August 1, 2011

U.S. Department of Commerce
Cybersecurity and Innovation in the Internet Economy
Docket No. 100721305-0305-01
Via electronic filing: SecurityGreenpaper@nist.gov

Comments of Google Inc.

Google thanks the Department of Commerce for the opportunity to comment on its draft report *Cybersecurity, Innovation and the Internet Economy* (herein "Green Paper"). We support designation of an "Internet and Innovation Infrastructure Sector," distinct from covered critical infrastructure. We welcome the Department's support for voluntary, private sector driven cybersecurity codes, practices, and standards. Going forward, we urge the Department to identify additional safeguards to ensure that such standards remain voluntary, flexible, and free from excessive regulatory overhang. Our comments focus on issues meriting further discussion in the Department's ongoing dialogue with the private sector regarding cybersecurity.

- **Distinguishing the Internet and Innovation Infrastructure Sector ("I3S") from Covered Critical Infrastructure ("CCI") will help preserve the flexibility needed to enhance cybersecurity through innovation.** The Internet has delivered breathtaking benefits to the U.S. economy and American consumers — from search, to email, to social networking and mobile services. Continued innovation is needed to respond to the broad range of dynamic cybersecurity challenges that attend these benefits. Regulating companies that, on the one hand, do not provide critical infrastructure and, on the other hand, are a significant driver of economic growth, entrepreneurship, and vitalization of the economy would be a lose-lose proposition, simultaneously undermining cybersecurity goals and diminishing economic benefits.

- **Voluntary codes of conduct, practices, and standards are the appropriate focus for effective I3S security efforts.** The need to earn and maintain user trust creates powerful incentives for I3S providers to enhance user safety and offer the best possible products and services. Google, for example, has deployed a robust security infrastructure and developed responsible security practices designed to protect our users and to make the Internet a safer place for everyone. Given the constant emergence of new cybersecurity challenges, however, we must remember how quickly today's best practices can become ineffective. So, while flexible standard setting and best practices

development should be promoted, codification of such standards and practices risks undermining cybersecurity by hindering innovation.

- **Meaningful and timely information sharing practices can enhance cybersecurity, but must be carefully designed to respect fundamental civil liberties.** Information sharing protocols that erode civil liberties protections can only undermine consumer confidence, make it harder for U.S. Internet companies to compete in the global marketplace, and ultimately diminish cybersecurity. Enhanced information sharing should focus on enhancing the government's ability to share more information to help the private sector defends its systems.

I. The Internet and Innovation Infrastructure Sector should not be regulated as CCI.

Google commends the Department's efforts to define an "Internet and Information Innovation Sector" or "I3S" that encompasses the private sector's provision of information services and content and that would fall outside the classification of "covered critical infrastructure" or "CCI." We agree that CCI regulation should not apply to private actors in this sector, including those engaged in, for example, the provision of: information, software, services, or content to users via the Internet; intermediary services that facilitate online transactions; content storing or hosting services; or online products and services such as applications, browsers, social networking platforms, search services, online collaboration tools, web mail and other information sharing services. While it may be difficult to create a bright line test for products and services that fall within the proposed I3S category, Google urges the Department to err on the side of innovation and a safer Internet by defining the I3S expansively to encompass the broad array of hardware, software, and services offered by providers participating in this vibrant economic sector.

As a starting point, I3S products and services are quite different from "critical infrastructure," which has been defined in various Federal statutes and regulations, each of which reflect the overriding need to protect core systems and assets essential to national security and public health and safety. For example, Section 1016 of the USA Patriot Act defined the term to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters," including telecommunications networks, energy systems, financial services systems, water supply systems, and transportation networks. In 2003, Homeland Security Presidential Directive 7 described critical infrastructure and key resources activities as the provision of "essential services that underpin American society," and that require protection from acts that could threaten national security; cause mass casualties; weaken our economy through "cascading disruption" of other critical infrastructure, and profoundly damage public morale and confidence.

Because the creation and operation of critical infrastructure systems and assets generally require significant upfront investment in facilities and equipment, and long lead times to deployment, CCI typically involves little redundancy and limited sourcing alternatives. In addition, the pace of

deployment and transformation of critical infrastructure allows time for consensus-building via the regulatory process.

In contrast, I3S activities do not involve the same risks and are ill-suited to regulation as CCI.

