Written Testimony
U.S. Senate Committee on Commerce, Science & Transportation
Arthur W. Coviello, Jr.
Executive Chairman, RSA, The Security Division of EMC
July 25, 2013

Introduction:

Chairman Rockefeller, Ranking Member Thune, and Members of the Committee, my name is Art Coviello and I am an Executive Vice President of EMC Corporation and Executive Chairman of RSA, The Security Division of EMC. Thank you for the opportunity to testify today regarding the National Institute of Standards and Technology (NIST)'s work with industry in the area of cybersecurity. Today's hearing topic is one that is close to home for our company. EMC and RSA have enjoyed a partnership with NIST that has spanned decades, and we are pleased to be working with them today to enhance our nation's cybersecurity.

RSA provides security, compliance, and risk management solutions for organizations worldwide. We help the world's leading organizations succeed by solving their most complex and sensitive security challenges, making it possible for them to safely benefit from the tremendous opportunities of digital technology and the Internet. EMC Corporation is a global leader in enabling businesses and third-party providers to transform their operations and deliver Information Technology (IT) as a service through innovations in big data, cloud computing and data storage.

The United States, like many other nations, is highly dependent upon IT. Everything from national security and intelligence, to commerce and business, to personal communications and social networking depends on networked systems. The dynamic nature of this sector has created millions of jobs and generated significant economic growth. Every day, the Internet is increasing productivity; driving globalization and political change; and fueling every major industry and economy in the world.

Unfortunately, that same dynamism has given rise to an ever-evolving cyber threat that threatens every individual, every company, every industry, and every country in the networked world.

The recent rise in cyber attacks is nothing short of astounding. According to the Government Accountability Office (GAO), the number of cyber attacks reported by federal agencies increased by 782 percent from fiscal year 2006 to fiscal year 2012, from

5,503 to 48,562.[1] Clearly, our government is under attack, and those statistics do not account for the daily intrusions private sector entities and private citizens are facing from a wide range of threat actors.

As a provider of security solutions, we are seeing first-hand the rapid evolution of the threat landscape, with more varied targets, and in many cases, more advanced technologies and tactics than ever before. This ever-increasing risk is threatening to erode trust in digital commerce, communication and collaboration on which we have all come to depend.

I have been involved in the policy debates regarding information security and privacy for a number of years, and I appreciate this Committee's sustained leadership on these issues. Given its potential for loss and disruption, cybersecurity has become a vital economic and national security issue, and we applaud the Committee for its work to reach a bipartisan solution.

Partnership with NIST

EMC and RSA have long enjoyed a close partnership with NIST on a number of issues that are closely linked to information security. As a provider of security solutions, RSA's collaboration with NIST is at the heart of our collective goal of safeguarding the networked world from an advanced and evolving cyber threat. NIST's National Cybersecurity Center of Excellence (NCCoE) lab initiative offers U.S. companies a valuable opportunity to collaborate with NIST and the public sector to address a range of security risks and privacy protection imperatives. With a goal of securing critical infrastructure, the Center inspires technological innovation to find creative solutions to intractable cybersecurity challenges.

Director Gallagher and the NIST team have been exceptional partners with industry. Since the President announced in February his Executive Order "Improving Critical Infrastructure Cybersecurity," we have been working with other stakeholders and NIST to develop a voluntary framework for reducing cyber risks to critical infrastructure that references standards, guidelines, and best practices to promote the protection of critical infrastructure. We have also partnered with NIST in its NCCoE lab initiative to address a range of security risks in support of the National Cybersecurity Excellence Partnership (NCEP). As a public-private partnership, the NCEP offers U.S. companies the opportunity to form a long-term relationship with the NCCoE. Through a collaborative effort, participating companies work together to explore the "art of the possible" and bring our nation to the cutting edge of cybersecurity. The NCCoE's strategy is focused on and driven by the practical cybersecurity needs of American businesses, which is a secure cyber infrastructure that inspires technological innovation and fosters economic growth.

Collaboration among innovators provides real-world cybersecurity capabilities that

[1] GAO, *Cybersecurity: A Better Defined and Implemented Strategy is Needed to Address Persistent Challenges,* GAO 13 462T (Washington, D.C.: March 7, 2013).

address business needs and help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions. It also enables companies to rapidly adopt commercially-available cybersecurity technologies by reducing their total cost of ownership. Most importantly, it empowers innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment.[2]

RSA's "Archer" solution is one example this collaborative effort. Incorporated into the NCCoE's geo-location and security profiling environments, Archer allows adaptation to compliance requirements involving privacy, international safe-harbor restrictions and applications in the cloud.

