Intel Corporation is pleased to file comments on the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Global Free Flow of Information on the Internet." Intel commends the Department for conducting this inquiry and for its critical efforts on addressing privacy, innovation, and the free flow of information.

Please note that while we have tried to map the below submission to the Department's specific areas of inquiry, as noted, given the many areas of overlap certain questions have been grouped together, and several sections may have application to multiple questions other than those specifically listed.

I. Introduction

The Internet not only enables global information flows, but predominantly operates via interoperable hardware and software products deployed worldwide which are not varied significantly for individual countries or markets. These foundational information and communications technology (ICT) products make up a global digital infrastructure (GDI) that is the central nervous system of not only innovation, but global economic development, social interaction, and trade and investment. New innovations in ICT come about every day, from all corners of the globe, and continue to drive the GDI into the future. Yet, this process is stalled and sometimes blocked by a confusing and often conflicting array of country specific laws and regulations. While technological innovation must continue at a rapid rate, a different type of innovation is necessary as policymakers grapple with the challenges of shepherding the GDI in the coming decades: policy innovation and the development of a global digital infrastructure policy.

This need to develop policies aimed at making the digital environment reliable and trustworthy is becoming an important agenda item for governments and policymakers around the world as the Internet increasingly becomes an indispensable social medium and continues to foster economic growth. However, a siloed, country-specific regulatory approach may unintentionally disrupt a networked environment dependent upon global interoperability and connectivity, unnecessarily imposing restrictions on global information flows.

II. Types of Restrictions on the Free Flow of Information on the Internet (Question 1)

Over the past decade, innovations in ICT have driven the growth of the publicly accessed Internet, and have become foundational tools directly affecting individuals' lives and impacting the functioning of virtually all businesses and government entities.

In the not so distant future, individuals will expect to have ubiquitous access to their data and applications, as provided by a variety of interoperable devices (e.g. PCs, notebooks, netbooks, MIDs, smart phones, home appliances, cars, etc.). Intel's vision is to enable the evolution of the GDI by innovating platform and technology advancements across the breadth of those devices, which will help tackle big problems such as education, energy/environment and health. As the use of the technology evolves, how innovations are implemented to meet the privacy and security expectations of individuals will also need to be fundamental components of the technology.

Certain aspects of the current privacy and security policy structure, when examined globally, seem opposed to the optimal functioning of the GDI. Existing policies are often fragmented, uncoordinated, or geographically based. Each country sets its own rules and regulations in technology, privacy and security policy areas independently, and many countries lack developed privacy and information security laws and regulations entirely.

Such barriers create a need to examine in more detail the three components that have made the GDI successful: (1) maintaining openness; (2) maximizing interoperability; and (3) spurring economic development.

A. Openness

The NOI makes clear that the Department has made it a top priority to ensure that the Internet remains open for innovation. Indeed, the GDI was built on a principle of "openness," encouraging an environment marked by the free flow of data across borders, and an architecture allowing innovative new technologies and ideas to be launched globally. A major risk to the continued growth of the GDI is closing it off by allowing technology or network fragmentation, which can impede individuals from participating in the global network. This fragmentation can take many forms, such as segmented telecommunications networks, country specific filtering requirements and local standards.

Rather than struggle to apply a regulatory scheme that is arguably inapposite to GDI telecommunications, governments around the globe should apply GDI policy principles, such as technology neutrality and flexible laws and regulations that encourage openness.

B. Interoperability

An important benefit of the GDI is seamless operation of networks (or the network) irrespective of geographic borders. This interoperability has been enabled largely by global technical standards, yet the current policy environment is increasingly creating barriers to interoperability that threaten to undermine the benefits of these standards. For example, if security and authentication features based on international peer reviewed cryptography ciphers are not allowed in systems deployed in some countries, then global service providers may have great difficulty in enabling parties to adequately authenticate the trustworthiness of international transactions. Driving adoption of a GDI policy helps avoid such interoperability innovation issues, allowing innovators to focus on meeting the needs of the entire GDI.

C. Enabled Economic Growth

Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, irrespective of country of origin, to continue the innovations necessary to drive the GDI, and remain competitive in the global marketplace. At the same time, in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the GDI forward. Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of GDI technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth.

An example of an area where such restrictions are manifesting themselves is encryption laws and regulations. Currently, the U.S., China, Russia and other countries variously impose regulations ranging from limited export controls to import authorization/declaration requirements for ICT products with cryptographic technology to restrictions on distribution, sales and use of such products (including R&D and manufacturing in some cases).[1] Some of these regulations have the impact of requiring the adoption of certain country specific standards and technologies, which run the risk of mandating a particular technology as the innovation that must be deployed. Even the application of more limited encryption export controls by the US is increasingly creating burdens and supply chain instabilities, since the substantial liberalization of the controls a decade ago are now being outpaced by the pervasiveness of encryption capability in ICT products. Such proscriptive technology focused regulations are forcing companies like Intel and its customers to attempt to preserve the ability to functionally disable (fuse off) innovative security technologies in products sold in some countries. If not for these regulations, these security enhancing features would be deployed globally. Fusing off this technology creates portions of the GDI that operate in a less secure environment and over time will frustrate interoperability and international transactions, which will decrease trust in the global free flow of information.