First, I3S providers generally *use* third-party network infrastructure and information technology to access and communicate information that is often created or provided by third parties. In conducting these activities, I3S firms may rely on critical infrastructure, but are not themselves CCI providers.

Second, many features of I3S services make them less prone to catastrophic system-wide failure. Data processed in connection with the provision of I3S services is often easily replicated and backed up in real time, and I3S providers rely on a variety of redundancies to protect against systemic disruptions or intrusions. I3S services can be affected by system failures or attacks on critical infrastructure, but absent damage to the infrastructure itself, are often readily restored using backup or redundant systems. And even when there is an extended service outage, other I3S firms are generally positioned and incentivized to provide additional capacity and overflow services.

Third, as the Green Paper recognizes, the pace of technological change in the I3S sphere can be dizzying. I3S services and products can be deployed quickly across existing networks, updated or improved in real time, and often transformed or replaced with little upfront cost (as demonstrated by the I3S firms and services that once appeared to be permanent fixtures of social and economic life only to be quickly overtaken by new offerings or models).

Finally, I3S products and services are simply bad candidates for regulation. Diverting potential resources from the critical infrastructure sphere to the I3S sphere risks muddling government priorities, to the detriment of overall risk mitigation. Moreover, government management and direction in the I3S sector is unlikely to keep pace with the rapid technological change in that sphere. At best, direct regulation of the I3S sector will be slow to adapt to new innovations, and rules will be quickly rendered irrelevant by the next wave of technological change. At worst, close regulatory involvement could impair the very innovation that makes the I3S sector less vulnerable to systemic failure or attack. Google urges the Department to steer clear of prescriptive government involvement in the I3S market that could create a drag on innovation and economic growth in one of the U.S. economy's bright spots.

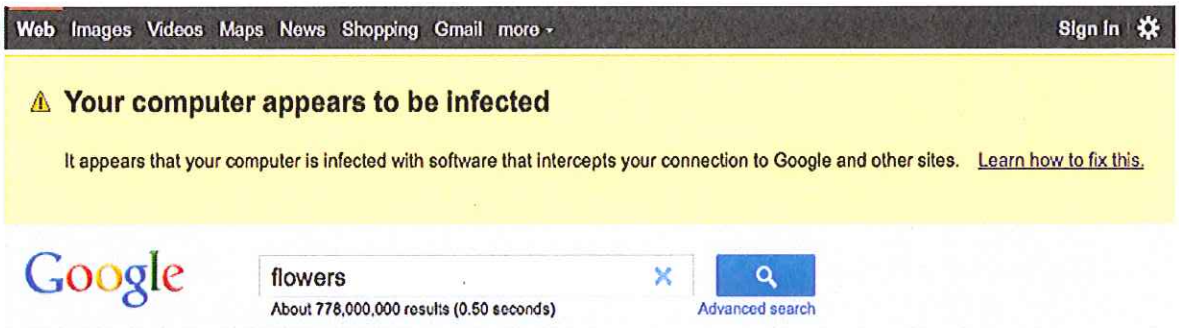
II. Voluntary standards setting and best practices development are enhancing user security without regulation.

The competitive and customer service realities of the I3S environment provide strong incentives for companies like Google to invest in security. To offer the best products and services, to win and keep customer loyalty, and to preserve confidence in the online environment on which our business depends, Google is constantly innovating to offer state of the art security for individual

and enterprise users, and to raise the best practices bar. In doing so, Google strives to leverage the strength of the Internet as a distributed system, a powerful source of important information about emerging threats, and a venue for creative collaboration across the globe. Because our goal is to increase Internet security across the board, Google facilitates free access to security related data and technology (including by its competitors), develops security enhancing tools in an open environment, and publishes these tools subject to open source licenses.

Harnessing Internet Data to Enhance Cybersecurity

As part of providing services to the public, Google analyzes billions of webpages daily for malware and phishing, uses automated detection processes to update information on millions of suspected phishing and malware webpages, and incorporates this information in various Google products. For example, Google delivers warnings about search results pointing to potentially dangerous sites, and Chrome web-browser users receive the same kinds of warnings as they navigate the World Wide Web. Google constantly analyzes this data to identify and respond to new and emerging threats. For example, we recently observed an enormous increase in the use of bulk subdomain services (services that sell third level domain name registrations such as "example.example.com") to distribute malicious software, or "malware." In response, Google modified its systems to identify bulk subdomain services being abused to distribute malware and fake anti-virus programs. Similarly, when we came across unusual network traffic while performing routine maintenance on one of our data centers, our outreach to security engineers at companies that were sending this anomalous traffic enabled Google to determine that their computers were infected with a particular strain of malware. To notify users of computers infected with this particular family of malware, and to help them install or update their antivirus software, Google provides those users with the following notice at the top of their Google web search results:



Other I3S providers are taking similar proactive steps. Comcast's Constant Guard Bot Detection and Notification system, for example, warns Comcast customers whenever malicious viruses are detected, and guides them through the removal process. Internet Service Providers in countries such as Australia, Japan and Germany have done similar work. In some countries, ISPs point users to public-private entities that help users clean their computers. Google encourages the Department

to explore and encourage similar approaches.

Google provides a variety of tools to alert webmasters when their sites are being misused for phishing or malware distribution, and our database of suspected malware and phishing can help website operators recover from third party attacks. Google, together with the Center for Democracy & Technology, PayPal, Mozilla, Nominum, Qualys, Verizon, among others, are supporters of StopBadware, an organization devoted to helping web site operators to remove malware that infects users' computers (www.stopbadware.org). The organization is a good example of private sector initiative in the fast-changing cyber-security environment.

Google uses information to advance Internet security in still other ways. Google's enterprise security offering, Postini, analyzes billions of daily email messages to detect and block threats in real-time. The Google Certificate Catalog is a database of all of the SSL certificates on sites crawled by Google to produce search results, which can be used to warn users about potentially dangerous sites. If a certificate does not appear in our publicly available database, despite being correctly signed by a well-known certificate authority and having a matching domain name, then there may be something suspicious about that certificate. Google is also participating in the Internet Engineering Task Force's Domain Name System (DNS)-based Authentication of Named Entities (DANE) project, intended to allow domain operators to publish information about SSL certificates used on their hosts, and to use these records to specify particular certificates that are valid, or certification authorities that are allowed to sign certificates for those hosts. If a certificate is not consistent with the DANE records, it should be treated with suspicion.

Security Deployment Leadership

Google's Internet security initiatives regularly raise the bar for industry best practices. Alone among major web mail providers, for example, Google has made HTTPS — a secure protocol for authenticated and encrypted communications — the *default setting* for all Gmail users. Last year Google introduced 2-step verification, a two factor authentication feature for Google Apps accounts, requiring enrolled users to enter both a password and a random verification code sent to or generated by a user's mobile device, and earlier this year we made two-factor authentication available to Gmail users. Recently, we made two-factor authentication available in 40 languages and in over 150 countries. Postini uses SSL or TLS protocols to protect sensitive business information in transit, and the Postini-powered Google Message Security delivers enterprise-grade spam and virus protection and email content filtering to enterprise users, helping businesses to secure inbound and outbound messages against email-borne threats, set and enforce central content management policies, and receive email messages even if their mail server is down. We support open standards for email authentication such as DomainKeys Identified Mail (DKIM). Finally, Google recently enabled Postini services customers to authenticate inbound email and to set their own policies for handling suspicious emails.

Because of its open, distributed design, the DNS is vulnerable to various forms of attack including

DNS spoofing, cache poisoning, and denial of service attacks. Last year, Google introduced Google Public DNS as a faster and safer alternative to existing DNS providers. Google Public DNS supports IPv6 and accepts and forwards messages formatted using DNS Security Extensions, a set of extensions to DNS, that provide origin authentication of DNS data, data integrity, and authenticated denial of existence.

Open, Crowd-Sourced Security

Google's Chrome browser is the product of an open-source project, Chromium, to help build a safer, faster, and more stable platform to experience the web and for developing a new generation of web applications. All of the code in the project was open source, and project participants collaborated to build a better browser focused on speed, simplicity, and security. In 2010, the Chromium project launched an incentive program that rewards external researchers who identify and report original vulnerabilities with rewards ranging from $500 to over $3,000. To date, the Chromium project has awarded more than $169,983 to more than 40 researchers who have identified more than 182 discrete medium and high severity bugs. Earlier this year, in connection with the CanSecWest conference, Google challenged security experts to identify vulnerabilities in the Chrome "sandbox" technology, offering a reward ($20,000 and a Chrome notebook) for the first person to successfully hack its code. The Chromium vulnerability reward program has been so successful that we expanded it to cover bugs discovered in connection with any Google web property that displays or manages authenticated user data or accounts including google.com, youtube.com. blogger.com, and orkut.com. This program is inspiring a large, diverse, and talented set of professional technologists and technology enthusiasts to scour our sites for vulnerabilities and report them to us so we can fix them.