As a multi-national corporation that operates in over 80 countries around the world, we favor global standards whenever possible. The use of international standards is critical as we seek to meet the broad needs of our user base, but these standards must again be industry-led, voluntary and non-prescriptive. If developed in a transparent, flexible manner, international standards make it possible for global organizations and their customers to continue to make improvements as needs change.

Even so, we recognize that in some cases NIST must develop new standards for federal government non-classified information systems. In these cases, we urge NIST to continue to work in an open, transparent process with stakeholder input. Here are a few examples of our ongoing engagement with NIST around standards development and use:

- RSA's BSAFE product is validated against FIPS 140-2 on a regular basis to ensure our cryptographic implementations. It is our understanding that NIST made a significant contribution from their FIPS 140-2 work to the development of the complementary international standard for cryptographic modules.[3]

- NIST cited EMC's contributions to a NIST Interagency Report on supply chain (NIST IR 7622) as we offered detailed, constructive suggestions over several years to improve the document.[4]

- An RSA employee co-authored a (Draft) NIST Interagency Report: *Trusted Geolocation in the Cloud: Proof of Concept Implementation* (NIST IR 7904 Draft).[5]

- EMC works closely with our Federal customers to help them assess the risks of their new proposed information systems following the Federal Information Security Management Act (FISMA) process. The risk-based FISMA process,

[2] http://csrc.nist.gov/nccoe/The-Center/Mission/Strategy.html
[3] ISO/IEC 19790: Information technology -- Security techniques -- Security requirements for cryptographic modules
[4] http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf
[5] http://csrc.nist.gov/publications/drafts/ir7904/draft_nistir_7904.pdf

which itself deserves further updating, is in turn anchored in NIST standards such as the recently updated NIST 800-53 Rev 4 security control catalog.[6] We appreciate that this new security catalog has a detailed mapping to two key international standards in wide industry use: ISO 27001[7] and The Common Criteria.[8] For the first time, this prominent U.S. Federal standard outlines controls for privacy along with security, a key linkage that we were pleased to see acknowledged in your draft legislation.

EMC/RSA as an Industry Leader

In addition to our longstanding history working with NIST, EMC, and RSA have a proven track record as an industry leader in security. RSA has long recognized that cybersecurity is dynamic, and all stakeholders must continue to evolve our collective ability to counter cyber threats. In 1991, we responded to this new challenge by creating one of the largest security thought-leadership conferences in the world, RSA Conference. It is an annual industry event, which seeks to help drive the global information security agenda. Throughout its history, RSA Conference has consistently attracted the best and brightest in the field, creating opportunities for conference attendees to learn about IT security's most important issues through first-hand interactions with peers, luminaries and both established and emerging companies. As the IT security field continues to grow in importance and influence, RSA Conference, in conjunction with our many industry partners, plays an integral role in keeping security professionals across the globe connected and educated.

EMC/RSA has demonstrated a longstanding commitment to improving our industry's best practices, particularly in the secure development field. In 2007, EMC, along with other industry leaders, created the Software Assurance Forum for Excellence in Code (SAFECode) to define, promote and share best practices and guidance outlining how to build secure software. SAFECode represents the first coherent, user-friendly collection of industry best practices in the development space. Available to the public free of charge, SAFECode's best practice guidance documents outline realistic approaches to secure development.[9] The SAFECode initiative has produced a wealth of accumulated knowledge and shareable training materials that are being leveraged every day by developers to create software that is more secure than anything we have seen before.

RSA knows first hand that no one is immune to the cyber threat. In 2011, RSA detected a targeted cyber attack on our systems. Certain information related to an RSA product had been extracted. We publicly disclosed the breach and immediately began working to develop and publish best practices and remediation steps, so that others could learn from our experience. We proactively reached out to thousands of customers across the public and private sectors to help them mitigate the effects of the breach. Further, we worked

[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[7] ISO/IEC 27001: Information technology–Security techniques–Information security management systems–Requirements
[8] ISO/IEC 15408: Information technology -- Security techniques -- Evaluation criteria for IT security
[9] SAFECode.org/publications

with the appropriate U.S. federal government agencies, including NIST, and several information sharing and analysis centers (ISACs) to ensure broad communication of these best practices and remediation steps, as well as information about the attack.

Our experience was not unique. Individuals, governments, and companies deal with threats every day from nation states, criminals, hacktivists, and rogue actors. We have made great strides in the security space, but there is much work left to be done. As Robert Bigman, former CISO of the Central Intelligence Agency (CIA), has stated, the United States is "exactly where the cyber criminals want us to be. They're very happy with our current situation." [10]

The cyber threats we collectively face are real and immediate, and there are a number of steps that must be taken to enhance our economic and national security.

