NYS Senate Public Hearing

Cyber Security:
Defending New York from Cyber Attacks

Testimony of Benjamin M. Lawsky, Superintendent of Financial Services

The Griffiss Institute, Rome, New York
November 18, 2013

My name is Benjamin M. Lawsky and I am Superintendent of Financial Services. I also serve as Co-Chair of Governor Cuomo's Cyber Advisory Board.

I appreciate the opportunity to present testimony today and thank Senator Griffo and the members of the committee for inviting me and for shining a light on an issue that we all need to focus on to ensure the security of our state and nation. I also want to thank the Chairs of the other committees represented here today, Senators Ball, Gallivan, Golden, Seward and Valesky.

Cyber security is a critical issue for all of us as public officials and particularly by virtue of New York's status in the world. New York City is a global and national center of finance and commerce. We are the home of Wall Street and hundreds of corporations with interests in banking, insurance, securities and countless other sectors of the economy.

Obviously, New York presents tempting targets for cyber criminals intent on disrupting or even destroying our institutions, or stealing the confidential information of those institutions and their customers. Major New York City-based institutions have already been targeted. Within the past year, the web sites of American Express, JPMorgan Chase, The New York Times, and Citigroup were disrupted in well-publicized cyber-attacks.

Today, I will discuss the Cyber Advisory Board appointed by Governor Cuomo last May and the work of the Department of Financial Services (DFS) related to strengthening cyber security in New York's financial services community.

New York State Cyber Security Initiative

Last January, Governor Cuomo launched a two-pronged cyber security initiative aimed at helping New York defend against the threat of cybercrime – the creation of a new facility bringing together the monitoring of both the cyber and physical aspects of critical infrastructure in the state and the formation of a Governor's Cyber Security Advisory Board.

The creation of an integrated facility to address physical and cyber infrastructure issues is designed to improve information sharing between organizations monitoring cyber and physical security within the state.

Previously, there were separate intelligence gathering and dissemination centers for physical and cyber infrastructure. The New York State Intelligence Center (NYSIC), administered by the State Police, served as the statewide criminal intelligence center, and the State's cyber security was handled mainly through the Division of Homeland Security and Emergency Services and the Center for Internet Security (CIS), a non-profit with which the State contracts to monitor a number of agency and authority computer systems.

The second part of the Governor's initiative was the formation of the Cyber Security Advisory Board to advise on the latest research and best practices in order to inform the state's cyber strategy.

The Cyber Security Advisory Board is comprised of recognized experts in the field, including current and former high ranking individuals in relevant government and private sector offices. The group meets periodically to consult with the Governor and/or administration officials on recent developments in cyber security nationwide and key strategies for securing the state's cyber infrastructure. The Board is also studying ways in which the State may be able to create incentives to grow our cyber security workforce—especially here in upstate New York, which has so many organizations at the forefront of this field.

One of the benefits of the Board is that it has brought together experts and officials from different industries, such as finance, energy, and transportation. This has allowed us to take the best ideas from one sector and find ways to apply them in other areas.

Finally, the Board is partnering with administration officials to analyze what the state is and should be doing do to ensure that all entities with impact on critical infrastructure are taking the appropriate cyber security measures. The combination of government and corporate experience on our Advisory Board will help ensure that our State policy is consistent with the principles of government transparency, reasonable regulation, and privacy protection.

DFS Activities

Now, I will discuss the three specific questions the Committee expressed interest in reviewing:

- First, DFS's initiatives to assure the security of information;
- Second, DFS's assessment of the risks that must guarded against in keeping information secure;
- And, third, DFS's recommendations to address future challenges.

As New York's regulator of financial services, DFS is responsible for regulating and supervising the activities of nearly 500 life insurance and 1,100 property/casualty insurance companies with assets of more than $4 trillion, health insurance companies, and nearly 300 state-chartered banks with assets of $2.1 trillion.

In addition, DFS regulates more than 1,600 other licensed financial entities. These include money transmitters, licensed lenders, budget planners, credit unions and mortgage servicers and other entities involved in delivering financial services of one kind or another.

Virtually all of these institutions—given the nature of their businesses, the volume of personal data processed, and their importance to the economy— are attractive targets and, therefore, vulnerable.

Under Governor Cuomo's direction, DFS has undertaken a strong initiative to thoroughly examine how the institutions we regulate are addressing cyber security risk.

The Department is exploring such issues as how our institutions identify and assess potential cyber-attacks; the level of risk they face; and the systems and processes they have or should have in place to ensure their security. Throughout this process, we have tried to remain mindful that our institutions vary dramatically in terms of their size, complexity and availability of resources.

DFS's goal is to ensure that all of our institutions are working proactively to minimize the risks they face to protect their business operations and safeguard the personal and financial information of the thousands of customers and clients they represent.

This initiative has involved surveys of more than 200 institutions—a total of 192 depository institutions, including 66 community and regional banks and credit unions, and 58 foreign branches and agencies—with assets ranging from $5 million to $282 billion. In addition, 8 of the largest money transmitters and more than thirty insurance companies with operations in New York participated.

DFS is now analyzing this data. We have also consulted with security experts and engaged in an informal dialogue with the industry, speaking to large and small institutions alike to learn more about the challenges they face in this area and what keeps them up at night. While our initiative to date has focused largely on banking organizations, we expect to shift our attention more fully to the insurance sector in the coming months.

With respect to DFS's assessment of the kinds of risks that must be guarded again, this is what we have learned so far:

- First, the rise in frequency and breadth of cyber attacks globally can be attributed to a number of factors. While unfriendly nation-states breach systems to seek intelligence or intellectual property, "hacktivists" aim to make political statements through systems disruptions. Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain—be it through account takeovers, ATM heists, or other mechanisms. A growing black market for breached data has only served to encourage wrongdoers further.
- Second, while attacks on large international institutions capture the attention of the media, we must remember that smaller institutions may be just as vulnerable. Smaller banks don't have the IT staffs and resources of larger institutions and, in some cases, may even have a false sense of security, believing that it is only the multi-billion interests which are subject to attack. That is not to say that community and regional banks do not have comprehensive cyber security programs—most of them do. But the speed of technological change and the increasingly sophisticated nature of threats create particular challenges for smaller institutions trying to remain vigilant.
- Third, threats come not just from outside but from within. Current and former employees or other business partners that have authorized access to an institution's network or systems may be tempted to misuse or steal confidential data or intellectual property. This

means that, amongst other things, institutions need to monitor their employees and have robust processes in place that limit access to data.

- Finally, we must focus not just on the institutions we regulate, but on IT vendors and third-party service providers. Our survey found that the vast majority of financial institutions, irrespective of size, utilize both internal and external resources to manage their IT systems. In addition, many also rely on third-party service providers for data-sensitive functions, such as payment processing. This means that an institution's cyber risk level depends substantially on the processes and controls put in place by others. As a result, it is essential that institutions have adequate insight into the sufficiency of those procedures.

It is apparent from our work over the past six months that the industry is engaged on this issue. Institutions want to know how they are doing on cyber security—especially relative to their peers—and how they can do better. With that in mind, I am pleased to announce that DFS has—with CIS's assistance—developed an interactive self-assessment tool that will enable institutions to evaluate their own cyber security readiness as compared to their peers, in a confidential and anonymous format. We are asking all of our community and regional banks, credit unions, and foreign branches and agencies to participate in this exercise, which will take place on December 12, 2013. We hope to offer this tool to insurance companies down the line as well.

Finally, with respect to future challenges, DFS is considering a number of additional initiatives aimed at providing more information to the industry and helping institutions' strengthen their cyber defenses. In the coming months, we hope to release reports on the findings of our cyber risk survey, which will enable the industry to better assess its strengths and weaknesses in this area. The first report will focus on banking with a second report to center on insurance. In addition, we plan to develop industry guidelines on best practices.

Conclusion

Based on what we have seen occur over the past few years, it is clear that cybercrime will continue to occur and that it will evolve over time, posing new threats and new challenges to our state and nation.

In conclusion, I want to stress the commitment of the Cuomo Administration to making sure that there is a continuing, focused effort on the part of state government to recognize the urgency of this issue and find ways to address it. And I thank this committee for your work in addressing this critical issue. Thank you for the opportunity to present testimony today.

###

PUBLIC TESTIMONY

JOSEPH A. D'AMICO
SUPERINTENDENT
NEW YORK STATE POLICE

PRESENTED TO:

NEW YORK STATE SENATE COMMITTEES ON BANKS, INSURANCE, VETERANS, CRIME AND CORRECTION
AND
NEW YORK STATE SENATE SELECT COMMITTEE ON SCIENCE, TECHNOLOGY, INCUBATION AND ENTREPRENEURSHIP

MONDAY, NOVEMBER 18, 2013

GRIFFISS INSTITUTE
725 DAEDALIAN DRIVE
ROME, NEW YORK 13441

Thank you Senators for the opportunity to discuss with you cyber security and how we can defend New York from cyber attacks. I am Joseph D'Amico, Superintendent of State Police.

Sophisticated cyber-attacks are on the rise, most recently targeting federal agencies, media outlets, social networking sites, top corporations, and leading financial institutions.

These attacks are being carried out by nation-states, hacktivists, and criminal organizations.

They compromise public safety, classified information, intellectual property, sensitive data, and business networks, putting our national and economic security at risk.

The issue of cyber security affects all New Yorkers. By now most New Yorkers have been victimized or targeted by identity thieves, con men, cyber bullies, network intruders, or email scammers. Their losses amount to hundreds of millions of dollars and untold heartbreak.

Our objective is to further establish New York State as a national leader in protecting its citizens, public institutions, and private companies from losses due to cyber attacks.

Our obligation as a State encompasses five responsibilities – to develop a comprehensive understanding of the risks we face, to create appropriate safeguards to protect our assets, to identify the occurrence of a cyber security event, to respond and take action when cyber security events occur, and to recover to normal operations to reduce the impact from a cyber security event.

Our activities underway and our planning for the future address each of these five areas. I begin with the last three of these where the New York

State Police plays an active role – in identifying and reporting cyber intrusions, responding to breaches, and mitigating the effects of cyber incidents.

One of the fundamental shifts in security in our post-9/11 world is the recognition that to achieve maximum security, there must be strong coordination between the physical and cyber security arenas. Our greatest defense against an attack is to ensure that we are able to maintain the highest level of situational awareness and actionable threat intelligence as possible.

However, gathering intelligence about priority cyber and physical threats is daunting, and the only way we can successfully accomplish this is to work together in a coordinated and collaborative environment.

It is essential that we create a mechanism to analyze information and collate what might seem like isolated bits of data across both the cyber and physical domains into a complete, enhanced situational awareness of what is happening at the state, local, tribal and territorial (SLTT) government level.

Integrated Intelligence Center (IIC)

To that end, through the leadership and vision of Governor Cuomo and efforts of the U.S. Department of Homeland Security (DHS) and the Center for Internet Security/Multi-State Information Sharing and Analysis Center (MSISAC), a unique collaboration has been established that provides a mechanism through which government, the private sector and law enforcement, and public safety organizations can come together with a common purpose and improve the ability to safeguard New York State and the nation.

The partnership has been accomplished by the co-location of the New

York State Intelligence Center (NYSIC) and the MSISAC at one physical location called the Integrated Intelligence Center (IIC).

MSISAC is a division of CIS, a global nonprofit organization located in East Greenbush, NY whose mission is to enhance the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS operates a 24/7 joint security operations center, through which it provides early cyber warning alerts, analysis, incident response and monitoring services. Coupling the state's ongoing counter terrorism and intelligence capabilities with the CIS's unique access to real time cyber threats from across the nation, makes this joint venture the first of its kind in U.S. law enforcement.

This new IIC provides an economical, efficient, and trusted resource for the development and dissemination of comprehensive, coordinated intelligence products that help improve security across New York State and the nation.

Collection of information, identification of threats and intelligence gaps, and reporting to SLTT partners not only allows them to defend their cyber and physical domains, it provides a ready-pool of information that can be shared with intelligence and law enforcement partners to assist them in their areas of responsibility.

IIC will also facilitate identifying the physical vulnerabilities of cyber infrastructure, whether it be fiber conduits across the span of a bridge or the safety of servers for first responder agencies. The center has developed a Risk Analysis Cell (RAC) comprised of both DHSES and NYSP intelligence analysts who work with DHSES' Office of Counter Terrorism Critical Infrastructure Protection Unit. While primary focus

has been physical threats and risks assessments related to critical infrastructure, cyber threats will now be addressed as well.

