



Prepared Testimony and
Statement for the Record of

Brian Tillett
Chief Security Strategist
Public Sector
Symantec Corporation

Hearing on

Cybersecurity: Threats to the Financial Sector

Before the

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

September 14, 2011

2128 Rayburn House Office Building

INTRODUCTION

Chairman Capito, Ranking Member Maloney, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers cybersecurity and threats to the financial sector.

My name is Brian Tillett, and I am the Chief Security Strategist for Symantec's Public Sector group, where I am responsible for the creation, dissemination and execution of security policy for the public sector team. I have been in the security and information technology fields for 18 years, beginning with my service in the U.S. Air Force, where I was assigned to the Air Force Pentagon Communications Agency and ultimately managed the Pentagon Secure Cryptographic Telecommunications Facility. As an engineer, I have also worked for a number of technology companies. I am in my fourth year at Symantec where I spend the majority of my time with government and industry partners collaborating to understand and address real world cyber threats around the globe.

Symantec¹ is the world's information security leader with over 25 years of experience in developing Internet security technology. Today we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. In short, if there is a class of threat on the Internet, Symantec knows about it.

At Symantec, we are committed to assuring the security, availability, and integrity of our customers' information and the protection of critical infrastructure is a top priority for us. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure critical financial systems from cyber attack. In my testimony today, I will provide the Committee with:

- our latest analysis of the threat landscape as detailed in the Symantec Internet Security Threat Report Volume XVI (ISTR XVI) and in the 2011 Norton Cybercrime Report;
- an assessment of threats to the financial sector; and
- risk mitigation measures for addressing the threat.

¹ Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

THREAT LANDSCAPE

The threats we face are constantly evolving, and it is our goal to ensure that we are thinking ten steps ahead of the attackers. Looking at the current threat landscape is not enough – we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report Volume XVI, we observed significant changes to the threat landscape in 2010.² The volume and sophistication of threat activity increased more than 19 percent over 2009, with Symantec identifying more than 286 million unique variations of malicious software or malware. These included threats to social networking sites and users, mobile devices, and phishing.

However, to understand the evolving threat landscape, we first need to look at who is behind the vast array of cyber attacks that we are seeing today. Attacks originate from a range of individuals and organizations, with a wide variety of motivations and intended consequences. Attackers can include hackers (both individual and organized gangs), cybercriminals (from petty operators to organized syndicates), cyber spies (industrial and nation state), and “hacktivists” (with a specific political or social agenda). Consequences can also take many forms, from stealing resources and information, to extorting money, to outright destruction of information systems.

It is also important to recognize that attackers have no boundaries when it comes to their intended victims. All organizations and individuals are potential targets. Corporate enterprises are often the object of targeted attacks not only to steal customer data and intellectual property, but also to disrupt business processes and commerce. Small businesses are often less resilient and the impacts of stolen bank accounts and business disruption can be catastrophic in a very short time frame. In addition, end-users or consumers are confronted with the financial and disruptive impacts of identity theft, scams, and system clean-ups, not to mention the lost productivity and frustration of restoring their accounts. Finally, governments are most often the victims of cyber sabotage, cyber espionage, and hactivism, all of which can have significant national security implications.

Over the years, we have observed an ominous change that has swept across the Internet. The threat landscape once dominated by worms and viruses developed by irresponsible hackers is now being ruled by a new breed of cybercriminals. Cybercrime has many facets and occurs in a variety of scenarios, using a variety of methods. As more people have access to technology, criminals leverage it for criminal purposes. Just last week we released our 2011 Norton Cybercrime Report where we examined online behavior in 24 countries and interviewed nearly 20,000 consumers. We calculated the cost of global cybercrime at \$114 billion annually.³ We also calculated that lost time due to recovery and impact on personal lives was an additional \$274 billion worldwide. Further, we found that more than two-thirds of online adults (69 percent) have been a victim of cybercrime in their lifetime. Every second, 14 adults become a victim of cybercrime, resulting in more than one million cybercrime victims every day⁴. These numbers are astounding.

² Symantec Internet Security Threat Report XVI, April 2011. <http://www.symantec.com/business/threatreport/index.jsp>

³ 2011 Norton Cybercrime Report. www.norton.com/cybercrimereport

⁴Id.