[1] See, e.g., Regulations on the Administration of Commercial Cipher Codes, promulgated and effective as of October 7, 1999, Provisions on the Administration of Production of Commercial Cipher Products, promulgated, and effective as of January 1, 2006, and Provisions on the Administration of Commercial Cipher Research, promulgated, and effective as of January 1, 2006.

III. Identifying Best Practices (Question 2) and International Cooperation (Question 6)

There is a growing recognition amongst policymakers worldwide that the legal and regulatory status quo in the areas of privacy and information security does not provide adequate levels of trust to sustain the GDI. While change seems inevitable due to increasing concerns surrounding cybersecurity, critical infrastructure protection, encryption, and other emerging policy issues, the question is which one of two divergent paths the change will follow: (1) individual countries increasingly and in isolation pass laws endeavoring to "regulate" different aspects of the GDI; or (2) multi-jurisdictional and transborder efforts gain significant traction, leading to some form of extra- or intergovernmental coordination between and cooperation among states in the management of the GDI. Examples of the need for this transborder approach include government desires to access private data, varying definitions of "critical infrastructure", and methods to provide product security assurance that deny market entry to foreign produced products.

The nature of the GDI encourages us to choose the path centered around policy structures and processes that are similarly global in scope and rooted in innovative thinking. Navigating the increasingly confusing and non-harmonized patchwork of global legislation with respect to privacy and security to extract elements common across cultures presents challenges.

Due to the difficulty in creating a global program out of such a patchwork, one useful approach is to continue to look to the high level principles which have gained broad acceptance (albeit to different extents in varying jurisdictions) over the past 40 years, and to how those principles have been applied in some of the major privacy and security legal and policy efforts around the globe. While certain novel transborder processes and structures may be needed to help implement a GDI policy vision, an examination of the current legislative and regulatory environment in privacy and security reveals certain mechanisms that can provide the foundation for a more productive policy environment:

A. Public-Private-NGO Partnerships: The Triangle of Trust

No single entity can achieve the goal of building trust in the GDI; it is clearly a shared responsibility. There is a role for governments, industry, and Non-Governmental Organizations/advocacy groups (NGOs) working together to form a "triangle of trust."

Government should establish the "base" of the Triangle by creating high level compliance principles and rules, and by conducting robust, predictable and harmonized enforcement. Industry comprises one of the "sides," working with government to propose best practices which can allow companies to comply with laws and regulations. NGOs form the final "side," assisting both government and industry to codify industry best practices, handle dispute resolution to free up scarce government enforcement resources for more pressing issues, and to help educate individuals and privacy/information security professionals.

The private sector is poised to be a helpful partner to governments as they build out a GDI-Policy. Governments and industry should work together to develop a policy and regulatory environment informed by the principles of openness, fairness, and flexibility. For there to be "predictable enforcement" of "flexible technology neutral laws and regulations," robust context specific implementation guidance is necessary. Industry best practices can play an important role in developing this enforcement guidance. NGOs can play an important convening role to help document this enforcement guidance. Finally, NGOs can help alleviate overburdened government resources by providing services for the external validation and certification of company programs/practices. To accomplish this goal, government and industry should work together to promote NGOs as indispensible trusted partners in the efficient and trustworthy functioning of the GDI.

Government can also play an important convening role in bringing the necessary parties to the discussion to diligently develop robust and practical best practices, and moving the industry best practice discussions forward. These best practices can then be championed by the US government to other countries as models they should adopt, and then potentially to take the best practices to international standards bodies. Industry efforts to reform Common Criteria provide an excellent example of such a best practices approach to build confidence in the GDI and enable the global free flow of information. NIST is well-situated to play the role of convener in these discussions.

B. Flexible Technology Neutral Laws and Regulations.

Sensible regulation of the GDI need not require the creation of new principles. Ample flexibility exists in many current laws, principles and regulations dealing with aspects of data protection, privacy and security. For example, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows contain a Security Safeguards Principle stating, "Personal data should be protected by reasonable security safeguards." The EU Data Protection Directive contains a similarly flexible Article regarding security, providing Data Controllers "must implement appropriate technical and organizational measures to protect personal data . . . " and should consider "the state of the art and the cost" of security measures. While the U.S. takes a sectoral approach to privacy and information security law, ultimately the approach taken with respect to information security has proven similarly flexible, at least in the sense that U.S. laws in this area are generally not proscriptive.

