**September 20, 2010**

**U.S. Department of Commerce**
**Docket No. 100721305-0305-01**
**Cybersecurity and Innovation in the Internet Economy**

## Comments of Google Inc.

Google thanks the Department of Commerce for the timely and important Notice of Inquiry on improving cybersecurity while sustaining innovation.

The Internet has brought considerable social and economic benefit to the United States and the world. Notwithstanding the great benefits created by the Internet – and sometimes because of those very benefits – consumers face a broad range of cybersecurity challenges, ranging from hackers infecting computers with malware to poor cyber "hygiene" such as the use of weak passwords. In response, Google is engaged in its own and several industry efforts to educate consumers about how to protect themselves online and to develop tools that enhance the security of the web.

In our quickly evolving business environment, ensuring that we earn and keep our users' trust is essential to building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protecting the privacy of our users' personal information. The bedrock of Google's privacy practices are three design fundamentals: transparency, choice, and security. Security is paramount to Google and, to that end, we have implemented a sound security infrastructure and responsible security practices.

We appreciate the opportunity to provide comments on the NOI. Our comments are focused on raising awareness, website and component security, authentication and identity management, and cybersecurity research and development.

## Raising Awareness

Raising consumer awareness of security on the Internet is critical to ensuring that the Internet remains the powerful communications medium that it is today. Google's approach to education on this front has been to focus on accessible, positive, and action-oriented messages coupled with making tools available to empower consumers.

Our education efforts start with our users, through security-focused blog posts and security-related tips embedded in our products. For example, in addition to various blog posts on privacy and security, we also publish the Google Online Security blog, which is wholly dedicated to the security and safety of users of Google's products. Today, for example, we published a blog post on the critical importance of passwords in the security chain. We also make sure to remind our users of security features that are available to them when using our products.

We have also undertaken several educational projects in partnership with other companies to educate the larger Internet Community about cybersecurity. For example, Google is a strong supporter of the National Cyber Security Alliance. NCSA's mission is empowering individuals and organizations through education about how to use the Internet safely and securely at home, work, and school. Among other things, NCSA builds strong public-private partnerships to create and implement broad-reaching education and awareness efforts, and makes available tools and other resources to help individuals, small businesses, and others protect themselves online.

Google is also a co-founder of StopBadware.org, which hosts the Search Badware Website Clearinghouse, a searchable database of badware URLs that is voluntarily submitted by StopBadware's partners, sponsors, and data providers. StopBadware uses the data to analyze and report trends in web-based infections, provide the public with research tools such as the Top 50 Networks list, and assist web hosting companies and other network providers with identifying badware sites on their networks. Importantly, StopBadware takes a proactive, preventive approach rather than leaving users to react after their system has already been infected.

In terms of specific awareness campaigns, Google is working with a coalition of industry leaders, nonprofits, and government agencies to develop a unified public awareness message to help all Americans stay safer and more secure online. The message – "Stop. Think. Connect." – will be introduced to the public in October as part of National Cyber Security Awareness Month.

In addition to Google's own efforts – individually and with industry partners – to build cybersecurity awareness, we are supportive of government efforts to help educate consumers about how to be safe online. For example, we applaud the Federal Trade Commission's OnGuardOnline.org site. This site, a collaboration with various government agencies and private organizations, including the Department, helps even the most novice Internet users understand basic, important online security measures. The site even has simple games and videos aimed at children and teens. OnGuardOnline presents a valuable model for broad-based consumer security education.

Empowering consumers and other stakeholders about how to protect themselves online is a key component to an effective cybersecurity strategy. We also believe that information sharing should be part of the overall awareness effort.

The Department's NOI asks about the importance of increasing information sharing and asks specifically whether the government should create a cybersecurity service center. Google believes that sharing information about security threats – including sharing with users – is critically important. We have begun to make progress in that regard by sharing data about security threats with other private sector entities, government, and academia. Through our support for and collaboration with NCSA, independent research, and participation in federal government initiatives (such as US-CERT), Google actively seeks to add to the repository of knowledge about security threats.