With an estimated 431 million adult victims globally in the past year, and at an annual combined cost of \$388 billion globally based on financial losses and time lost, cybercrime costs are significantly more than the global black market in marijuana, cocaine and heroin combined (\$288 billion).⁵

It is not just our computers that we need to secure from cybercriminals. Today, a high percentage of consumers use their mobile phones to conduct nearly every aspect of their life, from basic communication to online shopping to mobile banking. Most of these phones are not secure. The Norton Cybercrime Report revealed that 10 percent of adults online have experienced cybercrime on their mobile phone. Further, we reported in the Symantec ISTR XVI that there were 42 percent more mobile vulnerabilities in 2010 compared to 2009 – a sign that cybercriminals are starting to focus their efforts on the mobile space.

Recently, there has been an up-swing in press reports regarding cyber attacks and the “advanced persistent threat” or APT. While APT is one of the most overused terms in the security industry today, it is nevertheless something to be taken seriously. APTs covertly infiltrate systems and hide and wait for opportune moments to steal information or damage systems.

The APT is not one entity; rather it is many different and independent entities, with a tremendous range of motivations for their endeavors. Some of these motivations include financial gain, exfiltration of sensitive and personal information, cyber espionage, and a new turn in the last 18 months, cyber sabotage as exemplified by the Stuxnet malware.

Another trait of the APT is to infiltrate a system, enterprise, or organization, but not immediately execute the ultimate mission. Often the APT will lie in wait, gaining intelligence, observing patterns, and use this information to glean information to further refine the ultimate attack. The APT will even go so far as to patch systems that it finds are un-patched or vulnerable to other attacks. This is done for several reasons, including to ensure that no one else within the targeted organization finds the vulnerability or path that the APT took to get into the enterprise or system; and to make sure that no other APT or other outside rogue entity can exploit the same vulnerability or path into the enterprise.

The threats we are seeing are not new, they are just newly packaged. However, while the attacks are not new, they are becoming more targeted and the monetary losses have grown exponentially.

THREATS TO THE FINANCIAL SECTOR

We have been monitoring an array of threats to the financial sector for many years, and some of the trends we have identified are associated directly with cybercrime, ATM heists, fraud, and Banking Trojans. As observed in the ISTR XVI, the financial sector was the top sector in 2010 for identities exposed in data breaches, with 23 percent—although this was a dramatic decrease from 60 percent in 2009.⁶ It is forecasted that these threats will only continue to mature and increase as society becomes more dependent on using IT for financial and banking needs. Further, with the proliferation of mobile devices -- note that 35 percent of American adults now use smartphones -- mobile banking is expected to increase significantly, as well as the threats targeted at mobile users.⁷

⁵ *Id.*

⁶ Symantec Internet Security Threat Report XVI, April 2011. <http://www.symantec.com/business/threatreport/index.jsp>

⁷ Smart Phone Adoption & Usage, Pew Internet & Life Project, Aaron Smith, <http://pewinternet.org/Reports/2011/Smartphones.aspx>

- **Botnets**

A botnet is group of computers which have been compromised and brought under the control of an individual. The individual uses malware installed on the compromised computers to launch denial-of-service attacks, send spam, or perpetrate other malicious acts.⁸

One such botnet targeting the financial services industry is called “Qakbot”. It is a sophisticated worm that has been spreading through network shares, removable drives, and infected web pages, and infecting computers since mid-2009. Its primary purpose is to steal online bank account information from compromised computers. The malware controllers use the stolen information to access client accounts within various financial service websites with the intent of moving currency to accounts from which they can withdraw funds. It employs a classic keylogger, (software that monitors and captures everything a user types into a computer keyboard) but it is unique in that it also steals active session authentication tokens and then piggy backs on the existing online banking sessions. It then quickly uses that information for malicious purposes.

One of the most important attributes of Qakbot is that it is not focused on the financial institutions themselves, but rather the consumer and their individual financial transaction sessions. It is aimed at infecting and exploiting as many individual consumer transactions as possible. Financial institutions are doing their due diligence with security technologies to thwart this malware from infecting their internal systems. It is the consumer and their mobile and other devices that are vulnerable to this threat.

With more and more users performing financial transactions online on a regular basis, the underground malware society is ramping up efforts to profit from this huge consumer base. Information-stealing malware continues to be prevalent; however, very few have shown the sophistication and continued evolution presented by Qakbot. Analysis of a recent version of Qakbot shows that this malware can result in significant monetary loss for infected networks. By capturing and sending session information to the malware controllers in real time, the malware authors are able to extend legitimate online sessions, gain quick and comprehensive access to end-user bank accounts, and make transfers without giving the banks much reason to believe something is amiss.