Furthermore, CIS is designated by DHS as a key resource for all homeland security advisors, fusion centers and cyber security and chief information officers representing all SLTT governments covering both cyber and physical domains across the country. The IIC directly supports the DHS vision for fusion centers to be a centerpiece of state and local government intelligence sharing with the federal government.

Finally, New York State Police is staffing the FBI Cyber Task Force Initiative. State Police members will be trained through the FBI and work on both criminal and national security investigations involving cyber intrusions and theft.

Coordination at this level provides tremendous value. Two-way sharing of information between and among partners and the IIC results in improved overall situational awareness along with enhanced preparedness and response resources. The collective view is much more powerful than the singular view, and only by working together will we be able to identify, confront and contain the cyber threats we face.

New York State Cyber Security Advisory Board

In response to the need to develop a comprehensive and coordinated approach to cyber security, in May 2013 Governor Andrew Cuomo created the NYS Cyber Security Advisory Board.

The Advisory Board is co-chaired by Thomas P. Abt, NYS Deputy Secretary for Public Safety; Benjamin M. Lawsky, Superintendent of the NYS Department of Financial Services; and William F. Pelgrin, CEO and President of the Center for Internet Security, CIS.

The Advisory Board members are among the world's leading experts in cyber security and bring vast experience in both the public and private sectors.

Members include Richard Clarke, Chairman and CEO of Good Harbor Consulting, LLC; Shawn Henry, President of Crowd Strike Services; Phil Reitinger, Senior Vice President and Chief Information Security Officer, Sony Corporation; and Howard Schmidt, former White House Cyber Security Coordinator and Special Assistant to President Obama. All have held senior cyber-security positions in the federal government and/or private industry.

Peter Bloniarz, until recently the former dean of the University at Albany's College of Computing and Information, serves as Executive Director and Senior Policy Advisor for the Advisory Board. Peter is here with us today and I would ask he stand for an introduction to the committees.

The Board's charge is to help the Administration develop a comprehensive set of innovative and effective strategies that can be implemented to keep New York citizens, businesses, and public institutions safe from cyber threats.

The Board has held two meetings, in May 2013 and earlier this month. To date, the Board's attention has been focused on the first two responsibilities in a comprehensive program for cyber security – identifying sectors where the state faces the highest risk, and ensuring that the state creates appropriate safeguards for protecting those sectors.

The Board has identified several priority areas for attention -- infrastructures critical to the New York State economy, including the energy and finance sectors, and education and workforce development. At the recent meeting, the Board received briefings on the efforts that

are currently underway to protect the energy and finance sectors, as well as an update on cyber educational initiatives in the State.

Over the next eight months, the Advisory Board will identify a set of concrete and specific near-term activities and programs that will take advantage of NYS assets and interest in cyber security and that will increase the ability of New York State organizations and citizens to protect themselves from cyber crime and cyber attacks. In addition, the Advisory Board will develop a roadmap for New York State, consisting of additional short-term, medium-term, and long-term actions to put into place plans and policies that will further protect the state. The engagement of the Advisory Board is a key mechanism for ensuring that New York State will be aligned with federal plans and priorities, utilize best practices from across the nation, and leverage all available public and private resources.

An example of the kind of comprehensive cyber security approach that is required can be found in the state's program for protecting our energy sector. Under the direction of Richard Kauffman, Chairman of Energy Finance, and Audrey Zibelman, chair of the Public Services Commission, the PSC late last year required each of the state's energy facilities to prepare updated cyber security plans. These plans were to address federal standards as well as additional items that ensured that cyber security received full executive-level attention. This past winter, PSC staff reviewed these plans and conducted on-site reviews to ascertain their thoroughness and the quality of organizational attention that these plans received. Subsequent analysis led to several recommendations that are now under consideration. Among these are technical enhancements to increase the energy facilities' cyber defenses, and forensic capabilities that will enhance the ability of local, state, and federal responders to deal with any intrusions that might occur. This

comprehensive approach – from identification of risk to comprehensive defenses to increased ability to respond to incidents – is a model for ensuring that our state's critical infrastructures are minimizing their risks in cyber space.

Through all these efforts, , the Cuomo administration commits itself to developing a comprehensive set of programs and policies that assist all New Yorkers and all New York institutions in protecting themselves from cybercrime and cyber intrusions, and ensuring that the state's critical infrastructures are taking appropriate action to protect themselves.

Let me sum up by saying that the need for improved cyber security has never been greater. Especially in New York State with our significant financial, transportation and energy sectors relied upon by individuals and communities from not only the state, but the nation and beyond. It is for these reasons and many others that New York State and the State Police are taking timely and significant steps to combat these threats.

PUBLIC TESTIMONY

JEROME M. HAUER
COMMISSIONER
NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

PRESENTED TO:

NEW YORK STATE SENATE COMMITTEES ON BANKS, INSURANCE, VETERANS, CRIME AND CORRECTION
AND
NEW YORK STATE SENATE SELECT COMMITTEE ON SCIENCE, TECHNOLOGY, INCUBATION AND ENTREPRENEURSHIP

MONDAY, NOVEMBER 18, 2013

GRIFFISS INSTITUTE
725 DAEDALIAN DRIVE
ROME, NEW YORK 13441

Good afternoon Senators and thank you for the opportunity to testify today on the important issue of cyber security and the actions my agency and others are taking to address this growing threat. I am Jerry Hauer, Commissioner of the NYS Division of Homeland Security and Emergency Services.

Threat Posture

My agency, alongside our other State partners, has been very aggressive since the September 11th attacks in addressing the physical threats of terrorism against our citizens and critical infrastructure. As any type of threat emerges, we adapt our posture and programs, and it has been no different when it comes to cyber threats.

New York State agencies, like other enterprises, are faced with constant attempts at cyber-intrusion and exploitation from a wide array of adversaries, ranging from nuisance attacks to potentially significant threats from nation-states and terrorists. Let me begin by outlining for you what I see as the current threat environment.

- Organizations based in countries like China, Iran, Russia and North Korea, among others, are well known in the public domain to be responsible for attacks aimed at stealing intellectual property and conducting espionage. General James Clapper, Director of National Intelligence, said Chinese cyber theft of American intellectual property is ``the greatest pillaging of wealth in history.''
    - A recent public report by the private company Mandiant illustrated an Advanced Persistent Threat attributed to an organization that Mandiant linked to the Chinese government. The Director of National Intelligence has also reported that intelligence services, private sector companies, academia and others are targeted by nation-state sponsored groups to collect economic and other valuable information.
- We also have groups, mostly proxies of the Syrian and Iranian government, who have been conducting attacks against our financial institutions, media corporations and governments in attempt to disrupt business, steal information or promote the agenda of their government backers. The Syrian Electronic Army, to cite one example, is a group of online pro-Syrian Regime hacktivists, who in advance of possible US military involvement in Syria this summer, conducted a series of spear phishing attacks against and disrupted web access to the NY Times and Twitter. They were also credited with the defacement of the US Marine Corps Recruiting Command

website and claimed responsibility for hacking the AP's Twitter account to report false explosions at the White House, which resulted in the Dow plummeting nearly 100 points.

- We also face organized crime online, threatening our privacy and personal property through online banking scams and fraud. Russia, Ukraine and Romania have sophisticated cyber-criminal networks.
- Hackers with political or social agendas, or "hacktivists", groups like Anonymous and Lulzsec, who largely conduct web site defacements, denial of service attacks and virtual sabotage continue to be a significant concern.
- Insiders also pose a significant threat. These are people with legitimate access to systems who act with malicious intent to use information for personal gain or to cause disruption or damage. The recent reporting on the high profile release of US national security information by a cleared employee, among other incidents in recent history, has led the country to refocus prevention and mitigation efforts as it relates to the insider threat. Additionally, the insider threat extends to inadvertent human error which can cause as much disruption and damage. A good example is the 2012 South Carolina data breach in which an employee fell victim to a phishing email that resulted in the release of large amounts of personally identifiable information.

Again, these global cyber attacks, which are continuously increasing in number and sophistication, focus on a variety of malicious objectives, including compromising systems, stealing or corrupting data, and harming critical infrastructure. Consequently, it is essential for our State to maintain robust, layered defenses which incorporate people, technology, and operations in order to continuously enhance our cyber security threat posture.

DHSES and OITS Mission

To protect against these threats against New York State government in particular, it is the job of our intelligence analysts to ask "who and why" and the job of our technical cyber staff to focus on the "what and how" to prevent the exploitation of vulnerabilities in our systems. As such, DHSES is cross-training intelligence analysts, who are fully integrated at the New York State Intelligence Center – the state's designated all-crimes fusion center. The analysts have been working closely with New York State Police and the state's Chief Information Security Officer (Tom Smith) to identify cyber threats and risks. Now, with the co-location of the fusion center with the Center for Internet Security, New York State will be able to leverage additional sources of data and expertise to ensure full awareness of all aspects of the

threats to our systems so that we can properly detect and defend against these threats. Superintendent D'Amico will discuss the co-location in more detail.

New York State has had a dedicated cyber security function since 2002. Currently, it resides in the Office of Information Technology Services (ITS). This presents a unique opportunity to improve the security of the networks that control essential government services that process vast amounts of sensitive information. The Enterprise Information Security Office is positioned to assess risks and evaluate resource requirements that impact the delivery of IT services that support critical agency programs.

Consistent with the provisions of the State Technology Law, ITS, through the Enterprise Information Security Office, is responsible for providing for the protection of the state government's cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the state. The Enterprise Information Security Office also provides services and support to a wide variety of public entities outside of the Executive Branch, including the Office of the State Comptroller, the Office of the Attorney General, and local governments.

In fulfilling its mission, the Enterprise Information Security Office coordinates with internal and external partners on statewide information security issues; works to maintain the alignment of State policies with Federal and industry best practices and applicable regulations; coordinates cyber security incident response planning and execution; and administers Federal grants for cyber programs. Key members of the Enterprise Information Security Office hold security clearances for access to classified information, facilitating coordination with Federal partners, including the FBI and the U.S. Department of Homeland Security, as well as the MS-ISAC and New York State Intelligence Center, and assisting in detection of and response to cyber incidents. Finally, the Enterprise Information Security Office is now offering support to and receiving guidance from the Governor's Cyber Security Advisory Board. The Cyber Security Operations Center within ITS provides reasoned and actionable cyber security information to State agencies and others. Based on research and information from trusted third party sources, CSOC staff draft and disseminate alerts, advisories, information bulletins, and white papers concerning current threats and vulnerabilities.

Before I close I also want to discuss two additional State initiatives to combat cyber threats – a Division of Military and Naval Affairs proposal to create cyber protection teams and the recently created Cyber Research Institute.

DMNA Cyber Squads

On October 9th, the New York National Guard requested assignment of one of ten Army National Guard Cyber Protection Teams from the National Guard Bureau that are expected to be fielded in the next two years. This team would be staffed by 39 New York Army National Guard Soldiers with some full-time personnel; be headquartered in Latham with another secure facility at Camp Smith in Peekskill and secure access at the Air Force Research Lab in Rome; undergo approximately two years of staffing, training, and equipping with a fully operational capability date in 2015; and support FEMA Region II states and territories (New York, New Jersey, Puerto Rico and The U.S. Virgin Islands) in a state or federal capacity to augment civilian and military cyber personnel and infrastructure, conduct vulnerability and risk assessments, test cyber infrastructure, and conduct forensic investigations.

Cyber Research Institute

The Cyber Research Institute (CRI) is an independent not-for-profit corporation being established at Griffiss Business and Technology Park in Rome, NY. Its creation was called for in legislation (A02295) sponsored by Senator Griffo and Assemblyman Brindisi, and signed by Governor Cuomo on March 13, 2013. The law charged the CRI with partnering with the Air Force Research Laboratory in Rome, NY, as well as educational institutions, businesses, government entities, and other organizations to "grow the cyber-based economy in New York State and protect the integrity of cyber-based infrastructure; promote and increase economic activity as it relates to the cyber-based economy; facilitate the transfer of cyber technology from the [Air Force Research] lab to practical market application..."

The CRI is just now being established. It has the potential to be a significant asset that can help protect the state's critical infrastructures and key public and private institutions.

As I close today, I don't want anyone to be lulled into a false sense of security or complacency about the threat. It is very real, very serious, evolving and expanding. As you have heard today, we are doing all we can to ensure the state stays current and as protected as possible, but these attacks will continue and our goal is to prevent those we can and minimizes the impact of those we cannot. Thank you again for the opportunity to share my thoughts.