Implementing the President's Executive Order

Recently, EMC and RSA, along with other private sector companies, have appreciated the opportunity to work closely with NIST on the implementation of the President's Executive Order to Improve Critical Infrastructure Cybersecurity.

This collaboration between industry and NIST is a great example of what the public and private sectors can do together and represents an important step in the right direction. However, legislation is still needed to create a more effective partnership between the public and private sectors.

Key Elements of the Draft Legislation

We applaud the Committee for its work to develop bi-partisan legislation based on an industry-driven, voluntary approach. This legislation complements the President's Executive Order by codifying the important steps the Administration has already taken to protect critical infrastructure and gives government and industry additional tools to bolster our cyber defenses. We are pleased to see that the draft bill requires a voluntary, non-regulatory process, enabling further collaboration between the public and private sectors to leverage non-prescriptive and technology-neutral, global cybersecurity standards for critical infrastructure. We also commend the Committee for including crucial provisions to support cyber research and development; increase awareness of cyber risks; and improve cybersecurity education and workforce training.

As efforts progress, we urge you to consider a few key points:

1) Any successful cybersecurity effort must be industry-driven.

[10] http://www.usnews.com/news/articles/2012/12/04/former-cia-officer-united-states-lags-far-behind-in-cyber-security

With the rapid pace of innovation, owners and operators of critical infrastructure need the flexibility to keep pace with the rapidly-evolving and sometimes equally innovative threat landscape. For this reason, standards and best practices should be non-prescriptive, non-regulatory, and technology-neutral. This draft legislation achieves those objectives by initiating a voluntary, industry-led standards development process that will build on the great work that is already being done in the private sector. This close and continuous coordination between government and industry is vital to the ongoing development of best practices to combat the ever-changing threats we all face.

Collaborative efforts between government and industry have been similarly successful in addressing supply chain security issues. EMC has been an early adopter of industry best practices to strengthen the security of our supply chain and ensure the global integrity of our software and hardware development processes. EMC shared its experience in two SAFECode whitepapers on software integrity.[11] As a leader in the security field, RSA has actively engaged with government and industry partners to develop global supply chain security standards.

The following are a few examples of industry-led efforts to develop and implement security standards:

The Common Criteria: The Common Criteria[12] are a set of international computer security standards developed by governments that include Canada, France, Germany, the Netherlands, the United Kingdom and the United States through active engagement with industry. EMC/RSA has made substantial investments over many years to certify many of our products against the Common Criteria, which are now recognized by 26 countries. U.S. policy should encourage those countries that do not yet recognize The Common Criteria to follow suit as a baseline assessment and avoid separate, custom national evaluations in order to access their markets.

Protection Profiles: Industry has taken the lead to contribute technical content related to supply chain evaluations against standard "Protection Profiles" for different classes of technology. This directly supports a strategy by The Common Criteria Development Board and the National Security Agency (NSA)'s National Information Assurance Partnership (NIAP) unit to reorient product evaluations towards protection profiles, many of which are also developed by industry.

Open Trusted Technology Provider Standard (O-TTPS): In 2009, RSA's Chief Technology Officer worked with the U.S. Department of Defense to launch a joint public-private initiative that led to a published global supply chain standard in April 2013. The resulting standard, The Open Group's O-TTPS Standard for *Mitigating Maliciously Tainted and Counterfeit Products*[13] addresses two of our most important

[11] SAFECode.org/publications
[12] ISO/IEC 15408: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
[13] http://www.opengroup.org/news/press/open-group-releases-global-technology-supply-chain-security-standard

threats. Earlier this month at their international conference, The Open Group's Trusted Technology Forum awarded EMC for its "outstanding contribution" to this multi-year standard development process. The new, global O-TTPS standard will have a measurable accreditation program by year's end, enabling compliance down into the technology supply chain. This non-prescriptive pilot program focuses on measuring the outcomes of practices, while giving each organization the latitude to determine how best to reach the performance goals. This Open Group industry standards effort also has a formal liaison with ISO/IEC's emerging standard on supplier relationships that has itself been developed with significant industry review and comments.[14]

2) Public and private sector collaboration is essential to bolstering cybersecurity.

EMC and RSA strongly support the bill's aim of establishing more effective collaboration between industry and government to address cybersecurity issues. We already participate in two successful initiatives that we believe can serve as a model for future public-private partnerships in the cybersecurity field.

At the national level, the Enduring Security Framework (ESF) is a partnership of senior industry and government executives to identify critical cyber vulnerabilities and mobilize experts to address the risks. At the regional level, the New England Advanced Cyber Security Center is a consortium of industry, government, and universities working together to share cyber threats and explore new areas of research required to improve our defenses.