Based on the changes observed in the recent Qakbot version, we expect continued evolution of the threat, along with additional changes to the list of targeted financial institutions. We have already seen additions made that would enable the malware authors to control what data the infected host sees. This same code could be used on a per user basis to manipulate the account balances that are seen when a legitimate user visits his or her banking institution’s website. At present, the attackers can remove links that allow users to terminate online sessions. In the future, it may be possible for the worm authors to mask the evidence of any stolen money by displaying the end user’s balance information prior to malicious actions occurring.

One effective means of blocking the actions of Qakbot is forcing a second mode of authentication. Additionally, it is effective to force user authorization when online accounts are used to make transfers. Even after hijacking an unsuspecting client’s session, the malware controllers would not be able to complete the “challenge handshake” in order to remove funds from the account.⁹

⁸ Symantec, *W.32 Qakbot in Detail*, June 2011.

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf

⁹ Symantec White Paper, *W.32 Qakbot in Detail*, June 2011,

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf

- **Banking Trojans**

Malware continues to grow at exponential rates, with Trojans now being the most common type – 66 percent of all malware.¹⁰ Trojans infect a victim's computer to enable a cybercriminal to perform malicious functions, such as making it part of a botnet (a collection of remotely-controlled computers) or stealing confidential data like passwords and credit card information. Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. New variations are constantly being introduced to thwart detection by antivirus software, and real-time capabilities built into the Trojans make it difficult for banks and account holders to spot fraud attempts as they occur.

Trojans today pose a clear threat to the trust in online banking that financial institutions have worked so hard to establish for their customers, let alone the extensive losses associated with fraud and potential lawsuits. For example, in 2009, a Maine-based construction firm sued its local bank after cyber thieves stole more than a half million dollars through illegal transfers from the company's online account.¹¹

The most prevalent of all banking Trojans is known as Zeus. Hundreds of criminal groups are operating Zeus-fueled botnets or Zbot botnets. The number of infected PCs is estimated at 3.6 million in the U.S., or one percent of all PCs in the country.¹² Zeus has been stealing data and circulating since 2006, capturing infected users' banking logon credentials and sending them back to a command-and-control hub. Zeus is propagated through scams such as spam messages purportedly from well known telecommunications and software companies, social networking sites, and government agencies.

Zeus infects PCs, waits for their users to log on to a list of targeted banks and financial institutions, steals their credentials and sends them to a remote server in real-time. In addition, it may inject code into the web pages shown by a user's browser, so that its own content is displayed together with (or instead of) the genuine pages from the bank's Web server. In this way it is able to ask the user to divulge additional personal information, such as payment card number and PIN, one-time passwords, and more.

To evade detection and removal, Zeus uses rootkit techniques. The Zeus kit is a binary generator. Each use creates a new binary file, and these files are different from each other — making them notoriously difficult for antivirus or security software to detect. To date, very few variants have had effective antivirus signatures against them, and each use of the kit usually makes existing signatures ineffective.

Using Zeus or other banking Trojans, cybercriminals can bypass many of today's standard security mechanisms. That is why a layered security defense is critical: no one security component is fail-proof against every possible threat. It takes a multilayer strategy to defend against sophisticated fraud attempts. By layering technology such as two-factor authentication and fraud detection, financial services companies can better protect themselves and their customers.

- **ATM Heists**

Over the past two years, cyber ATM heists have accounted for nearly \$30 million in fraudulent transactions. Recently, an international cybercrime gang stole \$13 million from a Florida-based bank by

¹⁰ Symantec White Paper, *Banking Trojans: Understanding Their Impact and How they Impact Your Institution*, http://www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_info_risk_comp&pvid=fds_1

¹¹ *Id.*

¹² *Id.*

cashing out stolen pre-paid debit cards.¹³ The attackers were able to breach the institution's network, targeted pre-paid debit cards, and distribute the cloned prepaid cards globally.