Testimony of

Doug Johnson

On behalf of the

New York Bankers Association

before the

New York State Senate Joint Public Hearing:

"Cybersecurity: Defending New York from Cyber Attacks"

November 18, 2013

NYBA

American Bankers Association

Testimony of
Doug Johnson
On behalf of the
New York Bankers Association
Before the
New York State Senate Joint Public Hearing:
"Cybersecurity: Defending New York from Cyber Attacks"
November 18, 2013

Chairmen Griffo, Seward, Ball, Valesky, Gallivan and Golden, my name is Doug Johnson, Vice President and Senior Advisor, Risk Management Policy for the American Bankers Association. In that capacity, I currently lead the ABA's enterprise risk, physical and cyber security, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership. I am also the current Vice Chairman of the Financial Services Sector Coordinating Council, which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues; as well as a board member of the Financial Services Information Sharing and Analysis Center, a private corporation that works with government to provide the financial sector with cyber and physical threat and vulnerability information as part of the nation's homeland security and critical infrastructure protection efforts.

I appreciate the opportunity to be here today representing the New York Bankers Association. In my testimony, I will discuss the nature of the cyber threat we face, both as an industry and as a country, and how our sector is organized and regulated to actively address that threat. I will also describe the actions that are underway at the Federal level to enhance cybersecurity, and close with how New York State can continue to play a leadership role in our nation's cybersecurity efforts.

I. The Cyber Threat is Real and Growing

As you are aware, our nation's financial sector experienced a large number of cyber-attacks during 2013, mostly in the form of distributed denial of service, or DDoS attacks. These attacks

were largely designed to disrupt our sector's customer-facing online banking platforms, causing periodic loss of availability for those customers. They did not compromise the privacy of customer information or the integrity of bank systems. They were, however, large sustained attacks that challenged the resources of the money center, regional, and community banks that were targeted.

Many of our efforts in the financial services sector are to ensure that attacks designed to disrupt users do not set the stage for data compromises or attacks on system integrity. We have seen some instances of blended attacks, where DDoS traffic is used as a diversion from a simultaneous attack on high value customers. We are also aware that a DDoS attack can also be an attempt to test various points of entry within a financial institution's system for later, more sophisticated attacks. We are always alert for these possibilities. And we expect the nature of attacks to change over time, continuing to increase in sophistication and strength.

Our sector is also mindful of attacks that have occurred overseas which, if conducted against U.S. financial institutions, could have significant impact on systems and customers. The attack on Aramco Oil in August of 2012, where an insider distributed a computer virus called Shamoon wiped the data off approximately 30,000 computers, and the attacks against South Korean banks, purportedly by North Korea, that shut down ATM systems for several hours and disabled over 3,000 computers. These are just two examples of the types of attacks necessitating a high level of readiness on the part of our government and industries.

We are also aware that our vulnerability to such attacks are in many instances based on security gaps that may exist on the part of our retail and business customers, outsourced service providers, or other business partners. The irony is that within the army of computers that bombard a bank's online banking platform with traffic during a denial of service attack may be compromised computers of that bank's customers. Many financial institutions, particularly those that are community-based, are also highly dependent on core banking system processors and internet banking service providers for cybersecurity protection. It is thus important that we strive to protect the entire financial ecosystem, and ensure that our critical service providers abide by the same cybersecurity requirements that the financial institutions must adhere to, as a regulatory requirement but also as a business imperative.

II. The Financial Sector is Actively Addressing the Cyber Threat

The nature and frequency of the recent cyber-attacks has focused a great deal of financial institution attention on whether their institutions, regardless of size, are properly prepared for such events, and whether the appropriate level of resources are being expended both as a sector and as institutions to detect and defend against them. Attention has also been directed toward whether the financial sector is organized appropriately to detect and respond to future attacks and whether government is an active and engaged partner in our efforts. These efforts build on long-standing, collaborative efforts on the part of the financial sector to protect institutions and customers from physical as well as cyber events. A significant protection infrastructure, in partnership with government, exists and is continually being improved.

As I have already indicated, in addition to my role at ABA, I am proud to currently serve as the Vice Chairman of the Financial Services Sector Coordinating Council (FSSCC). I am also on the board of its sister organization, the Financial Services Information Sharing and Analysis Center (FS-ISAC). We have been deeply involved in and supportive of these two organizations since their inception.

Established in 2002, FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, and collaborating with the U.S. government. The Council has 60 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms. During the past decade the partnership has continued to grow, both in terms of the size and commitment of its membership as well as the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation.

The FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical

infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts and other critical information throughout the financial sector. The FS-ISAC has also recently taken over the role of coordinating crisis response for the sector, formerly a responsibility of FSSCC.

Our government partner in these efforts is the Financial and Banking Information Infrastructure Committee, or FBIIC, which is led by Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Essential to the FSSCC's success is the public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime.

The deep involvement of ABA in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial organizations are heavily involved in both. And this collaboration does not include only the largest financial organizations. Our diverse sector is made up of organizations of all sizes and types. ABA has been a primary driver behind expanding the FS-ISAC's reach from under 100 to over 4,000 members to ensure that vital cyber threat information, and the means to defeat those threats, reaches as many financial organizations as possible.

New York financial institutions have always played a leadership role within these two organizations, and indeed were the founding members of the FS-ISAC. Currently, the chief information security officer of Citi, Charles Blauner, and JP Morgan Chase's Chief Information Risk Officer, Anish Bhimani, respectively serve as the chairs of the FSSCC and the FS-ISAC.

The financial services sector develops and implements leading practices through the FSSCC, the FS-ISAC and the FBIIC. For example, under the joint partnership of the FSSCC and FBIIC, our sector has developed leading practices to mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, pandemic flu preparations, and other important risks or threats facing the security and resilience of the sector.

The most recent example of the high degree of interaction and collaboration between these bodies is of course our sector's unified response to the recent DDoS attacks that have occurred since September, 2012. As the number of affected organizations increased, the FS-ISAC was able to organize them into a group to collaborate on measures to mitigate the attacks. Individual organizations were able to, through FBIIC and Treasury, request specific governmental technical assistance as necessary. Due to the tight relationship between the FS-ISAC and the FSSCC, actions such as these are factored into the actions taken by the FSSCC as the Council makes and refines legislative and administrative policy recommendations.

The financial sector's response to Superstorm Sandy is another example of effective collaboration. Prior, during, and after the storm, the FS-ISAC and the FSSCC organized a large number of calls for the sector with New York and New Jersey emergency management personnel, Treasury, and DHS to ensure that financial services were available to those within the affected areas as soon as possible. As such events are inherently local, the New York and New Jersey state bankers associations were vital components of the recovery as we ensured that cash was distributed where it was most needed and that we had an accurate picture of where broader financial services were available.

III. Federal Action is Needed to Further Improve Cybersecurity

It is our sector's view that, given the escalating nature of the cybersecurity threat, further Federal action is necessary to properly address that threat. ABA continues to support the goals of the Administration and Congress to limit cybersecurity threats to business, our government, and the American people.[1]

As Congress and the Administration contemplate changes to the national cybersecurity framework, in addition to considering the cybersecurity measures our sector currently takes collaboratively, also important are the stringent laws and regulations within the financial services sector. Our sector is subject to a wide variety of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained

[1] The FSSCC Comment Letter in Response to the NIST Request for Information, "Developing a Framework to Improve Infrastructure Cybersecurity" is available here: http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.

within the Gramm-Leach-Bliley Act of 1999. For example, financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC). This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks.

Likewise, the Securities and Exchange Commission (SEC) and the self -regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA) review the cybersecurity programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities. Insurance companies' privacy and security programs are subject to review by state insurance regulators.

We applaud the release of the Administration's recent Cybersecurity Executive Order and believe implementation of the Cybersecurity Framework envisioned in the Order can be an important tool in improving our nation's overall cybersecurity. Collaboratively, through the FSSCC, ABA is committed to working toward formulating and implementing this Framework in a manner that:

- ✓ Develops sector-specific frameworks recognizing the unique nature of and levels of protection within each critical sector;
- ✓ Ensures that each sector's primary regulatory authorities remain independent as the overseer and enforcement body for the critical sectors they regulate;
- ✓ Leverages existing audit and examination processes, encourages complementary, not redundant audit requirements when building voluntary cybersecurity practices, and;
- ✓ Creates incentives that are tailored to address specific market gaps.

Even considering the implementation of the Executive Order and the Cybersecurity Framework it envisions, the progress we are making is ultimately inadequate without Congressional action to enhance, facilitate, and protect threat information sharing across sectors and with government.

It is for this reason that ABA and NYBA supports the House passage of the Cyber Intelligence Sharing and Protection Act. The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective

measures against malicious cyber activity. While the cyber threat data that is shared by the financial services sector is machine language and not attributable to an individual, the provisions in the Act concerning liability protections for the sharing of information are also extremely important and transcend our sector. This legislation provides important clarifications that will help facilitate increased cyber intelligence information sharing between the private and public sectors.

Last week, the ABA, the Financial Services Roundtable, and the Securities Industry and Financial Markets Association sent a joint letter to Chairman Dianne Feinstein and Ranking Member Saxby Chambliss of the Senate Select Committee on Intelligence, indicating our support for the Committee's efforts to develop legislation that further strengthens the ability of the private sector and the Federal government to work together to develop a more effective information sharing framework to respond to cyber threats and providing liability protections while balancing the need for privacy protection. We are committed to continuing to work with Congress as it debates policies to strengthen our nation's cyber defense.

IV. New York State Has an Important Cybersecurity Role

New York will continue to play a leading role as we move forward collectively to improve our cybersecurity environment. National and state efforts must be complementary if we are to be successful, and there are a number of current initiatives underway in the states that meet that test.

New York City received the 2012 City Government Cybersecurity Leadership and Innovation Award from the Center for Digital Government for the development of an information security cloud implemented in 48 agencies. As a result of this initiative the city now has direct visibility into over 73,000 endpoints and serves as a model for securing government databases.

The recent establishment of the Governor's Cyber Advisory Board, designed to work with the administration on innovative strategies to keep New Yorkers safe from cyber threats and make recommendations for protecting the state's critical infrastructure and information systems, is another important development.

Cyber innovation closer to the location of this hearing is in the form of the CYBER NY Alliance and its associated New York State Cyber Research Institute (CRI). A primary focus

area of the CRI will be sensitive and classified cyber security research and development, designed to develop solutions to defend the safety, security and stability of our critical state and local infrastructures. Investments in such R&D initiatives should be encouraged, and we are supportive of any Congressional action at the Federal level that enhances tax and other incentives for cybersecurity research and development.

V. Conclusion

Thank you for holding this important hearing. Banks and other financial services companies have made cybersecurity a top priority. We have invested an enormous amount of time, energy and money to put in place the highest level of security among critical sectors, and we are subject to the most stringent regulatory requirements. We look forward to continuing to work with you toward our mutual goal of protecting our nation's critical assets.

Introduction

Senator Seward and members of the Committee, thank you for scheduling today's hearing on Cyber security and thank you for inviting me to provide testimony.

My name is Josiah Wilkinson and I work as an attorney at Nationwide Insurance, reporting directly to the Kirk Herath, Nationwide's Chief Privacy Officer. Prior to my role with the Office of Privacy at Nationwide, I worked within Nationwide's Information Security department for over 7 years. The views I am expressing today, however, are my own and should not be attributed to Nationwide.

Nationwide is a fortune 100 company based in Columbus, OH. Nationwide is a large insurance and financial services company, which offers our members insurance products, financial services products, banking, and mortgages.

As a long-time information security professional, I applaud the state of New York's efforts to progress in the area of cyber security. In my testimony today, I will stress that cyber threats are a very real issue. To combat these threats, I will then emphasize the importance of continued public-private partnerships, and the use of risks-based methodologies to mitigate cyber risks.

Threat Assessment - What's the current danger?

In the Symantec 2013 Internet Security Threat Report, Symantec reports that there has been a 42% increase in targeted attacks and web-based attacks have increased 30% in the last year across all industries.[1] Unfortunately, last year was not an anomaly; each year generally reveals an increase in the amount of malware, number of vulnerabilities attackers may attempt to exploit, and number of direct cyber attacks. The statistics demonstrate that we all must continue to anticipate that the spectrum and sophistication of attacks will continue to grow.

The Financial Services sector, including "risk transfer products", is considered one of 16 critical infrastructure sectors. The Department of Homeland Security has recognized that the "Financial Services Sector represents a vital component of our nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyber attacks demonstrate the wide range of potential risks facing the sector." We too recognize the nature of this environment and have long spent considerable time and effort towards understanding and responding to these threats.