With that in mind, we encourage the Department to continue exploring the concept of a cybersecurity service center as a means of assisting the business community in implementing protection measures, sharing information about cyber threats reported by businesses and other sources, and dealing with cybersecurity incidents that occur. We believe that this service center concept merits further exploration. The service center could build on the National Institute of Standards and Technology's work in this area and complement existing efforts such as US-CERT's information sharing program. Ideally, such a center would serve to coordinate the flow of information and provision of responses to cyber-emergencies among government entities and the private sector. However, the center should not duplicate existing federal efforts and should be a service available on a voluntary basis as a means to encourage informal cooperation between the public and private sectors.

## Website and Component Security

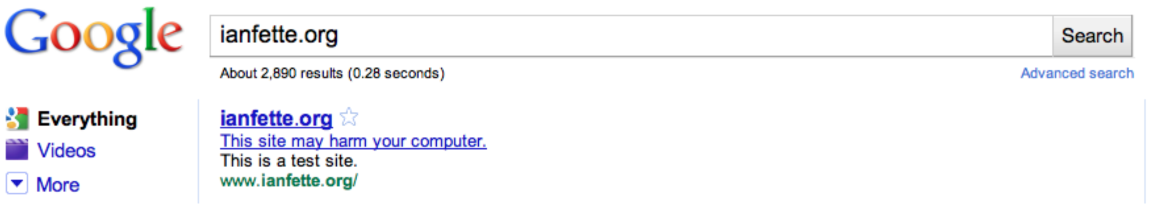
In addition to providing user education, Google also works to build security features into many of our products to make it easier for our users to use the Internet safely and securely.

### *Website Security*

Google is committed to building security measures and features into its products as well as sharing its insight about some of today's most pressing security concerns. The contents of any particular website are only as secure as the set of applications used to deliver the content, including the actual HTTP server and scripting applications such as PHP and ASP. In 2007, a group of Google anti-malware engineers conducted a seminal year-long study of one of the fastest growing threats to users online – web-based malware infections – and presented their findings in a white paper entitled *The Ghost in the Browser: Analysis of Web-Based Malware*. Although the study observed a variety of web server compromises, the most common infection vector was via scripting applications. Any websites that allow user-inserted content are potentially subject to HTML exploits, which can expose all visitors to attack.

Given this type of malware threat, the Department's questions in the NOI on third-party verification of website security are timely. Google believes that this is an issue best led by the private sector. Already, many private sector actors are responding and adapting to a complex and evolving threat environment, and it is important that private sector actors continue their innovation in a flexible environment that allows individual companies and other private sector entities to respond quickly and effectively to evolving challenges.

One example of private sector innovation is Google's Safe Browsing data. Google analyzes billions of pages daily for malware and phishing. For example, we automate our phishing detection process, which looks for certain telltale signs that a page is designed for phishing. Google's Safe Browsing data is constantly updated and contains millions of suspected phishing and malware pages. This data is incorporated into various Google products, including Google ad properties, to protect users and is shared at no cost with third parties via Google's Safe Browsing Application Programming Interface. For example, we use the Safe Browsing data to warn users of dangerous sites included in our search index, as in the example below.

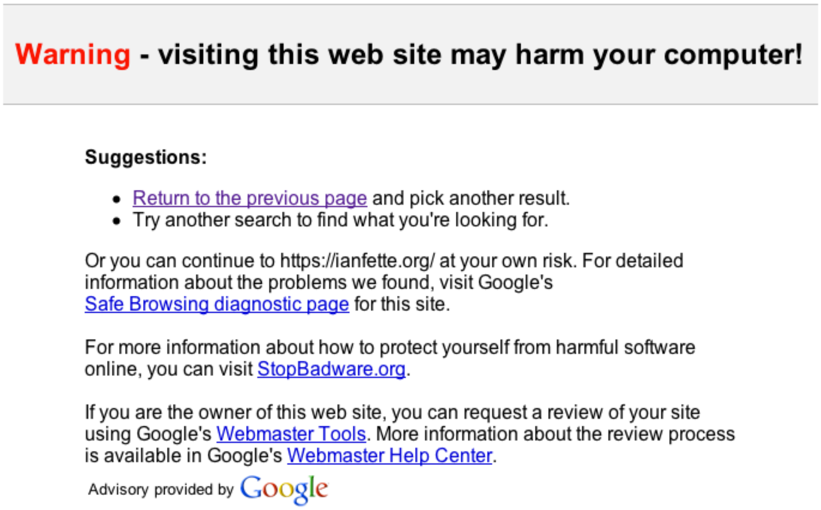


ianfette.org

About 2,890 results (0.28 seconds)

ianfette.org ☆
This site may harm your computer.
This is a test site.
www.ianfette.org/

If users attempt to click through to a suspected dangerous site, they will see a "hard stop" interstitial page that again reminds them of the threat.



