquiry: *International internet Policy Priorities*
Docket No. 180124068–8068–01; RIN 0660–XC041
83 *Fed. Reg*. 108, 26036 (June 5, 2018).

Dear Ms. Alexander:

The Financial Services Sector Coordinating Council (FSSCC)[1] submits this letter to the United States Department of Commerce's National Telecommunications and Information Administration (NTIA) in response to its Notice of Inquiry on *International internet Policy Priorities* (Notice) issued for comment on June 5, 2018. We commend the NTIA on its efforts to reach a broad cross section of stakeholders to assist in the identification of policy priorities and welcome the opportunity to work with NTIA to effectively leverage resources and expertise.

As FSSCC, our perspective on international internet policy is shaped by our position as identified critical sector within the United States, and the role of the internet within critical infrastructure. We suggest the goal of any internet policy priority is protecting domestic critical infrastructure while facilitating the global delivery of critical products and services. Although this letter focuses on our immediate concerns with the expansion of data localization internationally, we invite the opportunity to engage with you further on the other themes highlighted in the Notice: internet governance, privacy, and innovation. We offer this letter as the initiation of a longer and more detailed conversation with FSSCC and the financial services industry.

A Functioning Internet is an Essential Component of Critical Infrastructure

The free flow of data between countries is essential to a functioning global digital economy. The financial sector relies upon the exchange of data between markets to execute business transactions, communicate with customers, address cybersecurity risks, and meet compliance requirements. To support the international financial system, financial institutions have global

[1] Formed in 2002 as a public/private partnership with the support of the United States Department of the Treasury, FSSCC collaborates with the Treasury and the financial regulatory agencies at the federal and state levels through the Financial and Banking Information Infrastructure Committee, which also formed in 2002 under Treasury's leadership. Members include 72 of the largest financial institutions and their industry associations representing banking, insurance, credit card networks, credit unions, exchanges, financial utilities in payments, clearing and settlement.

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr. Suite 230
Reston, VA 20191

communications networks and data processing operations, which often rely on a global internet infrastructure.

Government capability must be applied to protect infrastructure—whether public or private—and should be prioritized based on the criticality of the infrastructure to national and economic security. While there are many efforts to increase private sector cybersecurity, an effort focusing on those sectors providing the most critical services is needed.

Each of the identified critical sectors has sector, cross-sector, and government coordinating councils. Increasingly, these councils are appropriately focusing resources and coordination on identifying and addressing systemic threats to that infrastructure. Each is establishing a relationship with the public sector that goes beyond information sharing, seeking instead operational collaboration. These partnerships continue to evolve, but the current framework could serve as a model internationally.

RECOMMENDATIONS

To enhance security, international and domestic critical sector public and private partners should more closely adhere to these principles:

1. As expressed in the 2013 National Infrastructure Protection Plan –

   "[C]ritical infrastructure partners must collectively identify national priorities; articulate clear goals; mitigate risk; measure progress; and adapt based on feedback and the changing environment. Success in this complex endeavor leverages the full spectrum of capabilities, expertise, and experience from across a robust partnership…Individual efforts to manage risk are enhanced by a collaborative public-private partnership that operates as a unified national effort, as opposed to a hierarchical, command-and-control structure."

2. Operational collaboration requires scalable structures on the private sector side—governments cannot establish relationships with every private sector entity, even in the critical infrastructure sectors.

3. Governments must be willing to think beyond information sharing when it comes to protecting critical infrastructure.

4. In the United States, coordinating a critical infrastructure response plan with cross-sector collaboration is an active part of our efforts, including scenario testing and developing all-hazards playbook via councils, information sharing organizations and industry response teams.

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr. Suite 230
Reston, VA 20191

Data Localization Hinders Commerce, Security, and Innovation

In opposition to the ideas of a free and open Internet, a growing number of jurisdictions have adopted or considered requirements for data to be stored, processed, or accessed within certain geographic boundaries. These measures have been introduced under various rationales – securing citizen privacy, protecting domestic technology industry, enabling law enforcement investigations, and supporting regulator requests for information. While the sentiment behind these measures may be appropriate and laudable, it is often misguided from technical, business, and policy perspectives. However, collaborative working models exist of bilateral and multilateral agreements, such as the Unites States – Korea Free Trade Agreement (KORUS FTA),[2] and Asian Pacific Economic Cooperation (APEC)[3] Cross Border Privacy Rules (CBPR),[4] respectively. These agreements demonstrate the ability of nations to maintain the free flow of data across borders while addressing legitimate public policy concerns.