When considering potential risks, an entity should consider their likely threat actor. Broadly defined, there are external, internal, and partner cyber security threat actors. An external actor, for example, would likely be a public user of a website. An internal actor could be an employee or onsite contractor. A partner could be a trusted supplier or vendor, such as an IT service

[1] Symantec Internet Security Threat Report 2013 (April 2013) http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

provider or payroll firm. Based on the Verizon 2013 Data Breach Investigations Report, external threat actors are easily the largest source of cyber attacks based on data breaches and therefore the focus of my testimony.[2] In general there are three major external threat actor categories 1) Cybercriminals 2) Nation States and 3) Hacktivists. The attributes defining the category that an attacker fits is based on his or her intent or motive and, to some extent, his or her sophistication. Cybercriminals often are financially motivated, and while their sophistication can be high, they are largely opportunistic in choosing their victim. Nation States generally seek state secrets or intellectual property and are likely to target a specific victim based on the data they seek. Nation States often are well funded and highly sophisticated and have joined cyber warfare for the long game—they often choose to silently lurk inside a company for years before taking action. Finally, Hacktivists generally are motivated by social issues, politics, or simple irritation at an organization and usually target a specific victim, but as with the infamous LulzSec may simply exploit seemingly random victims based on some principle. Hacktivists can commonly be less sophisticated than Cybercriminals and Nation States.

By considering its probable threat actor, an entity can begin to anticipate the kinds of response that may follow if an attack occurs. For a state entity (e.g. New York), the external threat actors could be any one of the three kinds of threat actors, and the state therefore could find itself dealing with the entire range of attack types and targets – information about individuals or businesses, about infrastructure and industrial controls, or about political interests or programs. The response scenarios could vary accordingly as well. Overall, the danger of cyber threats is significant and growing. Based on data breach data, external threat actors are the most significant threat. Entities can begin to understand their risks by thinking about the motives and potential targets of their likely threat actors and then considering the response scenarios that they would face.

Current Best Practices - What efforts exist to combat cyber threats?

There are numerous approaches that have been developed to counter the increase of cyber threats, and many security professionals would voice that we do not need additional approaches in this space. A few of these approaches, for example, include the ISO (International Organization for Standards) 27000 series, the SANS (System Administration, Networking, and Security Institute) "Top 20", the PCI (Payment Card Industry) Data Security Standard (DSS) and Open Web Application Security Project (OWASP) "Top 10". The concepts in these existing approaches are based on industry expertise and if understood and well executed may be successful in mitigating much of the risk presented by cyber threats. I applaud the recent efforts of NIST in recognizing that another, completely new approach is not needed in driving towards executing a response to Executive Order 13636. NIST has instead developed a framework that incorporates many of these efforts and does so using a risk based approach. While I see the NIST effort as promising as they do incorporate many of industry's best practices, I do have some concerns relevant to the understandability of their material, which I will cover shortly.

---

[2] Verizon 2013 Data Breach Investigations Report (April 2013) http://www.verizonenterprise.com/DBIR/2013/

Nationwide, like many other financial services and insurance entities, has been participating in the NIST Cyber Security framework workshops. While some of the specific recommendations resulting from NIST's efforts differ from Nationwide's long-established practices in this space, there are many similarities, due to NIST's involvement of industry experts through a public-private partnership, reuse of existing approaches, and incorporation of a flexible risk-based methodology.

Public-private partnership:

Without strong, active partnership between public and private entities, any proposed guidance, methodology or legislation is unlikely to represent the combined strengths of both government and industry. We therefore strongly voice support for further joint efforts as we firmly believe we are all smarter and more capable together than apart. The Federal Bureau of Investigation (FBI) has long been supporters of the type of discrete information sharing that could further such a partnership, however this practice must be extended to other government entities so that government and private entities can truly partner together in the fight against cybercrime.

Use of existing approaches:

One of the primary reasons, Nationwide shares so many similarities to the drafted NIST framework is that NIST and its industry participants have wisely chosen to not "re-invent the wheel" and have instead elected to rely on existing industry approaches, several of which Nationwide has consulted to design its own security program. The framework incorporates these standards to call for an entity to develop processes that 1) Identify 2) Protect 3) Detect 4) Respond and 5) Recover.

Identify – "Understand the battlefield"

An entity must first strive to be able to understand its assets, including devices, applications, business processes, people, roles, interfaces, etc.

Protect – "Defend against infiltrations"

Once an entity understands its business and technology, it can undertake activities to enhance measures to strive to protect its assets, such as its servers, routers, and business processes and the various people, processes, and technology that interconnect these systems.

Detect – "Identify infiltrations"

An organization should strive to have appropriate controls in place to protect against attacks. Given the increasing sophistication of, and increase in, cyber threats, however, an entity should expect that its attackers will in any event find a way to be successful. There is no such thing as perfect security; even a sophisticated organization is not going to be perfect in its cyber defenses or in its imperviousness to ever-more-able and ingenious cyber-criminals. This principle is evidenced by data security breaches that have occurred at Google, RSA, and the New York Times. A mature organization however realizes that while it cannot stop all attacks, it can strive to quickly identify, contain, and quash them.

Respond – "Quash the infiltration"

Once an infiltration occurs, the potential for interaction with the network likely will increase, the longer the attacker can persist in the environment. An entity should have established processes for communication, forensics, and ultimately eradication of the threat.

Recover – "Plan for the next attack"

After addressing an attack, an entity must be open to learning and evolving, just as the criminal attackers learn and evolve.

Risk -

In all phases of the cyber security lifecycle, an entity should use a risk-based approach; else its resources will be squandered on efforts that do not ultimately decrease risks. There are numerous methodologies, but all generally focus on identification of the loss magnitude (dollars, assets, widgets), combined with the loss event frequency. If an entity can identify those assets of most value, it can then focus its efforts to protect, detect, respond, and recover from attacks on those assets so that loss frequency is reduced, thereby reducing risk to the entity.

Improvements needed –

While the NIST framework does pull together many of the cyber security approaches that are needed within an entity, it currently needs improvement. Primarily, the improvement needed is not in its technical detail, but rather in delivery. The current draft document is filled with primarily text. Individuals outside of the cyber security profession are unlikely to read, yet alone understand this document. A marketing component is additionally needed so that sophisticated and non-sophisticated entities can quickly digest the concepts in the framework. Videos, social media, and commercials should promote the concepts presented from not only an entity perspective but also from an individual perspective. A good example of an attempt at this approach is the Payment Card Industry (PCI) Council working to create reference guides and guidance documents geared towards small businesses, which otherwise would not likely have the sophistication to understand the PCI Data Security Standard (DSS).

"Concrete solutions" for New York –

As I alluded to when describing industry best practices, there is no silver bullet to addressing cyber threats. A comprehensive plan is needed per entity that identifies assets based on risk, takes steps to protect those assets, and then prepares to identify breakdowns of that protection via a well documented and understood incident response process. Premium vendor provided technology solutions can be useful in reducing the effort needed to secure an environment; however, overreliance on vendor solutions would be to the detriment of New York and its citizens.

In addition to comprehensive plans and the practices that support these plans, cybersecurity must be communicated in such a way that that executives, employees and even laypersons understand these concepts. If an average layperson understands the basics of cybersecurity,

they will protect themselves not only at home, but also when at their place of employment. Cybersecurity cannot continue to be seen as the responsibility of only sophisticated organizations and government entities. Only when average individuals understand their role and value in the fight against cyber threats, will we be able to holistically turn the tide of cybercrime. Branding-based educational and promotional efforts are needed in the space of cyber security.

Conclusion

In conclusion, cyber threats are very real threats. Efforts are underway to combat these threats. One of the most recent efforts, the NIST Cyber Security framework, encourages private-public partnerships, takes advantage of existing approaches and takes into account organizational risk. While this framework is progressing, more work is needed to market the concepts to a broad audience. New York can takes steps to protect itself and its commercial enterprises by encouraging adoption of comprehensive approaches to cybersecurity, by educating its citizens on their role and value in the fight against cyber threats and most importantly continuing to promote public-private partnerships in the fight against cyber threats because like many other challenges we've faced in society, we know that united we stand, divided we fall.

I would like to thank you for holding today's hearing to continue to raise awareness on this critical issue and for inviting me to testify. I am happy to answer any questions.

SCIPP INTERNATIONAL™
THE SECURITY AWARENESS CERTIFICATION COMPANY

Executive Director

Testimony

New York State Senate
Public Hearing on Cyber Security
"Defending New York from Cyber Attacks"

November 18, 2013

Thank you, Mr. Chairman and the distinguished members of the New York State Senate for holding this Public Hearing on Cyber Security. It is my honor to appear before you today to discuss the critical need to ensure that the nearly 20 million citizens of New York state are familiar with security awareness best business practices as the "first line of defense" for defending New York from cyber attacks. This is not a trivial undertaking. The theme of my remarks today is that New York has an opportunity to, once again, lead the nation by placing its cyber security emphasis on being proactive, with regard to the security awareness posture of its citizens – in stark contrast to the traditional, reactive cyber security posture where the emphasis is placed on how to respond to a cyber attack.

My name is Dow Williamson and I am the Executive Director of SCIPP International - a global non-profit organization dedicated to addressing security awareness problems

where they are most prevalent – at the human level. Based in Vienna, Virginia, with offices in London and Hong Kong, SCIPP offers personal and organizational risk mitigation, including compliance risk mitigation, through its world-class American National Standards Institute (ANSI)-accredited security awareness certificate programs for end-users and web application developers. All SCIPP certificate programs are based upon the SCIPP Generally Accepted Practices (GAP™) – the common body of knowledge describing SCIPP's 10 generally accepted best business practice areas vetted by an international advisory board of cyber security luminaries. I am a cyber security professional and have spent the last 25 years protecting sensitive information for citizens, employees, corporations, and governments around the world. I have held senior cyber security-related management positions within both the United States federal government and in the private sector. I was previously the chief architect for the International Information Systems Security Certification Consortium, known as (ISC)², Certified Information Systems Security Professional (CISSP) credential training seminar – the "Gold Standard" in cyber security professional credentials with nearly 100,000 cyber security professionals certified in 140 countries. I was also the (ISC)² CISSP Chief Instructor – educating senior-level cyber security professionals around the world on international cyber security best business practices. Over the past 25 years, I have become very familiar with the need to ensure that both individuals and organizations are familiar with security awareness best business practices as the "first line of defense" for

protecting the confidentiality, integrity, and availability of sensitive personal, corporate, and government information. Today, I am here to offer New York some specific recommendations based upon my experiences and lessons learned.

Cyber security affects all New Yorkers. I firmly believe that one of the most important duties which must be faithfully discharged by state governments is to ensure their citizens are properly prepared to deal with current and emerging cyber security threats, both at home and at work – this starts with security awareness. Security awareness is a lot more than firewalls and anti-virus software – it's not about technical gadgets. It's a mindset – it's about inculcating a security awareness routine in people's daily lives. People are the first and last line of defense in protecting New York from cyber attacks – behavior is the only thing that matters. It's not about creating security experts – it's about knowing when to call one. It's about creating a culture of security aware behavior. Creating an effective security aware culture results in improved awareness among individuals of the risks, responsibilities, and safeguards associated with living and working in our cyber environments. Legislation alone cannot create a security aware culture. It must be coupled with recognition of best business practices and why they are important – like our society has done for health wellness, smoking, drunk driving, illegal drug use, and preventing forest fires. Much like the vigilance of all New Yorkers has kept the Metropolitan Transportation Authority buses, subways, and

railroads safe from the continued terrorist threat and led the nation with its "If You See Something, Say Something" campaign since 2002, New York has an opportunity to show its leadership in cyber security with a campaign all New Yorkers would immediately recognize and understand – a campaign along the lines of "Only You Can Prevent Cyber Attacks". A campaign to ensure all New Yorkers are cyber security aware – both at home and at work. Smokey the Bear would certainly be proud!