Warning - visiting this web site may harm your computer!

**Suggestions:**

- Return to the previous page and pick another result.
- Try another search to find what you're looking for.

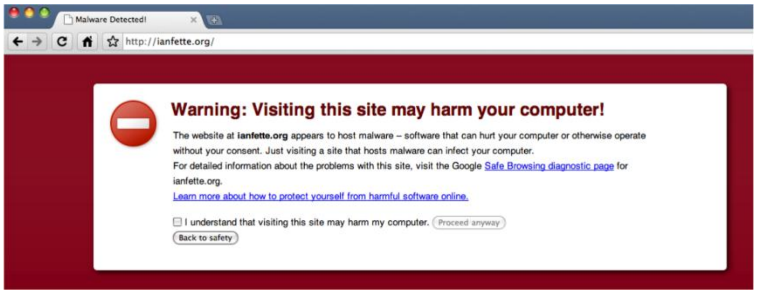
Or you can continue to https://ianfette.org/ at your own risk. For detailed information about the problems we found, visit Google's Safe Browsing diagnostic page for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this web site, you can request a review of your site using Google's Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Advisory provided by Google

Similarly, Google's Chrome browser uses Safe Browsing data to alert users if a webpage they are about to visit is associated with suspected phishing attacks or malware.



Warning: Visiting this site may harm your computer!

The website at **ianfette.org** appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that hosts malware can infect your computer.

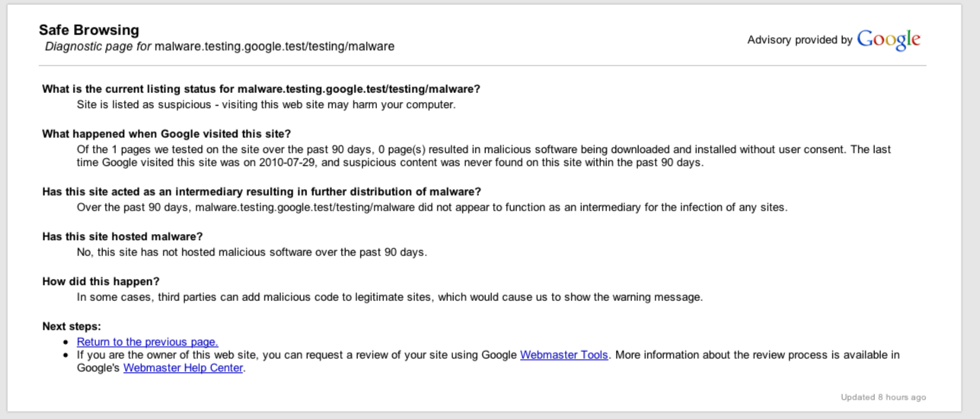
For detailed information about the problems with this site, visit the Google Safe Browsing diagnostic page for ianfette.org.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer. Proceed anyway

Back to safety

Google provides a free Safe Browsing diagnostic page (see below) that allows users to check the history of malware associated with a specific URL.  This page also helps webmasters clean up their sites after they have been compromised.   In addition, our Webmaster Tools feature of Google Webmaster Tools provides additional information to verified site owners.



**Safe Browsing**
*Diagnostic page for* malware.testing.google.test/testing/malware

Advisory provided by Google

**What is the current listing status for malware.testing.google.test/testing/malware?**
Site is listed as suspicious - visiting this web site may harm your computer.

**What happened when Google visited this site?**
Of the 1 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2010-07-29, and suspicious content was never found on this site within the past 90 days.

**Has this site acted as an intermediary resulting in further distribution of malware?**
Over the past 90 days, malware.testing.google.test/testing/malware did not appear to function as an intermediary for the infection of any sites.