In 2009, another similarly coordinated attack resulted in the heist of \$9 million in cash, after a hacker penetrated a server at a payment processor. About a month later, the processor announced that they'd been hacked, and personal information on approximately 1.5 million payroll-card and gift-card customers had been stolen.¹⁴

Another scheme in 2007 targeted a payment card company. In just two days, four payment cards were hit with more than 9,000 actual and attempted withdrawals from ATM machines around the world, resulting in losses of \$5 million. A similar technique was employed against a major financial institution last year, after a processing server that handled withdrawals from the bank's ATMs at convenience stores was breached. In that case, cashers converged on a major northeast city and withdrew at least \$2 million from the bank's accounts and then sent most of it out of the country.¹⁵

- ***Mobile Devices, Payment, and Banking Applications***

With the increased use of mobile phones for banking comes increased risks. As more users download and install third-party applications for mobile devices, the opportunity for installing malicious applications is also increasing. Most malicious code is now designed to generate revenue. Hence, there will likely be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking. Trojans that steal data from mobile devices and phishing attacks are some of the first of these threats to arrive.

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals globally, there was a 42 percent increase in the number of reported new mobile operating system vulnerabilities from 2009 to 2010.¹⁶ Currently, the majority of malicious code for mobile devices is in the form of Trojans that pose as legitimate applications. These applications are uploaded to mobile application marketplaces where users download and install them. In some cases, attackers may take a popular legitimate application and add additional code to it, as happened in the case of the Pjapps Trojan. Indications from the ISTR XVI are such that not only are the operating systems of the mobile devices prime targets for threats, malware, and exploited vulnerabilities, but the applications (or Apps) that are used on these mobile devices are increasingly growing as threat vectors.

The potential for fake and/or rogue applications that are designed to look, feel, and act like a trusted mobile banking application are an increasing threat and propagation method for malware and illicit activity. Often, the propagation/enticement method includes a "free" version of a popular application that an individual would normally have to pay for. The unknowing consumer opts to download the "free" version of the application, which could be a financial management/banking application, or any type of application, and once the application is downloaded to the mobile device, the malware begins to execute without the user's knowledge.

¹³ *Coordinated ATM Heists Net Hackers \$13M*, Brian Krebs, Krebs on Security Blog, August 26, 2011

¹⁴ *Global ATM Caper Nets Hackers \$9 Million in One Day*, Kevin Poulsen, Wired, 2/4/09

¹⁵ *Id.*

¹⁶ *Id.*

The safest and most secure mobile banking application transactions utilize technologies including but not limited to: encryption of information during transmission; encryption of any persistent information stored on the mobile device; authentication and tracking of the device based on constant attributes of the mobile device associated with that user account; and lastly and most significant, two-factor authentication including a persistent PIN and a onetime use password which is initiated once per transaction. The onetime use password via two-factor authentication is a significant security measure that allows only one person to be authenticated to a financial transaction application for a singular session. Once that session is completed, another two-factor authentication takes place producing another singular session that can be tracked and logged to provide an accountability system of checks and balances.

FINANCIAL SERVICES LEADS IN SECURITY

The financial services sector has been a leader in taking both voluntary and required measures toward the goal of cybersecurity protection for their customers, commercial clients and their own franchises. Industry professionals are increasingly focused on safeguards, investing tens of billions of dollars in data protection as they recognize the criticality of confidentiality, reliability and confidence to their success in the marketplace as well as national security. This market-based discipline is enforced through an increasingly informed consumer base, and by a very active commercial clientele that often specifies security standards and negotiates for audit and notification rights.

To strengthen public confidence and to ensure consistency across a wide variety of institutions, self-regulatory organizations and government agencies codify and enforce a comprehensive system of requirements. Many of these represent the distillation of best practices previously developed on a voluntary, collaborative basis by the industry and codified into law by this Committee. These include the provisions of Gramm-Leach-Bliley, the Financial Services Modernization Act of 1999, which fostered the promulgation of Regulation P by the Federal Financial Institutions Examinations Council (FFIEC) and Regulation S-P by the Securities and Exchange Commission (SEC). These oversight mechanisms of data security are unique to the financial services industry.

This Committee, and the financial services industry generally, has been ahead of the curve on cybersecurity, recognizing the importance of these issues long before they were common in daily headlines. Thus, the need for action is not so much an issue of additional legislation or regulation, but rather an issue of responding to evolving threats by implementing mitigation and protection measures.

MITIGATING RISKS

There are a number of steps that industry can take to lessen the impact or prevent future attacks. We recommend the following measures be implemented to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.
- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving

your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.

- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.
- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

However, while technological improvements are necessary, they must be paired with increased education and awareness. People, processes, organization and technology must all be addressed to mitigate cyber threats. We see the need for improved education efforts across the spectrum of learning institutions from the classroom and colleges, to corporate management and professional education.