We've been warned over the years from experts in both the government and private sector about the importance of security awareness. The Computer Security Institute and the Federal Bureau of Investigations in their annual "Computer Crime and Security Survey" have been warning us of the importance of security awareness since 1996. The National Cyber Security Alliance has been promoting cyber security awareness via the National Cyber Security Awareness Month campaign since 2001. And, the International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$, has been educating cyber security professionals and documenting the critical need for security awareness among citizens and employees since 1989. A professional, comprehensive security awareness program is the single most cost effective measure New York can take to prepare its citizens to help defend New York from cyber attacks. In a recent article in CSO (Chief Security Officer) Magazine entitled "Security Awareness Can Be the Most Cost-effective Security Measure", cyber security

luminary Ira Winkler makes the case for the importance of security awareness training. He wrote, "I was once called into a multinational oil company which wanted advice on a situation. One of their employees called them, because a coworker was displaying unusual behaviors. An investigation was performed, and it was learned that the coworker was giving information to a Chinese intelligence operative. At another company, an employee stopped a person from tailgating him into a facility and it turns out the tailgater was responsible for stealing more than a dozen laptops from company facilities. While performing a penetration test at one company, the security manager told me I should take a long lunch at a very specific restaurant, and just listen to conversations. I learned of the company's marketing plans for a top product. Going to lunch at dozens of restaurants near the National Security Agency, an organization with extensive security awareness efforts, I can hear nothing of any significance. During a firewall penetration test, a strictly technical penetration test, I received a call from a bank vice president telling me to stop my social engineering BS. I asked what the person was talking about, and was told that their people received a call asking details about the firewall, and replied that they needed the person's contact information and would get back to them, as their security awareness training described, and the manager assumed that it must be part of my penetration test, which it wasn't. It was a real attack, and they responded appropriately." That is from Ira Winkler – one of our nation's greatest cyber security assets. We've been warned about the need for security

awareness for decades – now is the time to act. Cyber attacks are increasing in frequency, increasing in sophistication, and increasing in the damage they cause to both individuals and organizations. There are shining examples of organizations successfully implementing an effective, comprehensive security awareness program for their employees – but, nobody has done it on a scale which covers nearly 20 million individuals. This is the type of challenge for which New York has a history of successful solutions.

Cyber security protection measures been legislated over the years from both United States federal and state governments. In 1974, President Gerald Ford signed the Family Educational Rights and Privacy Act, known as FERPA, to protect the privacy of student education records – FERPA has a security awareness component. In 1987, President Ronald Reagan signed the Computer Security Act of 1987 to provide for the security and privacy of sensitive information in federal computer systems – this Act has a security awareness component. In 1996, President Bill Clinton signed the Health Insurance Portability and Accountability Act, known as HIPAA, to protect the privacy of individually identifiable health information – HIPAA has a security awareness component. State governments have also attempted to improve cyber security by increasing public visibility of firms with weak security. As I have previously mentioned, legislation alone cannot create a security aware culture. It must be coupled with

recognition and implementation of best business practices and why they are important. Governments have been "ringing the bell" about security awareness for decades. Those efforts, while important, have been somewhat fragmented. A comprehensive approach to security awareness is needed – now is the time to act.

The private sector has also raised the importance of cyber security through various "mandates". The most well known is the Payment Card Industry – Data Security Standard, known as PCI-DSS, which, since 2004, has set forth a set of requirements for enhancing payment account data security. Organizations, which take payment for products and services via VISA, MasterCard, Discover, American Express, and JCB, must follow these requirements – PCI-DSS has a security awareness component. The private sector has been issuing mandates addressing security awareness for almost a decade. Again, those efforts, while important, have been somewhat fragmented. A comprehensive approach to security awareness is needed – now is the time to act before a cyber Pearl Harbor attack strikes New York.

So, how can New York take action on this critical need to ensure that the nearly 20 million New Yorkers are familiar with security awareness best business practices as the "first line of defense" for defending New York from cyber attacks? How can New York

help its citizens, its consumers, its employees, and its corporations prevent cyber attacks?

- First, address the "actual problem". Traditionally, we spend approximately 75% of our cyber security budgets addressing the area where less than one percent (<1%) of security incidents actually occur – hardware and software – the technology level. Experts will quibble over the exact numbers – but, traditionally, we spend less than one percent (<1%) of our cyber security budgets addressing the area where 95% of security incidents occur – end-users – the human level. This is counterintuitive given this generally accepted principle – address the "actual problem".
- Second, develop a professional, comprehensive security awareness program for consumers, employees, and organizations. One which is built upon a common body of knowledge, created by instructional design methodologists, validated by subject matter experts, and measured by psychometricians. An independent third party should accredit this security awareness program – I recommend the American National Standards Institute, known as ANSI. ANSI is the voice of the United States standards and conformity assessment system – all security awareness programs should be ANSI-accredited. These are the essential elements of a quality security awareness program.

- And, third, implement this security awareness program as "preventive medicine" – not "reactive medicine". An effective security awareness program must produce a culture of security awareness among New Yorkers – much like doctors want their patients to live a healthy lifestyle all year. As my wife, who just retired after 29 years as a military officer in Navy medicine, puts it, "Cyber security is much like preventive medicine. It's about wellness; mitigating risk factors; and preventing injury, illness, and disease – not simply reacting to them." To be effective, the security awareness program must be a 365-days-a-year program – not a once-a-year program. The goal is to prevent cyber attacks – not simply to react to them. Remember, people are the first and last line of defense in protecting New York from cyber attacks – at the end of the day, security aware behavior is the only thing that matters. It's not about creating security experts – it's about living a healthy cyber security lifestyle and knowing when to call the cyber security "doctor". It's all about creating security aware behavior. To offer another analogy – my son was so proud a few years ago when he received his driver's license – demonstrating his awareness of the risks, responsibilities, and safeguards associated with operating a motor vehicle on the nation's highway system. I held some level of confidence that he knew how to drive safely. I believe we need to reach the point very soon where we can be assured individuals have attained a basic "internet driver's license", if you will –

demonstrating awareness of the risks, responsibilities, and safeguards associated with operating a computing device on the information superhighway. A critical component in defending New York from cyber attacks is to ensure all its citizens practice defensive computing – much like we teach our children to practice defensive driving.

Mr. Chairman, and the distinguished members of the New York State Senate, as Benjamin Franklin once famously said, "An ounce of prevention is worth a pound of cure." I'm not sure he was talking about cyber security – but, if New York takes proactive steps to prevent a cyber security incident from occurring in the first place, it will save a great deal more in time, effort, and cost than it would in trying to recover from the damage done later because attention was not paid to the potential problem earlier. Security awareness for all citizens is an ounce of cure!

Thank you.

Dow A. Williamson, CISSP, CSSLP, MBA

Executive Director, SCIPP International

Prepared Testimony and Statement for the Record of

Renault Ross

Technical Architect, Information Protection

Symantec Corporation

Hearing on

"Public Hearing on Cyber Security:

Cyber security: Defending New York from cyber-attacks"

Before the

Committees on Banks; Insurance; Veterans, Homeland Security and Military Affairs; Commerce, Economic Development and Small Business; Crime Victims, Crime and Correction; and the NYS Senate Select Committee on Science, Technology, Incubation and Entrepreneurship

November, 18 2013

Good afternoon Senators and thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Renault Ross, I serve as a Technical Architect for Symantec where I support Public Sector strategic programs, focusing on state and local education issues. My experience lies in virtualization, mobility, cloud and cyber security. Prior to joining Symantec, I worked as a global security architect at Bovis Lend Lease Corporation, and a member of the team that established the first global security program that included compliance, vulnerability management and incident response.

Symantec is the largest security software company in the world, with over 31 years of experience developing Internet security technology. We provide security, storage, and systems management solutions to help consumers and organizations secure and manage their information and identities. Our Global Intelligence Network is comprised of more than 69 million attack sensors in over 200 countries, and records thousands of events per second.

These resources allow us to capture worldwide security intelligence data that gives our analysts a view of the entire Internet threat landscape, including emerging cyber-attack trends, malicious code activity, phishing and spam. We welcome the opportunity to provide comments as you continue this important effort to bolster the state of cyber security. In my testimony today, I will provide you with:

- An overview of the trends from our Internet Security Threat Report of Internet threat activity worldwide from data obtained from our Global Intelligence Network.

- A Symantec best practice strategy that an organization can leverage to reduce the risk of losing PII to a security breach, malware or social engineering campaign.

- Recommendations on how the State can align with those best practices along with other mitigations and considerations.

Today's Threat Landscape

We rely on technology for virtually every aspect of our lives, from driving to and from work, to mobile banking, to securing our most critical systems. Here are some recent trends we identified in our latest Symantec Internet Security Threat Report (ISTR):

- We estimate that there were 93 million identities were exposed in 2012
- The average breach involved data for 605,000 individuals.
- Hackers make up 40% of these attacks, followed by 23% to theft from loss computers or drives.

[1] *Symantec Internet Security Threat Report* XVIII (April 2013), 17.
http://www.symantec.com/security_response/publications/threatreport.jsp
[1] *Id.*
[1] *Id.*

Symantec's recommended strategy to protect information
Includes a Governance framework to develop and enforce IT policies, Strong Access Control to Authenticate Identities along with Information Protection, Infrastructure Management and Infrastructure Protection.

Protecting information starts with the creation of a governance, risk and compliance program that consists of people, processes and technology. This includes dedicated people whose sole focus is ensuring that an organization conforms to stringent regulatory compliance requirements.

An example of regulatory compliance would be the Health Insurance Portability and Accountability Act (HIPAA) under which an organization must ensure that measures are in-place to prevent the disclosure of electronic personal health information. This would include administrative policies, technology and physical controls. Policy violation can lead to hefty federal fines from $ 50,000 per incident to a maximum of 1.5 million .

A couple of headlines:

- One company had to pay $1.7M after a hard drive was stolen containing Medicaid information
- Another company misplaced a USB drive containing PHI for 280,000 Medicaid recipients. Fines pending

An organization should leverage technologies that automate the assessment process to include producing on-demand reports to internal and external auditors to demonstrate compliance.

Access Control strategy to authenticate identities
An Access Control strategy makes it difficult for unauthorized personnel to access the network or system.

Currently, single-factor authentication is the traditional and less secure method. It requires only a user name and password. However, for increased security two-factor authentication is an approach which requires the user to provide two or more authentication factors.

An example of two-factor authentication is where the user would need to enter something they know, like their username and password, along with a random pin that changes every 30 seconds from a separate device like their mobile phone to access the network or system.

Information Protection strategy
Being aware of where sensitive information resides on a network, who has access to that information and where is it being shared both within and outside the network is core to an information protection strategy. Data Loss Prevention technology allows an organization to identify and block sensitive information from leaving the network.

It's not only the external bad actors trying to steal this sensitive information but in many cases its employees with privileged access stealing and monetizing this data.

To address this threat at Symantec, we deploy our own products across our large corporate infrastructure to protect our sensitive data. We've even tailored our Data Loss Prevention solution to scan for, identify, and enforce policy to protect PII and customer information. Because our Data Loss

Prevention "sensors" are tailored to protect such data, an alert will be generated within minutes of a violation and immediate actions are taken to protect exfiltration of the data (e.g., block, log and alert).

Infrastructure management and protection
Organizations are lowering their IT costs and gaining efficiency within their network infrastructure by moving services to the cloud (public or private) and embracing mobility.

As organizations improve efficiency, the cloud service provider or organization should deploy appropriate security protocols. Early warning threat intelligence, IT malware scanning coupled with other strong security tools will provide a layered defense against cyber-threats.

Finally, recommendations on how the state can align with those best practices along with other mitigations

Symantec recommends that the State:

A. Leverage Governance, Risk and Compliance technologies to ensure external mandates (HIPAA, PCI or SOX) are being met with policies and compliance reporting.

B. Consider using two-factor authentication to strengthen the security for user access. The State currently has an IT transformation project to provide Single Sign-on to state services. While Single Sign-on is a great way to allow the user to logon once with a single username and password and have access to multiple services, the downside is if those credentials are stolen, it would grant the criminal or adversary access to multiple systems.

C. Implement Data Loss Prevention technologies to safeguard sensitive information. This should be coupled with encryption which scrambles data and renders it unreadable to unauthorized users.

D. Use a layered defense of security technologies to increase the work effort of malware and deploy mobile security technologies. Also the State should continue to use early warning threat detection services (e.g, Multi-State ISAC).

In closing, with the threats and vulnerabilities on the rise, organizations big and small must first ensure regulatory compliance mandates are being met, increase security access to systems or network while making it difficult to exfiltrate sensitive information once inside the network.

Early warning threat intelligence and a layered defense approach will help to contain malware.

Thank you again for the opportunity to be here today with you as you address this very important issue and I welcome any questions at this time.

SYRACUSE UNIVERSITY

Good afternoon Senators Griffo, Seward, Ball, Valesky, Gallivan, and Golden. I am Professor Shiu-Kai Chin from Syracuse University. Thank you for the opportunity to speak with you today on the critically important topic of cybersecurity. I am a computer engineer. My job is developing methods, technologies, and most importantly, the people who assure the integrity and security of command-and-control in cyberspace. The work I do is used by the Air Force Research Lab as well as by JP Morgan's wholesale banking division to assure mission-critical cyber operations and high-value commercial electronic transactions.