Google's open source policies actively encourage broad uptake of security innovations. For example, all of the improvements embodied in the Chrome browser are freely available to anyone with an Internet connection. Likewise, Google Public DNS has made many improvements in the areas of speed, security, and validity of results – all of which are described in free, publicly available documentation.

Innovation without Regulation

The level of innovation described above could not thrive in the context of formal standards development and adherence models of the sort used for CCI. For example, earlier this year, the National Institute of Standards and Technology (NIST) announced its intention to update by year end its 2009 catalog of management, operational, and technical security controls for both national security systems and non-national security systems. While a twenty-eight month update cycle can make sense in some environments, it is not compatible with the kind of innovation regularly deployed by I3S providers to respond to emerging threats in near real time. Similarly, while adherence to the Common Criteria for Information Technology Security Evaluation and

the companion Common Methodology for Information Technology Security Evaluation provide useful global consistency in the CCI context, the certification process is both time-consuming and expensive, and would dramatically hamper the ability of I3S providers to respond to ever-changing security threats. Finally, while standardized identity management systems may provide important assurances in highly sensitive environments, they will take time to develop.

Accordingly, while voluntary self-regulation and voluntary standard setting can enhance cyber security, further safeguards are needed to ensure that "voluntary" cybersecurity standards for the I3S do not become "de facto" regulatory mandates. In the cyber security context, overly prescriptive approaches to disclosures about information security practices or rigid vulnerability reporting mandates could undermine rather than further online safety objectives. Google supports a "rough consensus and running code" approach to I3S cyber security-related standards development. This approach, which dates back to ARPANet and is described in a 2006 Internet Engineering Task Force memo, "The Tao of IETF" (RFC 4677), has served the Internet community well for many years, precisely because it reflects, embraces, and takes full advantage of the power of the distributed nature of the Internet.

Google recognizes the value of documenting practices that have improved security in the I3S sector. Adoption of these practices should remain discretionary for the simple reason that systems in the I3S sector evolve rapidly and the details vary from provider to provider. Google agrees, however, that interoperability among actors in the I3S sector can enhance security and that standards can provide a basis for achieving that objective. Voluntary adoption of interoperability standards should remain discretionary, but NIST can provide useful documentation regarding their utility and effectiveness.

In the I3S setting, the most effective role for government is to facilitate private development of flexible voluntary standards, best practices, and industry norms that serve to reduce cybersecurity risks globally. For example, the government can disseminate useful information about the utility and effectiveness of interoperability standards that promote cybersecurity. The U.S. government should not, however, manage "national" standards setting activities or set standards for the private I3S sector. It should instead support continued international private-sector standards setting activities that allow I3S industry norms to evolve and adapt to new security challenges. The government can also support these efforts through additional dialogue, greater information sharing, and actively encouraging governments around the world to look to the private sector rather than regulation for leadership in responding to cyber security challenges facing I3S providers.

III. Information Sharing, Research, Development, and Education

Google agrees with the Department that more and better information sharing is needed to enhance cybersecurity. To this end, Google actively contributes to and participates in the US-CERT. Likewise, Google is committed to disclosing security vulnerabilities in a timely manner and

encourages the industry to fix high-severity vulnerabilities within sixty (60) days.

But we also think that information sharing procedures and mechanisms will ultimately fail unless they are transparent, effective, timely, and protect users from unwarranted government intrusion into their private affairs. Information sharing that erodes civil liberties or routes around the Wiretap Act or the Electronic Communications Privacy Act would put U.S. I3S players at a competitive disadvantage globally and, by constraining resources these companies would otherwise have to support innovation, undermine the very cybersecurity goals we wish to achieve. In particular, the government should not function as the system's "traffic cop" by controlling the flow of information between and among private-sector participants, nor should it eliminate meaningful accountability for clear abuses in the collection, disclosure, and use of this information. Rather, mechanisms to support information sharing about cybersecurity threats should be both voluntary and private-sector managed and operated, require continued adherence to electronic surveillance statutes (except to the extent relevant statutes would preclude disclosures about specific attacks and malicious code), and involve sufficient transparency to make it possible for the public to be informed about the amount and nature of information that is shared. Further, such systems should enable the government to share technical vulnerability information for use by the private sector in connection with research and development and for incident prevention and detection.