3) Cybersecurity standards should be voluntary, non-prescriptive, and technology-neutral.

The voluntary nature of the legislation is of paramount importance. While we support the development of standards and best practices, we firmly believe that companies should have the flexibility to determine for themselves how best to secure their networks. In this highly-innovative sector, companies need the flexibility to explore creative approaches and technologies. Government regulations cannot reasonably keep pace with innovation, and companies must be free to design and build secure products in a global environment as they see fit without government intrusion. This ensures ongoing technology innovation in a global marketplace, resulting in increased productivity, job creation, and economic growth.

4) Both government and the private sector must invest in increasing public awareness of the cyber threat.

In today's increasingly interconnected world, every individual has a role to play in enhancing cybersecurity. As we have seen, simple errors such as the use of weak passwords and poor cyber hygiene can have serious consequences. For this reason, we

[14] ISO/IEC 27036: Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts

strongly support the legislation's call for NIST to launch a cybersecurity awareness campaign. Increased awareness is our first line of defense against cyber attacks, and we applaud the Committee for recognizing this. As NIST undertakes this effort, there are a number of existing public-private partnerships upon which we can build.

The National Cyber Security Alliance (NCSA) is a non-profit organization comprised of captains of industry ranging from defense and IT companies to financial institutions and e-commerce providers to telecommunications companies and ISPs. Founded in 2001, the Alliance works with all levels of government to promote cybersecurity awareness. As one its founding members, EMC/RSA has been involved in this partnership since its inception and as the cyber security challenge has grown, so has the Alliance.[15]

In collaboration with its public-sector partners, NCSA established National Cyber Security Month in October, which is designed to elevate and expand cyber security awareness programs. We appreciate the support of the President of the United States and the U.S. Congress in this effort, and we are pleased to see that the initiative has grown year after year. The U.S. Department of Homeland Security (DHS) is a long-time participant and supporter of this public-private partnership as are multiple other federal government agencies and many state and local governments.

NCSA has also partnered with the Anti-Phishing Working Group (APWG) and DHS to launch the Stop-Think-Connect awareness campaign; an effort we will continue supporting actively to help grow its influence as a nationwide and multi-national public awareness initiative.[16]

5) As we move forward, we must think not only of today's threats, but also of the cybersecurity challenges of the future.

Today, thousands of cybersecurity positions remain unfilled in both the public and private sectors, simply because of a lack of qualified candidates. We are pleased to see that the draft legislation includes provisions to increase cybersecurity research and to support the development of the cybersecurity workforce.

Title II of the draft legislation calls for a national cybersecurity research and development plan to be developed by the Office of Science and Technology Policy (OSTP) and the coordination of research and development activities at the National Science Foundation (NSF), NIST, other federal agencies, academia, and the private sector. We believe the authorization of coordinated research will address gaps in knowledge that prevent the development of secure technologies. In addition, the Networking and Information Technology Research and Development (NITRD) program has been successful in supporting research on the science of cybersecurity and will enhance the continuation of innovative approaches to new technology.

[15] www.staysafeonline.org
[16] http://stopthinkconnect.org/

Title III of the draft bill supports efforts to prepare the cybersecurity workforce of tomorrow. Our young people are our greatest asset, but our students are falling behind in the crucial fields of science, technology, engineering and math. Investments in cybersecurity education and workforce training today will develop the talent we need to strengthen our defenses for years to come.

As cyber threats continue to escalate at an alarming rate, we need to invest in building the cyber security workforce with the requisite skills to defend our systems and drive continued innovation. Two areas of investment are particularly important:

Cyber security programs in post-secondary schools: To defend our networks, we will need to graduate more individuals with expertise in computer sciences, risk assessment, data mining, data visualization and analytics, digital forensics, and human behavior. Our colleges and universities must place an emphasis on producing graduates with the technical and cross-functional skills needed to defend against our cyber adversaries. The federal government should support programs at the college and university levels that graduate qualified cyber security professionals. One such example is the Scholarship for Service program, funded by NSF, NSA and DHS, which has produced cybersecurity professionals now working in both the public and private sectors.[17] This and other successful government-funded scholarship programs should be expanded to continue to grow the cyber workforce.

Training, certification and accreditation programs to increase and maintain cyber security proficiency: In 2009, SAFECode members outlined a framework around secure engineering training that concluded that they could not sufficiently rely on colleges and universities to deliver graduates that could join the workforce without substantial, advanced company-led training.[18] Consequently, government and private enterprises should provide increased cybersecurity training opportunities for their IT staff. The SANS Institute and the International Information System Security Certification Consortium (ISC2) and Information Systems Audit and Control Association (ISACA) provide education and certification programs that can be replicated and expanded to further develop the cyber workforce.