Your committee's charge includes investigating best practices to prevent cyber-attacks. My Air Force boss, Dr. Kamal Jabbour, ST, Senior Scientist for Information Assurance says it best, he says, *"There is no threat without a corresponding vulnerability."* What this means is that we must build security and integrity into our cyber systems from the very start, not as an afterthought. Just like the cities of Holland, which are below sea level, are designed to eliminate vulnerabilities to the sea, we must design our systems with security and integrity in mind.

If you can only remember one best practice, please remember this one: security and integrity must be built-in from the initial conception of a system, into its design, and all the way through to its deployment and operation.

This best practice is oft-cited but seldom practiced. Why? Why should we believe that it is now feasible to adopt this best practice widely? There are three reasons.

1. Historically, the public thought security was unimportant, irrelevant, inconvenient, and too expensive. Your committee is evidence that this is changing.

2. Historically, the principles and technologies for realizing cyber security were thought to be too impractical and costly. Decades of research and new tools have changed this. Requiring systems be designed with security and integrity from the start is now a reasonable and prudent demand.

3. Historically, the mathematically rigorous design and verification of security and integrity of cyber systems was omitted from the undergraduate curriculum of engineers and computer scientists. The vast majority of engineers and computer scientists, now in practice, do not know how to design secure systems. Faculty across US universities thought these topics were irrelevant. Many still think they are beyond the reach of undergraduates. Eleven years of research and educational experiments with 300 undergraduate students from over 50 US universities say otherwise.

Given the shortness of time, I will focus on this last point. Educational institutions, such as Syracuse University, play a central role in the mission to educate and equip the next generation of engineers, computer scientists, bankers, lawyers, and policy makers with the competence and courage to do the right things that will turn the lawless shantytown that is today's cyberspace into a modern, reliable, safe, and secure system of systems, much like our modern global cities.

While all educational levels are important, the BS in engineering and computer science is especially important. Why? The standard for competence in the engineering profession is set by the BS degree. If we want better systems, a handful of PhDs is insufficient. We need thousands of rank and file engineers and computer scientists, who know how to specify, design, build, deploy, operate, and procure tomorrow's secure systems.

Do we know how to do this? Yes! There are eighteen of us. Eight of us are engineers, computer scientists, and mathematicians from AFRL, including Dr. Jabbour. Four of us are in private industry including three retired senior Air Force Officers. The remaining six of us are professors from Syracuse University. This government, industry, and academic partnership in cyberspace research and education, is in its twelfth year of operation. Together, we have created and executed:

- The AFRL Advanced Course in Engineering Cybersecurity Boot Camp,
- The AFRL Information Assurance Internship, and
- The Syracuse University 18 credit hour Cyber Engineering Semester.

Together, we have graduated 300 undergraduate students from 50 US universities. Together, we have educated and equipped these graduates to:

- Build security into systems from the start,
- Relate what is happening at the bit and byte level of computer hardware to the desired outcomes and end states that reflect commanders' intent,
- Use methods that enable third parties to rapidly, easily, and thoroughly reproduce, audit, and verify the soundness of our designs, actions, and operations, and
- Solve real problems, not hypothetical ones. One real problem we have tackled is in wholesale banking. Our assurance methods are used to mathematically verify the logical soundness of credentials used to authenticate users and sign transactions. A single electronic transaction, unlike consumer transactions, could be worth upwards of several hundreds of millions of dollars. In these cases, there is no room for error. The methods we use in that real-world example are the same methods we teach our students.

In short, we have over a decade's worth of experience figuring out what works and what doesn't when it comes to educating future cyberspace leaders. Our goal is to share this knowledge widely, educate as many students, faculty, and practitioners as quickly as we can, so collectively we can secure mission-critical infrastructure such as financial services, power grid operations, communications, command-and-control, and governmental operations.

Please, see for yourselves what we are doing. Come visit us at SU and meet with our partners at AFRL and in private industry to see this working long-term partnership in action.

Let me leave you with this thought: this government, industry, and academic partnership could be the core of what amounts to a national cyber service academy. This academy, right here in Central New York, could fill a national need. We know how to do it. We just need the resolve to do it. People are already coming from all over the country (and from the United Kingdom) to our programs.

If we build it, they will come.

Thank you for your time and attention. I am happy to answer your questions.

SYRACUSE UNIVERSITY

"Fast Facts"
Regarding the Academic Role in Cyber Security

Shiu-Kai Chin, Ph.D.
Professor, Dept. of Electrical Engineering & Computer Science
Laura J. and L. Douglas Meredith Professor for Teaching Excellence
Syracuse University, Syracuse, New York

- Our nation's information technology infrastructure could be described as a cyberspace "shantytown"...Through the years, it has been cobbled together in an ad hoc fashion, like hastily built settlements in the Old West. It won't take much of a 'storm' to destroy it. We need to start rebuilding, better.

- The "Internet of Things" (appliances connected wirelessly to smartphones connected to other devices, etc.) leaves huge, widespread vulnerability.

- Academic engineering programs must be revamped to make sure the nation can address this situation...the Bachelor's Degree is the baseline for competency. Overall US programming competency is on the decline.

- Our nation's cyber graduates need to be:
  - Tough-minded problem solvers at the operational and tactical levels
  - Thoroughly aware of the workings of cyberspace and organizations
  - Mindful thinkers who are aware that things may not be as they appear
  - Effective at leading upwards
    - "It's a lot easier to speak up when you know what's right, you've done the math, and others can verify your claims quickly."

- We need thousands of engineers capable of mathematical analysis and leadership in support of designing, verifying, procuring, and operating cyber systems

- To start building that supply, Syracuse University works with members of the military (active and retired), including Rome Air Force Research Lab, to develop cyber curriculum that as its basis calls for rigorous mathematical and logical analysis and reasoning
  - AFRL Information Assurance Internship: Jointly taught by AFRL, industry, and SU
  - SU Cyber Engineering Semester: Junior Year, 18 credit hours, jointly taught by SU, AFRL. Unique program functions as a "study abroad" program for students from other colleges across the country. They come to SU for this demanding systems assurance training.

- We are optimistic!

SYRACUSE UNIVERSITY

Steve Chapin, Syracuse University
Associate Professor of Computer Science
Department of Electrical Engineering and Computer Science

- Current best practices in software and system development embody ad hoc methods developed over decades. These methods are good, but not perfect. A malicious actor only needs to find one flaw to exploit.

- Best practices give rise to a fragmented, variable security landscape, with some parts of the system defended in depth, some parts unprotected, and still other parts with conflicting defenses.

- Security cannot be patched in *ex post facto*, but must be considered from the start. Many systems were originally designed in environments where security was not a concern, and later have partial security grafted on.

- Academic research serves as a source of new methodologies, techniques, and technologies to address pressing problems, such as cybersecurity.

- We need holistic approaches to security, taking into account core technologies, management, economics, regulation, and most importantly, users. Within a single system, our solutions must encompass all levels of hardware and software. We also must consider both improving the security of legacy systems and how to develop better new systems.

- New models of system development, which can prove systems are free of entire classes of flaws and vulnerabilities, are in their infancy, but hold great promise for the future. Syracuse University is on the forefront of this movement, developing tools for proving system properties and applying these tools to ensure systems only run programs that are trusted.

- Systems are often trapped by backward compatibility concerns, but at the threshold of new epochs, the opportunity exists to start from a clean slate with security as a primary focus. We stand at such a threshold in the area of the Smart Grid. Researchers at SU are developing net methods to ensure the security and privacy of electric vehicle charging in the coming Smart Grid.

SYRACUSE UNIVERSITY

Good afternoon Senators Griffo, Seward, Ball, Valesky, Gallivan, and Golden. I'd like to thank the Senators for the opportunity to speak today. I am Steve Chapin, an Associate Professor of Computer Science at Syracuse University, where I specialize in the study of computer operating systems and cybersecurity. During my career I have developed grid computing systems, done research with the Air Force Research Lab, DARPA, and the NSF, as well as local companies in upstate NY, and spent four years as part of a team overseeing Microsoft's compliance with the consent decree in the Netscape case (US v Microsoft). This background has given me both experience in building secure systems and insight into how large, complex software systems are currently developed.

Current best practices in system development employ ad hoc techniques and heuristics developed over decades, and rely on testing of the resultant system to detect flaws and vulnerabilities. Such testing is often, by necessity, limited to components of an overall system that is too large to test as a whole. This can lead to outcomes such as the northeast power outage of 2003, in which individual components responded properly to overloads, but the overall result was system failure. The result of these ad hoc practices is a fragmented security landscape with variable protection. Some parts of the system are well-defended, while others are unprotected; some security solutions are mutually incompatible, rendering defense in depth impossible (e.g., many virus scanners do not allow the use of a second scanner).

Another challenge is that many of our extant systems were first conceived and developed under constraints and assumptions that no longer hold, and in particular, in which security was not a consideration. The Internet was originally developed as a research network with access limited to government and academia. The Windows operating system evolved from desktop computers that lacked networked communication. Cell phones running on closed networks have grown into smartphones that now connect to the Internet through 3G and WiFi. In each of these cases, responding to the security requirements of a new environment required wrestling with backwards compatibility and an installed base of systems and users that either were not interested in or were not capable of integrating new security mechanisms and procedures.

I wish to restate that last point: we cannot rely solely on Industry to provide secure systems---not because they are somehow evil or incompetent, but because the current market does not reward them sufficiently for doing so. This is particularly true when developing a new, secure system would require introducing incompatibilities with existing systems. The very success of a system can create a backwards compatibility trap for its manufacturer, making it too costly to radically change a system or product. Government and Academia, providing regulation and research, can team with Industry to move towards global, rather than local, optima. If our goal is to get to the top of the mountain, we don't want to be stuck at the top of a neighboring hill because our only plan is to climb higher. Sometimes we need a push to find the right place to climb.

How, then, do we escape our current "patch and pray" approach to security? There are three key principles for future solutions:

1. Security as a first-class product requirement: Security must take on a status equivalent to that of performance, efficiency, and cost. New products and features must be evaluated in the context of how they affect the security of the system as a whole.

2. A holistic approach: Security must take into account aspects of the overall system including technology, management, economics, regulation, and end users. A perfectly secure system that is too difficult to use is doomed to failure. Holism also implies working across all levels of the hardware-software stack, including secure architecture, operating systems, applications, and communication.
3. Formal verifiability: To bring rigor into the design and development of secure systems, we need to be able to prove that they have security properties. Not only that, we need to enable others to verify those properties.

My colleague, Dr. Shiu-Kai Chin, is testifying today with a focus on the implementation of these principles in education. I will devote the remainder of my time to describing research projects at Syracuse University that demonstrate these principles in action.

We are working with a local company in Utica, Critical Technologies, on an AFRL research contract to develop secure booting technologies. This technology will allow us to prove to users that their computers (or tablets, or phones) are running only the software that they are supposed to be--if an attacker corrupts or inserts any software in the boot process, our technology will refuse to load it. This is the first, necessary, step in having trustworthy computing systems. We are starting from scratch, using formal models so that not only can we build a secure boot loader, but anyone who wishes to can verify those security properties themselves.

In another project, Syracuse University researchers from across multiple disciplines---including Law, Economics, Computer Science, Computer Engineering, and Electrical Engineering---are working together to design secure charging and discharging protocols and service equipment for electric vehicles in the Smart Grid. We are addressing issues in regulation, markets, and security in concert with solving the core problem of moving electricity, using formal methods to verify the security of our work. This is an example not only of the holistic principle but also of an opportunistic paradigm shift. At times, we stand on the threshold of a new epoch of technology, with the opportunity to do a clean-slate redesign of a system. Because Smart Grid technologies are still in their infancy, we have an opportunity to do security "from the ground up" before there is significant resistance arising from existing insecure infrastructure.

In conclusion, I believe that New York State has the resources, in Academia and Industry, when supported by Government, to effect real gains in cybersecurity. I have described two research projects at Syracuse University demonstrating the key principles I outlined, and showing multidisciplinary collaboration between Academia, Industry, and Government. This is only a small fraction of what we do, but I must limit my remarks due to time constraints. I welcome further opportunities to discuss our research, and am happy to answer questions.

725 Daedalian Drive
Rome, New York 13441
Phone: 315-617-2821

Pioneers of Cyber Innovation

November 18, 2013

"Cyber Security: Defending New York from cyber attacks." Public Hearing

TESTIMONY

Prepared for the New York Standing Committees on Banks; Insurance; Veterans, Homeland Security and Military Affairs; Commerce, Economic Development and Small Business; Crime Victims, Crime and Correction; and the NYS Select Committee on Science, Technology, Incubation and Entrepreneurship.