A common historical thread regarding information security running through the EU Data Protection Directive, OECD guidelines, and U.S. privacy law is the absence of detailed regulations that would mandate or otherwise compel adoption of any one specific technology. This technology neutral approach to regulation allows engineers to do what they do best: solve problems. By describing neutral principles and objectives, global innovators can collaborate on the best way to implement solutions.

C. International Cooperation and Global Standards

Just as the GDI itself is a network of networks –and requires hardware and software working together to create a trusted stack – governments must work together to create a networked regulatory framework – a policy and legal infrastructure which promotes continued innovation and enabled economic growth. In developing solutions to the privacy and security problems threatening the GDI, we should avoid creating geographically siloed regulations that may impede the global interoperability and network connectivity that have spurred the growth of the GDI.

Governments would also be well-advised to avoid taking confrontational action which may provoke country specific regulation. While some coordinated efforts have been carried out such as the effort led by the Spanish Data Protection Agency (which resulted in the Joint Proposal for a Draft of International Standards with regard to the processing of Personal Data), and the Council of Europe's Convention on Cybercrime, additional efforts are needed as more policymakers at various other national governments continue to draft legislation, in areas such as cybersecurity, with little to no attention paid to cross-border realities.

Currently enacted cybersecurity legislation in China (e.g., MLPS), and contemplated regulation in the U.S. and elsewhere shares the common goal of securing the critical infrastructure from cyber threats. Although there is not a common definition of the "critical infrastructure" (CI), as a high-level principle, promoting measures aimed at protecting the most critical elements of the global digital infrastructure should be a component of GDI-Policy. At a finer level of granularity, we can identify commonalities across proposed definitions, and conclude that most definitions of the critical infrastructure must include the power, water, national security, information and finance sectors.

While each country shares a common goal of securing these sectors, many have different ideas of how best to do so. Unfortunately, several countries appear to favor the creation of national standards which may function as barriers to the use of technology developed or manufactured abroad, while it is this new technology which may offer security features which can help provide better protection for the critical infrastructure. More focus needs to be brought on global approaches to securing the infrastructure. Common Criteria has been an effective global tool for this assurance need, and more effort should be spent on understanding what part it can play, and what other global approaches can assist.

D. Accountability Systems.

Private sector companies should work together with all stakeholders - governments, NGOs, and users themselves - in creating and increasing trust. The primary means by which they can do so is by demonstrating accountability, both internal to their organization and to external stakeholders. Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation. Accountability can also play an important role in allowing organizations to demonstrate that their security assurance processes should be trusted.

Though definitions of what is meant by “accountability” vary across these instruments, a useful approximation is the following: “Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.”

But what does accountability mean in practice? We believe that a variety of accountability models can exist for different aspects of privacy and security but in general, such models are comprised of the following elements: 1) commitments which are interpreted from flexible and technology neutral laws, industry best practices and entity specific promises; 2) processes and procedures put in place to deliver on the commitments; 3) attestation by the entity demonstrating how it has fulfilled its commitments; 4) third party mechanisms (either regulators, certification authorities or NGOs) for measuring whether the commitments have been met. Although the focus of such accountability systems seems squarely on corporations, there are clear roles for the government and NGO “sides” of the Triangle of Trust to play here as well.

1. Demonstrating accountability internally

Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization’s ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts into the GDI that have been vetted through processes such as development lifecycles which have privacy and security integrated as foundational elements.

2. Demonstrating accountability externally

Demonstrating accountability externally is equally important and arguably more challenging for corporations and governments alike. Ultimately, regulators are responsible for ensuring that risks have been managed appropriately. This responsibility is why regulators are unlikely to simply defer to industry best practices in this area, but instead should play a role in commenting on global best practices and then in using them as enforcement guidance. Yet due to resource constraints and other factors, governments will still need additional mechanisms to enforce accountability.

Third party certification is one such additional mechanism that has been used previously in the areas of privacy and security. Third party certification mechanisms thus need to comprehend the processes by which an organization is ensuring it is accountable, including processes which check for common problems that may lead to a lack of trust (e.g. checking software code for known vulnerabilities or checking to make certain access controls are set appropriately). More focus should be placed on building global accountability structures for privacy and security. These global structures could greatly increase the trust and confidence in the global free flow of information.

IV. Impact of Restricted Internet Information Flows on Innovation, Trade, and Commerce (Question 3)

One potential impact of restrictive GDI policies is the risk of network fragmentation. The closing of parts of the networks comprising the GDI likely means foreclosing opportunities to develop global solutions, as the development of previously 'open' technological solutions could be blocked by layers of national laws, network operator standards, or other restrictive policies. (e.g., encryption regulations at the local level foreclosing global deployment of certain security technologies). Foreclosing global solutions can increase costs due to the duplication of development resources, and over time takes away resources which could be used to innovate new products, features and services.