**Has this site hosted malware?**
No, this site has not hosted malicious software over the past 90 days.

**How did this happen?**
In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

**Next steps:**
- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 8 hours ago

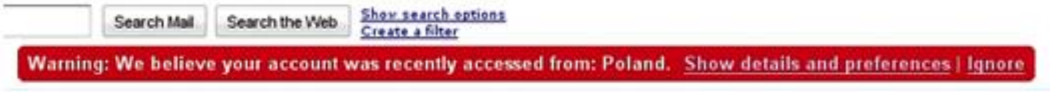
Efforts such as these are intended to make the Internet safer for everyone.  Most websites found to contain malware are sites that have been compromised by third parties and not by their operators; most webmasters did not even know their sites were installing malware on their users' computers before receiving an infection warning.  We use our data to help site owners understand how their sites have been attacked so they can fix the site and protect their users.

Google's Safe Browsing protocol enables third party applications to access our malware and phishing site data for free.  For example, both the Firefox and Safari browsers use our Safe Browsing API data to warn users of suspected dangerous sites.

### *E-mail Security*

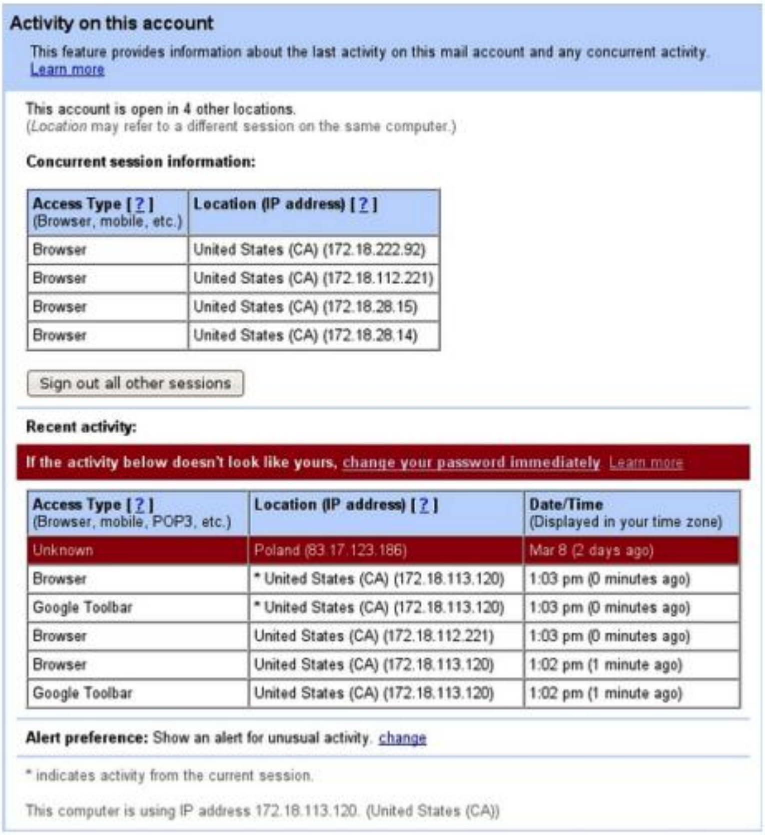
E-mail spam and the spyware and viruses that spam messages often contain are very significant security threats. By some estimates, spam e-mails account for as much as 90 percent of all e-mail traffic, and 20 percent of spam e-mails carry malware. To combat this threat, Google has developed an industry-leading spam and virus filtering engine that is built into Gmail.  Google also provides enterprise-level services by Postini for Google Apps customers or businesses with their own standalone e-mail environments. As a cloud service, Postini can be used without installing costly hardware or infrastructure. Postini also allows system administrators to set important controls and provides "set and forget" protections such as automatically encrypting e-mails to other businesses or government organizations.

Another e-mail security tool Google provides free of charge is the "Last Account Activity" feature for Gmail, which allows users to monitor their accounts for unusual activity by checking from which IP address their accounts have been accessed. If a user notices an unfamiliar IP address, the user can sign out of all other Gmail sessions. When possible, Gmail will also proactively detect suspicious account activity and alert users.



Warning: We believe your account was recently accessed from: Poland. Show details and preferences | Ignore

To determine when to display this message, our automated system matches the relevant IP address, logged per the Gmail privacy policy, to a broad geographical location. While Google does not have the capability to determine the specific location from which an account is accessed, a login appearing to come from one country and occurring a few hours after a login from another country may trigger an alert. Below is a sample of the last account activity alerting users. If a user thinks her account has been compromised, she can change her password from the same window. Or, if she believes it was legitimate access, she can click "Dismiss" to remove the message.



Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account is open in 4 other locations.
(*Location* may refer to a different session on the same computer.)

**Concurrent session information:**

| Access Type [ ? ]<br>(Browser, mobile, etc.) | Location (IP address) [ ? ] |
|---|---|
| Browser | United States (CA) (172.18.222.92) |
| Browser | United States (CA) (172.18.112.221) |
| Browser | United States (CA) (172.18.28.15) |
| Browser | United States (CA) (172.18.28.14) |

**Recent activity:**

If the activity below doesn't look like yours, change your password immediately Learn more

| Access Type [ ? ]<br>(Browser, mobile, POP3, etc.) | Location (IP address) [ ? ] | Date/Time<br>(Displayed in your time zone) |
|---|---|---|
| Unknown | Poland (83.17.123.186) | Mar 8 (2 days ago) |
| Browser | * United States (CA) (172.18.113.120) | 1:03 pm (0 minutes ago) |
| Google Toolbar | * United States (CA) (172.18.113.120) | 1:03 pm (0 minutes ago) |
| Browser | United States (CA) (172.18.112.221) | 1:03 pm (0 minutes ago) |
| Browser | United States (CA) (172.18.113.120) | 1:02 pm (1 minute ago) |
| Google Toolbar | United States (CA) (172.18.113.120) | 1:02 pm (1 minute ago) |

**Alert preference:** Show an alert for unusual activity. change

* indicates activity from the current session.

This computer is using IP address 172.18.113.120. (United States (CA))

Google also supports e-mail security by making "Always use https" the default option for Gmail accounts.  HTTPS, or Hypertext Transfer Protocol Secure, is a secure protocol that provides authenticated and encrypted communication, helping to protect data from being snooped by third parties that might have access to the network. If a user trusts the security of her network and does not want default HTTPS turned on for performance reasons, the user can turn it off at any time by choosing "Don't always use https" from the Settings menu. Gmail will still always encrypt the login page to protect the user's password.  We are not aware of any other major provider of free webmail that has given all of its users the option of turning on HTTPS by default.

### *Operating System Security*

Google develops all of its products with security in mind. For example, last year, Google announced the Chromium Operating System (Google Chrome OS), an open source operating system which strives to protect against attackers through a combination of sandboxing, system hardening, process isolation, continued web security improvements in Chromium, secure auto-update, verified boot, encryption, and intuitive account management.  One key goal of Chrome OS is that, should either the operating system or the user detect that the system has been compromised, the system will warn the user and attempt to return to a known good state using a backup copy. In the rare event that the backup too has been corrupted, the user will be able to get back to a good state using a recovery disk image downloaded from our website.

## Authentication/Identity Management

One of the major areas of focus in the security community has been finding sophisticated ways to reduce the incidence of intrusions and attacks by improving authentication systems and identity management tools.  Google has been part of these efforts, and has worked on two efforts dedicated primarily to phishing and the reduction of vulnerabilities posed by password re-use across websites.

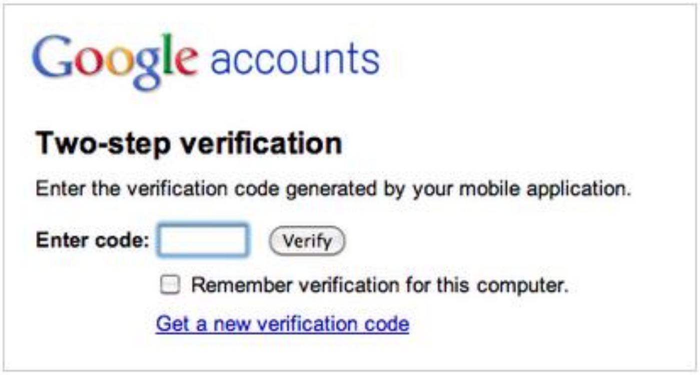
### *Authentication and Phishing*

For some time, Google has been working on improvements to log-in systems, and today we unveiled an option to add two-factor authentication to Google Apps accounts.  Strengthening authentication is critical to reducing phishing and other attacks by reducing the instances of unauthorized account access.