Senators Griffo, Seward, Ball, Valesky, Gallivan and Golden:

Thank you for the invitation to present testimony on cyber security and the importance of New York taking the lead on initiatives that meet the challenges head on. I'm the Executive Director of the CYBER NY Alliance whose mission is to Promote, Advocate, Strengthen and Expand our New York Cyber Eco-System in collaboration with our cornerstone asset, the Air Force Research Laboratory Rome Research Site (AFRL Rome), here at the Griffiss Business and Technology Park. Our goal is to develop ***"Cyber Valley" with CNY as the nerve center and information clearinghouse on cyber technology***.

The term cyber captures those technologies that have immersed us into a digital world through the use of wireless communications and networking, the cloud, and mobile apps. Everyday conveniences and efficiencies in business and our personal lives are overshadowed by the impact of attacks on our mobile devices, systems and infrastructure. Whether we are talking about privacy or national security and stability, cyber security is a national priority.

My testimony provides a detailed look at the cyber vulnerabilities and attacks that are growing with time. I also will talk about three Central New York resources, AFRL Rome, the New York State Cyber Research Institute and our Nanotech initiatives that offer a one of a kind research and development cluster that will provide the platform for the creation of cyber security solutions while also generating private sector business opportunities and employment.

The Central New York high-tech ecosystem has been doing research in cyber security before the term cyber existed. AFRL Rome (at the time, Rome Air Development Center, RADC) was part of the original internet (ARPANET) development team, and has been involved in network research, tools, and applications for over 40 years. The laboratory now manages science,

725 Daedalian Drive
Rome, New York 13441
Phone: 315-617-2821

Pioneers of Cyber Innovation

technology, and advanced development revenue in excess of $900 million per year, and together with its local and national partners, represents one of the largest concentrations of person-years of cyber security experience in the world. The Deputy Assistant Secretary of Defense for Research, Dr. Reginald Brothers refers to AFRL Rome as one of our nation's crown jewels.

Though the laboratory itself focuses on technology development for application to the defense and intelligence communities, information science and technology is ubiquitous. The CNY community, its regional colleges and universities, and its private industry contractors are transitioning that technology to a diverse range of application domains, including finance, healthcare, transportation, critical infrastructure, and everyday home networking and entertainment. It is with this background that the CYBER New York Alliance provides this perspective on cyber security priorities facing the State of New York today and in the future.

The first thing we want the people of New York to understand is how prevalent and real the threat of cyber attack is. It has been conservatively estimated that 50% of all general-purpose computers in the US are infected with malware. Researchers at Kansas State University have estimated that an unprotected computer can get infected within 8 seconds of connecting to the internet. Such infections are becoming more and more sophisticated, and in many respects, more difficult to prevent, contain, and control.

Although modern operating systems and commercial anti-virus software products are successfully able to prevent publicly known attacks, there is a largely uncontrolled class of attacks – the Advanced Persistent Threat, or APT – that represents a much more insidious and potentially harmful threat. APTs are threats from highly skilled and trained, well-organized and well-funded organizations. They are world-class experts in malware and computer security, and they know more about computer vulnerabilities than all common users, and most information security experts. They may be state-sponsored, but are mostly non-governmental organizations with a network of agents distributed world-wide, protected by a network of intermediate organizations and networks.

A typical APT begins with surveillance of online activity, through openly available data such as social networks or "sniffed" data streams. When a computer or network of interested is identified, access to that resource is usually trivially easy, using so-called "exploits" that are openly traded or easily discovered in the complex software we use every day. When malware has infected a device, it will connect to a network of command and control servers. The command and control network usually includes machines in the target country that have been infected with "bots" that act as intermediate communication nodes between the malware and the sponsoring/controlling entity. In this way, a great many computers, owned by law-abiding companies, agencies, and individuals become part of the APT network. Many home and business

CYBER NY ALLIANCE

725 Daedalian Drive
Rome, New York 13441
Phone: 315-617-2821

Pioneers of Cyber Innovation

users are often surprised to find that their machines are part of a "bot-net", controlled in China, Korea, or Kazakhstan.

Once malware is established on a target computer and connected to the command and control infrastructure, it generally has free reign to examine files, communications, and user input, and to exfiltrate that information. It can also replicate itself, infect other devices that are connected through the users' messages and cloud activity, and further strengthen and grow the malicious botnet. It is estimated that cyber crimes committed via such APT scenarios costs users in excess of $113billion per year, with a million people affected each day.

Such scenarios are not limited to traditional desktop computers. One of the fastest growing trends is for cyber attack on mobile and non-traditional devices. Although 49% of mobile computer owners (smartphones, tablets, etc.) use these devices for both personal and business applications, only 26% employ any form of security software. It took the Android mobile operating system only three years to generate as many malicious applications as PC/Windows systems did in the past fourteen. It is projected that by the end of 2013, there will be 1million malicious Android applications in circulation.

One of the reasons for the rate of growth of the mobile malware threat is the accelerating prevalence of cloud computing and remote networking. Distributed data storage and the use of unprotected WiFi connections facilitate the propagation of bots, malware, and other information (such as personal information from social networking). This allows people to easily transport their data, messages, and business information, but it also allows them to transport the APT threat.

Such threats indicate that not only do we need cyber security technologies of growing sophistication and complexity, but also an increased level of awareness and training for everyday users. They also illustrate that determining the source of the "next" threat is no harder than determining the latest trends in commerce, industry, and society. Like the criminal who robs banks "because that is where the money is," the threat will follow the opportunity. When social networks became prevalent, criminals co-opted them for malicious purposes. As the healthcare and transportation industries adopt software- and network-based technologies for control, access, and dissemination, so will the APT community. Automotive electronics, smart-cards, pacemakers, and public utility control systems are all vulnerable to intrusion, and when it becomes profitable for the attackers' monetary, political, or other motivations, they too will be attacked.

But it is sometimes too easy to blame the user for the cyber threat. There are many serious cyber security threats that we cannot prevent or defeat through training, education, and behavior modification. The Georgia Institute of Technology (Georgia Tech) predicts that the "supply

725 Daedalian Drive
Rome, New York 13441
Phone: 315-617-2821

Pioneers of Cyber Innovation

chain" will be a cyber threat of increasing concern for 2013 and beyond. Supply Chain threats are those that result from malicious capabilities built into software and hardware that the government, industry, and consumers buy for integration into larger networks and systems. Undocumented access vectors, or "backdoors", can be built into software or hardware, and can be found not only in counterfeit programs and equipment, but also in legitimate and authorized systems for which such backdoors were never suspected or detected.

In 2008, the FBI broke up a ring of distributors of counterfeit Cisco routers, manufactured in China, that were sold to the U.S. Navy, Marine Corps, Air Force, the FAA, and the FBI itself. Researchers have repeatedly demonstrated ways that computer chips software programs can be equipped with backdoors that evade even the most sophisticated testing and quality assurance methods. With globalization of high-technology component markets, most industrialized countries have distributed their supply networks world-wide. Neither the technology nor the resources yet exist to adequately test the integrity of component devices, and that means that no device of any reasonable complexity can be fully trusted, and there is not much we can do about that. This fact has spawned an entirely new emphasis in "cyber security for mission-assurance", which adopts the premise that our computing and networking technologies can be used to achieve trusted missions, even if the components themselves are not trusted.

With this characterization of the breadth and seriousness of the threat, we would like to summarize our message. It has long been recognized that the cyber "domain" is one that has a low "barrier to entry," and is characterized by "asymmetric advantage for the attacker." Together, these terms mean that the threat can come from anywhere, and is difficult to defend against. Complete and impervious defenses can result only from an impervious shield that faces all directions, and such an approach is difficult. More comprehensive approaches are required, such as technologies for resilience, reconstitution, and adaptation. Like the goal to achieve "mission assurance" in the face of uncontrollable threats, these goals are moving targets. The threats are ever-changing and will not go away. Just as the threats themselves are persistent, so must be our responses. Not only do we require diligence in our operations, care in our design, and vigilance of our users, we require a steady-stream of advanced research, rapid commercialization, and lifelong education.

The CYBER New York Alliance recognized the breadth and seriousness of today's cyber threats and with the support of Senator Griffo, Assemblyman Brindisi and Governor Cuomo, we worked to establish a New York State Cyber Research Institute (CRI) in 2012. The CRI provides the basic research and "discovery" function for sensitive and classified cyber research; leveraging the ground breaking cyber security work being done at AFRL Rome and transitioning that technology to a diverse range of application domains, including finance, healthcare, transportation, critical infrastructure, and everyday home networking and entertainment.

725 Daedalian Drive
Rome, New York 13441
Phone: 315-617-2821

Pioneers of Cyber Innovation

The creation of the CRI is another example of New York's recognition of the importance of and commitment to proactively addressing our cyber security challenges. The CRI will work to solve the complex problems, answer the tough questions and develop the tools that will address the Governor's Cyber Security Advisory Board and the Office of Cyber Security challenges.

The CRI is a critical step for New York State's progress in securing cyber security research and development as an economic development engine. Nowhere else in the country is there the depth of information systems knowledge and creativity than in Central New York. The CRI will enable the region to attract and retain the best academic and advanced research expertise. The CRI will facilitate multi-university collaboration for education, technology transition, and entrepreneurship in the region. This is a huge opportunity for the region to capitalize on its historical strengths and potential for local, regional, and national security priorities.

Also underway is collaboration between the CRI, SUNY IT, the College of Nano-scale Sciences and Engineering and AFRL Rome to address trusted processor and system component development challenges. Initiatives are kicking off that will harness the power of innovative manufacturing technologies, Nano chip fabrication technology, 3D chip stacking, and advanced cyber security methods that will enable the development of US based trusted hardware and software that will help secure our critical infrastructure. This will lead to powerful and cost effective solutions that meet current and future information device needs and drive innovation for a strong manufacturing business market.

By fostering the research, industry and educational ecosystem surrounding technology development for cyber security, NYS and CNY are poised to be a critical national asset to address national defense and commercial cyber threats; staying one-step ahead of our attackers, and positioning ourselves between the threats and our economy, and that is the least (and perhaps the best!) we can do.

Respectfully,

Mary Carol Chruscicki
Executive Director, CYBER New York Alliance

Testimony of William (Tony) Cole, VP / Global Government CTO, FireEye Inc.

November 18th, 2013

Cyber security: Defending New York from cyber attacks Public Hearing

Griffis Institute

Rome, NY

First, I would like to thank the New York State Senate and the Great State of New York for inviting FireEye to testify today. It's a dramatically changing world we live in today with many new threats and I'm encouraged to see our leaders take note of this and react accordingly to understand and counter these new threats that could dramatically impact our way of life.

How did we get here? The speed at which technology is progressing today is at an almost unbelievable and phenomenal pace. If you look back at the inventions during the last two hundred years and then the last ten years in detail, it's hard to imagine what the world will look like ten years from now. Just think, in 1903 the Wright brothers took their first flight and only sixty-six years later we put a man on the moon. Here we are today with many people carrying more processing power in their smartphone than what was needed to launch our Apollo missions. In fact that pace of innovation has continued to quicken, with just last year, a bioengineer at Harvard managed to store 700 Terabytes of data in a single gram of DNA. When we look at the world today, it's hard to keep up with today's inventions and new discoveries, let alone contemplate what the future will hold for us. This new wave of

innovation may have driven new ways to communicate, drive additional business, and allow our governments to more closely and frequently interact with their constituents however it also has a dark side. Our adversaries have also used this wave of innovation to identify new ways to attack us. Through the same social media we use for daily communication with our loved ones, business partners, and our government agencies, we put enormous amounts of data out there about ourselves. This gives would-be attackers a large picture of our daily lives from multiple perspectives and helps them craft a targeted attack that is difficult for any human to resist viewing. If you have young children and you received an email stating their daycare facility is on fire, would you open the attachment or click on an embedded link for more information? Who wouldn't? We're all human and having that inherent care and concern for others isn't something you can change so the risk is real and will remain for the foreseeable future. Crafting and sending a single targeted email or spear phishing email with either a weaponized attachment or an embedded link to a malicious website thats hosting malware to a single individual can be the start of a successful campaign that could devastate an organization or company. One single email.