We also need to embrace new and evolving security technologies, rather than looking to simply refine traditional security technologies around the changing threat landscape. An example of this is how to best address the APT. The design of the APT is to gain massive amounts of intelligence about a target before launching an attack. The financial organization, enterprise, or entity needs to understand and use this intelligence about how they normally do business and secure this from an offensive perspective. Once the financial organization has a blueprint of their normal business processes and hardens these processes, anything outside of the norm can be detected as an anomaly, and systems can be protected. This is the primary method for defending against APT types of malicious activity at the core of infrastructure protection.

Successful mitigation of cyber threats also requires increased coordination and communication among industry and between government and industry. Currently, there are a number of organizations in place to facilitate information sharing, including Information Sharing and Analysis Centers (ISACs) and the National Cyber-Forensics and Training Alliance (NCFTA).

- **ISACs**

ISACs were established in the late 1990s as a result of the recognition by industry and government that more needed to be done to address critical infrastructure security. Today, the majority of ISACs are operated by the private sector, and facilitate information sharing and comprehensive sector analysis on both physical and cyber events across their industry members, and with other ISACs through the National Council of ISACs. In addition, a number of the ISACs have established partnerships with various government agencies whereby information is shared, and incidents are jointly worked by government and industry. Services provided by ISACs include risk mitigation, incident response, and alert and information sharing. There are ISACs that represent IT (of which we are a member), Financial Services, Communications, Energy, and several other critical sectors.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 2002, and today reaches more than 20,000 industry partners daily. The FS-ISAC is considered a successful model for other ISACs, with its broad range of 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, and financial advisory services. In addition to supporting the needs of the financial services sector, it works closely with other ISACs and government partners to protect critical financial services and facilitate strong information sharing.

- **NCFTA**

Established as a non-profit corporation to address cybercrime, the NCFTA is a non-profit corporation that comprises a large network of experts from the public and private sectors. Functioning as a conduit between private industry and law enforcement, the NCFTA's core mission is to work with law enforcement to identify criminals or criminal groups responsible for cyber-based threats, and to provide law enforcement with actionable intelligence to mitigate threats.

The NCFTA has pursued a number of successful activities to neutralize cybercrime, including proactive law enforcement engagement (domestically and internationally), and implementation of interim technology solutions (i.e., null-routing of botnet traffic or similar interdiction action via Top Level Domains or ICANN).

The NCFTA regularly supports interaction into threat-specific initiatives to promote better intelligence sharing between the NCFTA and law enforcement. After a major cyber crime trend is identified, members of the NCFTA develop a tailored program whereby the NCFTA manages the collection and sharing of information with industry partners, appropriate law enforcement, and other cross-sector experts. As a result of these initiatives, hundreds of criminal (and some civil) investigations have been launched, with successful prosecutions of more than 300 cyber criminals worldwide. In addition, in the past three years alone, the NCFTA has developed more than 400 cyber threat intelligence reports to assist partners in mitigating the threats of cybercrime.

Over the years progress has been made to advance information sharing among critical infrastructure sector partners and the government. Organizations such as the NCFTA and FS-ISAC have done a commendable job of creating mechanisms to share intelligence among industry and between industry and government. In order to successfully mitigate against these threats however, information must be shared in a timely and actionable manner. In addition, there are still significant impediments to

government sharing information with industry, including classification designations, legal restrictions, and competitive advantage concerns.


CONCLUSION

I applaud the Committee's commitment to this critical topic and its leadership on data security issues for more than a decade. As the threats we face today continue to escalate in both sophistication and volume, we must continue to bolster cybersecurity, improve information sharing mechanisms, and increase awareness and education. Symantec looks forward to working with the Committee and our public and private sector partners to address these important issues.

United States House of Representatives
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

1. Name: Brian Tillett	2. Organization or organizations you are representing: Symantec Corporation
3. Business Address and telephone number: <div style="background-color: black; width: 100%; height: 40px;"></div>	
4. Have you received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	5. Have any of the organizations you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
6. If you answered yes to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets. <p>As the world's largest security software company, Symantec regularly does business with a wide array of Fortune 500 companies including financial institutions, and several federal cabinet level agencies. Symantec's federal and state government revenues for its fiscal year 2011 exceeded \$400M.</p>	
7. Signature: <div style="text-align: center;"></div>	

Please attach a copy of this form to your written testimony.