In addition, new programs such as the U.S. Cyber Challenge[19] and the National Initiative for Cybersecurity Education (NICE) should serve as models for future education programs. NICE has evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school.[20] The goal of NICE is to establish an operational, sustainable and continually-improving cybersecurity education program to enhance the nation's security. These vitally important initiatives are being put into place to identify, recruit and place the next generation of cyber security professionals.

---

[17] https://www.sfs.opm.gov/
[18] SAFECode.org/publications
[19] For more information, go to the U.S. Cyber Challenge Website at: http://workforce.cisecurity.org/ .
[20] http://csrc.nist.gov/nice/aboutUs.html

This effort will require significant investments today, but if these initiatives are implemented properly, our technological future is bright. We look forward to a time when government and industry work as true partners to combat cyber threats. We also look forward to having a skilled and savvy workforce that comes to the table understanding the threat landscape and best practices ready to apply their expertise in a rich economic environment. These cyber professionals will be the brightest and best-trained that we have ever seen, and they will develop innovative ways to combat the cyber threats more quickly and more creatively than we could ever dream of today.

For all of the reasons noted above, this draft legislation represents an important step in the right direction, but there is more work yet to be done.

Next Steps

In order to effectively address cyber threats there must be an "innovative and cooperative approach between the private sector and the federal government" and we need to collectively utilize expertise within both government and industry. As Commander of U.S. Cyber Command General Keith Alexander has said many times, "securing our nation's network is a team sport."[21] Without strong public-private partnerships and actionable cyber intelligence information sharing between government and industry, we will not be able to make the progress that is so desperately needed. Moving forward, we recommend two key next steps:

1) Government should explore additional opportunities to leverage public-private partnerships.

We greatly appreciate NIST's commitment to working with industry, and we believe similar public-private partnerships should be explored. The public sector should further leverage information available from commercial services to paint a fuller picture of the threat landscape.

For example, the RSA Anti- Fraud Command Center (AFCC) has worked globally with financial institutions, ISPs, law enforcement and other organizations to detect and shut down hundreds of thousands of phishing attacks since 2007.[22]

Similarly, we have worked with industry-led Information Sharing Analysis Centers (ISACs) that are partnering with government entities and law enforcement – such as the Financial Services ISAC – to provide timely and actionable information on cyber threats

[21] http://365.rsaconference.com/community/archive/usa/blog/2011/02/17/video-rsac-us-2011-keynote-the-department-of-defense-active-cyber-defense-and-the-secure-zone--general-keith-b-alexander

[22] For more information on the AFCC, see http://www.emc.com/collateral/solution-overview/10580-afcc-sb.pdf

and attacks.[23] Actionable information gained from these mechanisms and in other processes with industry is often as valuable as information from government sources.

2) It is imperative that Congress addresses other key cybersecurity issues not under this Committee's jurisdiction.

These include advancing the sharing of cyber threat intelligence between government and industry; establishing liability protections for entities that share threat information; and streamlining acquisition of technology. We urge the Congress to examine ways to break down barriers to information sharing and create incentives for the public and private sectors to work together to safely and securely share real-time, actionable information about cyber threats. Linking the adoption of cybersecurity standards to incentives such as liability protection and streamlined acquisition of technology will create a positive business climate while improving our nation's cybersecurity posture.

We also support additional legislative initiatives to update criminal laws and penalties; enact federal data breach law; modernize FISMA; and develop reasonable and effective policy approaches to supply chain protection that will not stifle innovation and competition.

Conclusion

We thank Chairman Rockefeller and Ranking Member Thune for their dedication to advancing this important legislation. I strongly believe the action undertaken by this Committee and the bipartisan leadership of its Members will set a positive course for others in Congress to realize the urgency in addressing this growing threat. As the Senate confronts the policy challenges of cybersecurity, I have every confidence in industry's ability to leverage its existing relationship with NIST to enhance the cybersecurity of our critical infrastructure. Under this Committee's leadership, we sincerely hope that Congress will act quickly to address this urgent threat to our national security.

Again, I thank you for the opportunity to be here today, and EMC and RSA look forward to working with you and your colleagues in Congress as this proposal advances.

[23] For more information on the FS-ISAC's information sharing practices and programs, see "Testimony of William B. Nelson, The Financial Services Information Sharing & Analysis Center" before the U.S. House of Representatives Financial Institutions and Consumer Credit Subcommittee, September 14, 2011.