Today we may only be at the dawn of the Internet Age, however cyber attacks have already proven themselves as a low-cost, high-payoff way to defend national sovereignty and to project national power. In fact many of today's headlines seem to be pulled from the pages of a science fiction novel. Code so sophisticated it destroys a nuclear centrifuge thousands of miles away. Malware that secretly records everything a user does on a computer, a software program that steals data from any nearby device that has Bluetooth connectivity, and encrypted code that decrypts only on one targeted device. Such sophistication speaks volumes about the maturity, size, and resources of the organizations behind these attacks.

Some surveys indicate that 50 percent of small businesses believe they are immune to targeted cyber attacks.

The levels of required expertise to launch these attacks are shrinking from a common standpoint. Would-be attackers can go into the underground areas of the Internet or Darknet and find code they can buy or borrow, expertise they can rent, or even rent compromised systems they can use for attacking other systems. Many of these products actually come with maintenance and support from the criminals and organized crime organizations that are building them. Also of significant concern are Flame, Operation Aurora, and a number of other cyber attacks that have set an entirely new standard for their complexity and sophistication. We're also seeing what is perhaps the world's most popular and notorious malware exploit kit, Blackhole which combines technical dexterity with an entrepreneurial business model to arm cyber attackers with the latest exploit updates coupled with enterprise-level support and zero-day updates. Fundamentally these developments make it clear that the cybercriminals and nation-states waging these attacks are growing increasingly sophisticated at stealing and sabotaging customer data as well as intellectual property. Leveraging changing or dynamic malware, targeted spear phishing emails, multi-stage attacks, and a host of other tactics, these attacks bypass traditional security mechanisms currently in place.

How prolific is the threat? No organization is immune: Cyber attackers routinely breach 95 percent of organizations to steal intellectual property, customer records, and other sensitive data and many of those organizations thought they had sufficient protection in place.

On that note, let's discuss the attackers and why they want access to our systems. Today we suffer from attacks from what most cyber security experts categorize as three different types of attackers; Nation-State backed attackers, Cyber Criminals, and Cyber Terrorists. Understanding each type of attacker can help us understand what they want and how we can potentially counter their attacks.

Nation state attackers have typically been the ones getting all the press as of late. They are well resourced and some, as recently industrialized nations, are attacking other nations to steal intellectual property to allow them to more quickly compete and win business in this competitive global economy. As if this isn't bad enough, we're also seeing mass stealing of national secrets for even more nefarious means, such as a future war. How do you win a war quickly in the not too distant future? Why not use your cyber experts to infiltrate the enemy's computer systems so you can disrupt them at will? Why not compromise their entire critical infrastructure so you can deny them power, water, and other vital commodities? Why not also steal all of their battle plans? You could likely win a war without putting many of your own countrymen in jeopardy simply by using electronic means to disable and disaffect any IT dependent nation.

Cyber criminals are now stealing so much money they've become an integral part of organized crime. They are using similar tools and tactics as nation state attackers to steal money from financial institutions or any organization that handles money although they are typically even more sophisticated to elude detection mechanisms.

Cyber Terrorists are a growing concern since they don't want to steal; they want to destroy our way of life. They are no different than regular terrorists and are part of the same organizations that exists today, however it is a growing concern that with the proper resources and a concerted effort, they could do massive harm to our country.

Nation-State attackers today continue to be the largest concern for most cyber security experts since they continue to compromise our systems, steal our national secrets, our intellectual property, and leave behind hidden code that allows them persistent access to our systems where they can return at their leisure to steal more data or worse yet, disrupt our systems during a future conflict. It's bad enough that we lose data on a continuous basis to these attacks, however what's truly terrifying is the possibility of a future attack on a previously compromised system that takes down our power grid, or water system, or fully opens our dam spillways with no notice. All of the actions I just stated are certainly possible with today's interconnected and very vulnerable systems that we rely on for our daily lives.
In the new era of cyber warfare, states, cities, and towns are directly in the crosshairs. Never before have state and local governments been expected to do so much with so little. Even as budgets remain tight in a post-recession environment, tech-savvy citizens demand higher levels of service. They want to pay taxes by credit card, renew their driver's license online, and do their banking from their smartphone. These responsibilities make cyber security critical for state agencies, municipalities, and public utilities. Governments possess residents' most sensitive information—including inviolable personal data such as Social Security numbers and birth certificates.

Clifford Clarke, CIO of the Public Technology Institute (PTI), in a recent interview with public policy magazine Governing the States and Localities stated "Personal data tends to be undervalued," and also that "Some municipalities don't think they have anything to protect." Equally critical for state and local governments is safeguarding critical infrastructure. Dams, freeway systems, power and water plants, airports, and emergency communication, are among the vital assets that either sit within or potentially fall under state or local purview.

U.S. officials, including President Barak Obama, have grown increasingly alarmed by the threat of attacks against state and municipal governments. In an editorial urging congress to pass the Cyber security Act of 2012, a law designed to strengthen cyber defense, Obama warned "computer systems in critical sectors of our economy are being increasingly targeted." He also stated "The lack of clean water or functioning hospitals could spark a public health emergency," he wrote. "And as we've seen in past blackouts, the loss of electricity can bring businesses, cities, and entire regions to a standstill."

In 2012, U.S. Defense Secretary Leon Panetta warned of a looming "cyber Pearl Harbor" surprise attack against utilities or transportation systems. He cited online breaches that have already occurred of control systems for chemical, water, and electrical plants, as well as public transportation control software.

And former U.S. Department of Homeland Security Secretary Janet Napolitano, in her farewell address, warned of "a major cyber event that will have a serious effect on our lives, our economy, and the everyday functioning of our society."

In the first half of 2013, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to more than 200 incidents across critical infrastructure sectors—

more than twice the volume of attacks in all of 2012—with half of those targeting electrical utilities. In May 2013, the U.S. Department of Homeland Security warned local governments that they were among the hundreds of high-profile targets identified by a group of Middle East and North Africa based criminal hackers known as "OpUSA." At the same time, many state and local agencies are not ready for the inevitable assault. In a recent survey, 44 percent of federal, state, and local government IT workers said their infrastructure was not prepared for cyber attacks.

Why are they successful and what can we do? Today's attacks are successful primarily because we built a security infrastructure around knowing and understanding what vulnerability and its associated malware characteristics look like and then we created a signature for it. Those signatures today are fed into almost every commodity security product we rely on to protect us. Attackers became wise to this and started reviewing code themselves to find new vulnerabilities that we would not know about and therefore not have signatures in place to detect, hence the name zero-day. It's inherently difficult to defend against threats you know nothing about and requires a new strategy.

What can we do? We must being to think differently and change how we react. The National Institute for Standards and Technology or NIST has started to quickly review and change their recommended policies and practices around cyber. In fact earlier this year NIST updated 800-53 which is the Security and Privacy Controls for Federal Information Systems and Organizations guide to Revision 4 and added new information. In my opinion, the most important change was the addition of Security Control 44, which outlines a need for detonation chambers. Why is this significant? Because it allows cyber defenders to see if

any attachments or website links (or URLs) are malicious in nature by reviewing what actions take place when those attachments are detonated or opened in a virtual environment. This includes emails with URLs embedded in them allowing you to see how the virtual system reacts. Does it attempt to download additional code? If so, why, what is the purpose? Stop those attacks at the perimeter by reviewing everything coming across the wire. You don't need to understand a vulnerability thoroughly to understand that your Adobe PDF file you just pulled down to read should not be beaconing back out to another server on the Internet. Education is critical as well. Task all organizations to understand that the threat is severe and can affect their way of life and train them around proper use of computer systems while exercising due care. We should drive more attendance in STEM education programs to build the needed expertise; adopt the NIST standards; demand architecture reviews, review new code before placing new systems online; conduct penetration tests on our own systems. There are many other things that we need to also be concerned with in defending our digital assets however since our time is limited, I'll close with the fact that we must change our current mindset and become agile in updating our processes, our policies, and our buying habits if we are going to succeed in protecting our data from our cyber adversaries. Our adversaries are innovative in their attacks and will continue to be, so we must also be innovative in our responses to their attacks if we wish to remain a great country.

I'm happy to see the Great State of New York realizes we have a problem that is growing in size and complexity and is taking action. Thank you for your time and attention.

Good afternoon:

Senator Griffo, Senator Seward, Senator Ball, Senator Valesky, Senator Gallivan and Senator Golden.

I appreciate the efforts of this committee and look forward to your findings. I am Peter Muscanelli: Vice President of Sales and Marketing for Colt Recycling and Refining. Colt is a fully integrated Electronics Recycling Company serving NY and The America's. I have been involved in the Electronics Recycling and Data Destruction industry since 1989.

The fact is: **"we have a problem"** and that problem is: **the illegal harvesting of data by criminal elements.**

My testimony today: is important to everyone who has a computer, cell phone, laptop, or other data storage devise. It doesn't matter if you use a portable devise like your cell phone tablet, office copier, search the web at a library, a friend's home, or view social media sites. **"You are vulnerable and at Risk"** however this risk is different.

Cyber security threats do not always come from the web.

I think a little history would be helpful to understand this vulnerability. When computers first became available there use was limited and often in controlled environments.

That has all changed: cell phones are readily available and contain more information, with more functionally. Than a full size computer did twenty years ago.

Most people take their electronics for granted and the data contained on them as safe as being in a banks vault.

That just isn't so.

Information is valuable and criminals know that.

Earlier Computers contained a hard drive. Individual's, business and governments learned the hard way, what happens if a hard drive is not correctly handled. Most of those lessons occurred at the **End of Life** for that equipment. There are many news stories, about computers found with sensitive data, personal data, or corporate or government records that were compromised by mishandling.

Awareness was built to understand the risk of mishandling and to help ensure the hard drive was destroyed the data tapes and back-ups, were wiped, shred or destroyed to minimize their cyber security exposure.

So the question we must ask is: Do you know where your data is stored on each devise you use?

The answer would have been:" the hard drive". But there is no hard drive on a cell phone, thumb drive, or even a tablet.

So the **risk has changed**: Once again we must learn how to manage this risk. Electronics can contain gigabytes and even Terabytes of data much of this data is on Solid State Drives and are not easily identified. The data chips can reside anywhere on the circuit board making it difficult to find and physically destroy. So how does End of Life equipment increase our Cyber security threat? **Very Easily**

Criminals look for the **point of least resistance.** Criminals cast a wide net to harvest a few select bigger opportunities. They can target an opportunity by purchasing equipment at surplus, on the web, from the local resale market or steal it. Then criminals can re-engineer a company, government or person by harvesting information from that End of Life equipment.

Most people think of **cyber security** as a threat from the internet. They do not feel there old cell phone, office copier, or other devise can be the **key** that unlocks there life, Corporate records, or government data to a criminal enterprise. The cyber thief doesn't have to crack code; they can get data that will let them in the front door by getting some surplus equipment with data. This happens more then we think.

I would like to share just three stories of equipment that came to our facility. The equipment was screened and cleared for recycling by IT staff. The data we found would have been detrimental if it fell into the wrong hands.

The **first incident** that I would like to tell you about was a state agency that refreshed 500 computers, all of the hard drives were to be removed before recycling. We received the computers in for processing and our de-manufacturing team found 6 hard drives all containing data. When we contacted the agency they said that was impossible. Only when they visited our facility did they realize how vulnerable they were and confirmed the six hard drives were threes.

The **second Incident** involved a large corporate client who shipped us a load of mixed electronics. One of the pieces was a photo copier; upon de-manufacturing of the piece a hard drive was located. The hard drive contained thousands of pages of documents many labeled "confidential".

The **last incident** troubles me most: a Department of Defense contractor who has the most sensitive data and has redundant systems in place to check equipment before it leaves there facilities have sent several devises containing data. The nature of this data would have compromised our national security. The list goes on and on: A law enforcement agency that sent us a digital camera with crime scene photos, a corporate attorney who sent a cell phone loaded with all his data and emails.

When we think of Cyber Security we have to think of all areas of risk which includes the End of Life aspects. The risk assessment has to take into account that data can sit on a

devise and is often forgotten about, then found when that devise becomes surplus maybe by a cyber thief.

This is a risk where we have a solution.

This committee should consider a protocol that includes all necessary procedures that ensures data is removed from all surplus, end of life electronic equipment. **We need to hold individuals, corporate and governments accountable for acts of leakage.** Colt processes several hundred tons of End of Life electronics monthly along with other recyclers. However: Colt has developed a redundant tiered approach to handle all data, so it cannot be compromised. There is no standard in place to ensure all recyclers, asset recovery facilities, individuals, corporations or Government agencies guard against this cyber threat.

This committee should also continue to build awareness by educating all stakeholders to the importance of this End of Life cyber security threat.

I thank you for giving me the privilege to testify.

I commend your efforts, and will take your questions.