Negative consequences of data localization for financial services include:

1. **Business complexity and compromising the preferred technology infrastructure of financial institutions.** The result is reduced efficiency, added cost, and less resilient delivery of services.

2. **Security risks**. Cybersecurity is most effective when conducted across the entirety of a network. Localizing cybersecurity operations undermines scaled security solutions, limits threat analysis and detection capabilities, and burdens cybersecurity workforce and resources.

3. **Increasing regulatory compliance costs**. Localization of data encumbers a financial institution's ability to quickly and efficiently respond to supervisory requests, and measures such as Know Your Customer, Bank Secrecy Act, and Anti-Money Laundering initiatives. Data localization measures may inhibit the ability of companies to respond to legitimate law enforcement requests, a matter being addressed in the United States by the Cloud Act.[5]

4. **Strategic threats to expanded digital trade and economic liberalization.** These measures challenge long held norms around a free and open internet, and as a result, hinder the ability of financial companies to innovate in response to technology trends and consumer preferences.

---

[2] The United States and the Republic of Korea signed the KORUS FTA on June 30, 2007, effective on March 15, 2012. https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta

[3] "…APEC is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific." http://publications.apec.org/About-Us/About-APEC

[4] "The APEC Privacy Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows." http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework

[5] "The CLOUD Act has two major components. The first facet addresses the U.S. government's ability to compel technology companies to disclose the contents of electronic communications stored on the companies' servers and data centers overseas…. The second facet of the CLOUD Act addresses the reciprocal issue of foreign governments' ability to access data in the United States as part of their investigation and prosecution of crimes." Congressional Reporting Service, *Cross-Border Data Sharing Under the CLOUD Act,* https://fas.org/sgp/crs/misc/R45173.pdf (April 2018).

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr. Suite 230
Reston, VA 20191

RECOMMENDATIONS

The data localization and cross-border data flow landscape is increasingly fragmented with little interoperability among approaches. This fragmentation will continue and increase as solitary jurisdictions consider new measures, bilateral trade agreements create permissible flows of data between countries, and broader trade agreements initiate regional frameworks governing the exchange of data and protection of privacy.

To enhance international security, facilitate global commerce, and encourage innovation, FSSCC suggests the adopting an international internet policy:

1. Advocating against data localization measures and technology requirements among trade partners and key economic markets, and within bilateral and multilateral free trade agreements, international forums and policy making bodies,

2. Ensuring cross-border exchange of data between the United Kingdom and European Union under Brexit[6] negotiations,

3. Promoting the interoperability of privacy regimes to support cross-border data flow, for example within the Organization for Economic Co-operation and Development (OECD),[7] and between APEC and the European Union,

4. Engaging domestic and global regulators to better understand concerns over access to data and promoting measures to address concerns, and

5. Encouraging US leadership to pursue implementation of the Cloud Act that mitigates risk and achieves beneficial outcomes.

CONCLUSION

We are living in a world of increased specialization, interconnection, and dependencies. In order for society to function properly, citizens need power for hospitals, homes, and work; the ability to send and receive communications; and the capacity to move money to pay for these services and other essentials. As a result, power, telecommunications, and financial services are among the most critical infrastructure sectors. They are also interdependent, and often depend on a functioning internet to communicate with customers as well as deliver essential products and services. NTIA's international internet policy priorities also should recognize the role of the internet within the critical sector as a part of the critical infrastructure's delivery of critical services.

---

[6] "On Thursday 23 June 2016 the EU referendum took place and the people of the United Kingdom voted to leave the European Union." https://www.gov.uk/government/topical-events/eu-referendum

[7] "The OECD's origins date back to 1960, when 18 European countries plus the United States and Canada joined forces to create an organization dedicated to economic development…Today, our 36 Member countries span the globe, from North and South America to Europe and Asia-Pacific. They include many of the world's most advanced countries but also emerging countries like Mexico, Chile and Turkey." www.oecd.org

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr. Suite 230
Reston, VA 20191

FSSCC welcomes further engagement and discussion with the NTIA about international internet policies and priorities. We look forward to collaborating with you and other stakeholders to identify policy priorities that support financial services, and other critical sector industries, in the management of risk while facilitating global commerce, respecting privacy, enhancing governance, and encouraging innovation.

Sincerely,

Craig Froelich
Chair, Financial Services Sector Coordinating Council
craig.froelich@baml.com