While the continued success of the GDI depends upon this fundamental "openness," some rationales for private networks to flourish (i.e., Intranets) will continue to exist. However, the ability for continuity of security and privacy across the Internet is facilitated and strengthened through common building blocks with common security related capabilities, allowing Intel and other IT companies to continue to innovate solutions for security and privacy across the GDI.

V. Trade Agreements (Question 5)

Intel is a strong proponent of free and vigorous trade, which we believe help strengthen American businesses and jobs. While approximately 75% of Intel's manufacturing capacity remains in the U.S., more than 75% of our revenue is generated overseas. The ability to access foreign markets is thus essential to Intel's continued growth and prosperity overall and especially in the U.S. The e-commerce chapters of recent free trade agreements have all contained the fundamentals needed for e-commerce to flourish, including non-discriminatory treatment of foreign digital goods and tariff/duty protection for digital products imported or exported by electronic transmission or fixed on a medium.

We recommend, however, that the Department of Commerce work with the United States Trade Representative to further expand this principle by including in future free trade agreements two additional provisions that would enable global data flow. First, we support a provision expressly allowing the free transfer of data across borders in conjunction with service commitments made by each Party (e.g., computer services), assuming appropriate privacy protections are included. This provision will become increasingly important as countries begin to allow foreign direct investment related to digital services, while at the same time may begin to interfere with associated data flows. Second, we support a provision expressly preventing any requirements to locate IT infrastructure (e.g., servers) within a country as a condition of providing products or services. Efforts to sever treatment of the data from service commitments or to require in-country infrastructure development or manufacturing often have protectionist purposes even when security or privacy concerns are raised; legitimate security and privacy concerns can be addressed in other ways such as through compliance with international standards and certifications.

VI. Conclusion and Recommendations

The data empowered world has brought enormous benefits to businesses, consumers and society as a whole. At the same time, the exponentially growing amount of data being processed on a global scale is accompanied by increased risks. All entities working within the GDI need to innovate solutions to provide security and protect privacy, while at the same time increasing the rate of economic growth and technological innovation. These interests can best be served by focusing policy efforts on the primary technological characteristics that have driven the GDI's growth – openness, interoperability, and enabled economic growth. A more cohesive global digital infrastructure policy should be further developed.

The underpinnings of such a sensible GDI-Policy are already in existence today:

- The ”Triangle of Trust,”
- Flexible technology neutral laws and regulations;
- International cooperation and global standards; and
- Accountability systems.

Yet enabling these GDI-Policy mechanisms in a meaningful and comprehensive way requires continuing the global dialogue between industry, governments and NGOs who are working to address the challenges of building trust in the global digital infrastructure. Collaboratively, we can build meaningful and attestable accountability into our organizational structures, technology development processes, and cooperative efforts and policies. The current environment presents an unprecedented opportunity for technology policy collaboration not only between governments, corporations, and NGOs, but between the technical and policy communities, and between the privacy and security communities.

Intel is committed to fostering these bridging efforts – by continuing to innovate in the technology sphere, by providing the solutions that build trust in the GDI, and by working with other stakeholders to innovate in the policy sphere. We offer up a vision of what we believe the contours of a GDI-Policy should look like in an effort to encourage not only dialogue, but action.

As part of that effort, Intel specifically recommends the following five actions to further the GDI-Policy:

1. Put an end to import, export and use restrictions on cryptography for commercial off the shelf products and public research;

2. Hold international discussions involving all stakeholders in the Triangle of Trust regarding decreasing cyber attacks, with the goal of an intergovernmental accord limiting the proliferation of such attacks;

3. Increase understanding and implementation of accountability practices among public and private sector organizations to an accepted global framework or standard, increase international government funding of NGOs as certifying agencies, and develop robust, harmonized, coordinated and predictable enforcement mechanisms against noncompliant entities;

4. Deepen government/private sector partnerships and international collaboration on cybersecurity research, including increased government funding;

5. Promote the widespread adoption of a unified certification process and global standards for product assurance and product security to ensure a secure platform for the GDI. More specifically, we recommend improving the reliability and cost effectiveness of Common Criteria by adopting a tiered approach to certifications (allowing companies to attest to compliance with an accepted global standard for certain levels of products, and for third parties to verify company attestations), expanding Common Criteria to development processes, and broadening the international mutual recognition of Common Criteria.

Intel again thanks the Department for its leadership on this important issue. We are supportive of the Department playing a role in this debate, and we look forward to continuing our engagement in helping to think about ways to improve the global digital infrastructure and ensure the global free flow of information on the Internet.