Ultimately, of course, effective cyber security depends upon informed and educated Internet users. As Deputy Secretary Jane Lute and Bruce McConnell of the Department of Homeland Security put it, "If the U.S. is to succeed in securing our identities and our information in cyberspace, it must build a system where the distributed nature of cyberspace is used for its own protection." (Op-Ed 2/14/2011). In order to harness the strength of the Internet to this end, everyone — individual users, small business operators, and the biggest publicly traded companies — must become more aware of, savvy about, and engaged in cybersecurity efforts.

Google's Cyber Security Awareness channel on YouTube is designed to build such awareness across the web community through educational videos created by users, non-profit groups, businesses, schools, and government agencies. Google's Online Security Blog provides regular news and updates about cybersecurity threats, safety tips, and security tools for users, developers, and webmasters. We also actively participate in the Stop. Think. Connect.™ campaign, a coordinated messaging campaign, created by an unprecedented coalition of private companies, nonprofits and government organizations to help all digital citizens stay safer and more secure online. The campaign hopes to achieve for online safety awareness what "Smokey Bear" did for forest fire safety and "Click It or Ticket" did for seatbelt safety.

Google also welcomes the Green Paper's support for cybersecurity-related research and development, which Google actively supports through grants and awards, faculty summits, visiting faculty programs, and publications. We continue to believe that more can and must be done in this area. As stated in our comments to the Department's Notice of Inquiry, *Cybersecurity, Innovation*

and the Internet Economy, R&D is needed to improve user interfaces, better empower users to protect themselves, and make security tools and notices accessible to all users in a meaningful and readily understandable way. To this end, Google has also partnered with Maryland Cybersecurity Center, a multidisciplinary initiative at the University of Maryland aimed at research, education, and technology development in cybersecurity, to produce six seminars per year examining a broad range of topics related to cybersecurity, including technology, policy, and economics. We also want to reiterate our call for the Department of Commerce to support the creation of a "Grand Challenge for Cybersecurity" — similar to the National Academy of Engineering's Grand Challenge for Engineering — in order to stimulate interest and progress in cybersecurity research and development. By establishing an ambitious but attainable goal with a mix of incentives, such a challenge could attract the best minds in both the private and public sectors. For example, an ongoing challenge with annual progress prizes, an additional grand prize, open-sourced results (e.g., published papers and disclosure of successful steps forward), and public recognition of the participants and their respective success could create a virtuous cycle of innovation and competition in this space. Google would welcome such a system and the opportunity to provide additional information on how such a system could operate.

Google also commends research efforts by the Defense Advanced Research Projects Agency (DARPA) that seek to move us beyond "just treading water" when it comes to cybersecurity. As stated by DARPA's Director, Dr. Regina E. Dugan, in March while testifying before Congress:

> Over the last 20 years, using lines of code as a proxy and relative measure, the effort and cost of information security software has grown exponentially — from software packages with thousands of lines of code to packages with nearly 10 million lines of code. By contrast, over that same period, and across roughly 9,000 examples of malware — viruses, worms, exploits and bots — our analysis revealed a nearly constant, average 125 lines of code for malware. This is a striking illustration of why it is easier to play offense than defense in cyber, but importantly, it also causes us to rethink our approach. To seek new approaches that might lead to convergence.

Google encourages the Department to support approaches similar to DARPA's "Cyber Fast Track" program, which seeks to harness non-traditional sources of cybersecurity expertise in order to more rapidly and inexpensively close the gap between attackers and defenders online.

Finally, Google applauds the Green Paper's recognition of the importance of international collaboration on cybersecurity issues, and urges the Department to provide leadership in this area. By avoiding excessive and unnecessary regulation of Internet activity, the U.S. government encouraged the innovation that, in the course of a few short years, transformed the Internet from a limited tool for government and academic research into a platform for global commerce, social networking, political engagement, and individual creativity. Complex or rigid regulatory regimes, including those based on technological mandates, would thwart the development of new services

and tools by I3S players, make the Internet a less robust medium, and make U.S. Internet companies less competitive globally. Google believes that the Department of Commerce can play a critical role in promoting international collaboration on cybersecurity issues and in promoting a global approach to cybersecurity issues that facilitates and rewards innovation.

***

Google appreciates the opportunity to share its perspectives and experience and we look forward to working with the Department as it continues its important efforts on cybersecurity.

Sincerely,

Alan Davidson
Director, Public Policy
Google Inc.