With two-factor authentication, Google will send a verification code to a user's phone, or let the user generate one herself using an application on Android, BlackBerry, or iPhone devices.  Entering this code, in addition to a normal password, gives us a strong indication that the person signing in is actually the person who owns the account.

This new feature significantly improves the security of a user's Google Account, as it requires not only something the user knows – username and password – but also something that only the user should have: her mobile phone. Even if someone has stolen a user's password, the unauthorized individual will need more than that to access the Google Account.

Google's two-step verification is built on an open standard designed to allow integration with other vendors' authentication technologies in the future. We are also open sourcing our mobile authentication app so that companies can customize it as they see fit.  Our feature is based on an industry standard called Open Authentication – or OATH – for the use of one-time passwords.



Two-step verification

Enter the verification code generated by your mobile application.

□ Remember verification for this computer.

### *Password Re-Use*

The other area of focus is password re-use.  Most users reuse the same password and e-mail address to log into multiple websites.  Once a hacker compromises any of those websites, he can then break into the user's accounts on other websites.

The security industry is working to address this threat through standards, such as OpenID and SAML, that allow websites to eliminate the need for a password and instead redirect the user to another website that acts as her identity provider.  Those identity providers have more expertise and advanced systems to handle user authentication securely.

To help websites evaluate the security of those identity providers, the industry created a certification organization called the Open Identity Exchange (OIX), which defines a process for auditors to evaluate whether an identity provider meets a certification profile.  The U.S. Government's Identity, Credential and Access Management Subcommittee (ICAM), co-chaired by the Department of Defense and the General Services Administration, has already defined such a certification profile for identity providers that can be used to enable U.S. citizens to log in to certain classes of government-operated websites.  Google was one of the first such identity providers to be certified.

OAuth (not to be confused with OATH, which is referenced above), defines a more user-friendly way to sign in to applications that run outside a browser (such as set-top boxes or installed applications on a mobile phone).  OAuth can also provide restricted delegated access to resources belonging to the user, rather than giving away her login credentials to a third party that wants to provide services that utilize those resources.

## Research and Development

Google applauds the Department's recognition of the importance of research and development in cybersecurity and has engaged in this area through research awards, faculty summits, visiting faculty programs, and publications. Indeed, Google's most recent faculty summit, *Cloud Computing, Security and Privacy, and the Social Web*, explored issues the Department highlights in its NOI. While many within government, industry, and academia pay considerable attention to promoting and undertaking research and development initiatives, Google believes more can be done.

### *Research to Improve User Interfaces*

Improvement of user interfaces is one area in which research and development could be especially fruitful in empowering users to protect themselves. Many security concerns result from UI weaknesses rather than bad code. Too often, there is a mismatch between what the user believes she is seeing online and what is actually appearing on her screen. A simple example is that, when the UI shows that mail is coming from a user's bank, the e-mail may actually have originated elsewhere, and the user has no easy way of verifying the e-mail's origin.

The methods currently used to alert users to potential security problems are often ineffective, and methods to protect oneself prove difficult for the typical user to put into practice. Despite the fact that PGP has existed for over a decade and can be used to encrypt and authenticate e-mail communication, few average users take advantage of this tool today because of the associated usability challenge. (See the research paper *Why Johnny Can't Encrypt* by Alma Whitten, Google's Privacy Engineering Lead, for an exploration of these issues.) Further research is required to develop effective ways of making these security tools and notices accessible to all users in a meaningful and readily understandable way.

### *Creation of a Cybersecurity Challenge*

The Department should consider supporting 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 thanks the Department for this opportunity to comment and urges the Department's continued involvement in the cybersecurity space. The Internet will drive the U.S. and world economies for years to come. Just as the Department showed global leadership in early Internet regulatory policy, it should lead in encouraging cybersecurity.

Google stands ready to assist the Department in its efforts to help develop and implement a policy framework for cybersecurity that protects commerce and promotes innovation. Should you have any follow up questions or comments, please contact Harry Wingo, Senior Policy Counsel for Google, at 202.346.1275 or at hwingo@google.com.

Sincerely,

Pablo L. Chavez
*Director of Public Policy*
*Google Inc.*