# U.S. House Homeland Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

## Hearing: “Oversight of the Cybersecurity Act of 2015”

*Testimony of:*

Mordecai Rosen, General Manager, Security Business Unit

CA Technologies

June 15, 2016
10:00 a.m.
311 Cannon House Office Building

Chairman Ratcliffe, Ranking Member Richmond and Members of the Subcommittee:

Thank you for the opportunity to appear before you today. My name is Mordecai Rosen and I serve as Senior Vice President and General Manager of the Security Business Unit at CA Technologies, where I manage global development of CA's cybersecurity products and solutions.

CA is one of the largest enterprise software companies in the world, serving global customers in nearly every major commercial and industrial sector. We are headquartered in New York, and have 11,000 employees across the globe, including many in districts represented on this Committee. CA delivers software that is mission critical to the development, management and security of technologies, which optimize business operations and enable digital transformation in what is being referred to as the "application economy."

I intend to focus my remarks today on two important and related topics. First, I want to highlight some of the emergent and serious cybersecurity threats we see in the application economy. Second, I'll plan to provide CA's specific perspective on the Cybersecurity Act of 2015—how it can be effectively implemented, and how we ultimately feel it can serve as a guidepost for reducing cyber risk in both government and commercial systems.

## Introduction

CA Technologies was a strong supporter of the Cybersecurity Act of 2015 and is encouraged by the implementation thus far. Cyber threat information sharing helps us improve our collective cyber defenses by enabling us to prioritize and deploy resources against current and anticipated attacks. Improving Federal agency cybersecurity helps defend national security and protect citizen data. We want to thank the Committee for your driving this legislation over the finish line last year.

The application economy is transforming the way organizations do business. From entertainment to communications to finance, applications are rewriting the world in which we live, and are enabling organizations and governments to provide services to customers and citizens in new ways that reduce costs, enhance efficiencies, and improve outcomes. Software has become the principal means through which organizations deliver these new services. Examples of these technologies include mobile banking applications, the smart grid to reduce energy costs, and connected vehicle communications to improve safety and efficiency.

Applications have become the critical point of engagement for organizations of all sizes, optimizing experiences and providing a direct and constant connection from organizations to their end users. CA software transforms businesses' ability to thrive in this new reality, delivering the means to deploy, monitor and secure their technology investments.

However, the increasing volume and sophistication of cyber-attacks threatens to undermine this progress through the illegal transfer of intellectual property, the theft of personally identifiable information (PII) and other sensitive data, and the undermining or destruction of critical infrastructure systems.

Cyber-attacks that disable systems, such as the electric grid, water utilities, financial markets or even mass transit systems, could have a potentially catastrophic effect, putting the health and safety of large populations at risk. Federal agency breaches that result in the loss of sensitive data can lead to massive identify theft and fraud, and can put national security at risk.

The Federal government has suffered significant and harmful breaches over the past few years, most notably the Office of Personnel Management (OPM) breach that compromised the data of more than 20 million current and former government employees and contractors. Yet, the government doesn't stand alone as a target for attack. The critical infrastructure community of the United States includes public and private operators of critical systems and assets, and they are all experiencing sophisticated attacks that carry with them the possibility of catastrophic outcomes. The German government recently said in a report that hackers successfully broke into the control systems of a domestic steel plant and caused massive damage to the blast furnace. Here in the United States, the Wall Street Journal recently reported that two years ago hackers infiltrated the control system of a small dam less than 20 miles from New York City.

As the federal government and critical infrastructure owners and operators look to create efficiencies through automation and modernization, they must build security in to their systems on the front end and abandon the model of bolting security on afterwards.

## The Role of Identity Protections in Robust Cybersecurity

In this new threat environment, CA believes that identity and access management technologies are central to protecting systems, networks, devices and data and to enabling secure interactions with customers and citizens. The traditional network perimeter can no longer provide a control mechanism for this access. Identities now constitute the new perimeter and are the single unifying control point across all apps, devices, data and users. As such, identities and application programming interfaces (APIs) serve as the foundations of the application economy because they enable easier deployment of secure apps and help simplify control of access to those apps. They are how you protect access to apps and data, whether that be by human to machine or machine to machine. APIs provide a way to connect computer software components and data. Broadly speaking, APIs make it possible for organizations to open their backend data and functionality for reuse in new application services (think hotel websites using Google or Bing for their maps and directions).

An API achieves this by facilitating interactions between code modules, applications and backend IT systems. The API specifies the way in which these different software components can interact with each other and enables content and data to be shared between components.

Given these new realities, identity is now the attack vector of choice for cyber criminals. In virtually every large network breach in recent memory, compromised identities were the common thread. Protecting identities is foundational to robust security in the application economy.

CA Technologies has made a strategic commitment to addressing identity-centric cybersecurity challenges in today's dynamic threat environment by developing effective identity management solutions through our in-house development process. CA software manages millions of user identities in most major countries around the world. We provide identity-centric security solutions to multiple Federal agencies. Our API Management tools are used within the Federal government and the commercial sector to protect network and application interfaces, to facilitate the secure exchange of information, and to ensure that any data shared protects personal privacy. We believe all of these capabilities will further enable robust cyber threat information sharing. I'll touch more on this below.

## DHS Implementation of Cyber Threat Information Sharing Provisions in the Cybersecurity Act

Congress passed the Cybersecurity Act of 2015 to help businesses and governments better protect themselves against cyber-attacks. The Act promotes cybersecurity information sharing between the private sector and the government, and across the private sector. In addition, the Act includes provisions to strengthen Federal agency cybersecurity through a Federal intrusion and detection system, through capabilities to continuously diagnose and mitigate cybersecurity risks, and through other measures.

CA Technologies supported the passage of the Cybersecurity Act of 2015 because it includes key provisions for which CA has been an active advocate: the bill includes targeted liability protections for program participants; it includes measures to protect the privacy of individuals; and it promotes the further development of automated mechanisms for sharing cyber threat indicators.

CA Technologies believes the Cybersecurity Act will enhance security and provide businesses with the assurances needed to securely share with trusted partners the security threats they are seeing on their own networks, and to receive threat indicators from the wider ecosystem, which will help them optimize defenses. We believe the automated capabilities provided through the DHS Automated Indicator Sharing (AIS) program will make it easier to accept and exchange cyber threat data in real-time. CA Technologies welcomes the opportunity to provide our insight on implementation to date, and to make recommendations to encourage greater participation in the information sharing program and to improve Federal agency cybersecurity.

At the outset, I want to congratulate DHS for the job they've done thus far on implementation. The Cybersecurity Act of 2015 contained very aggressive timelines for DHS to release initial and final guidance to implement the program and to designate the primary system that would be used to exchange threat data between participants. DHS has met those deadlines thus far, and has worked collaboratively with their government and industry partners to provide clarity around the overall requirements for sharing, the privacy protections and processes required to participate, and the process required to take full advantage of the program's benefits. We know how challenging it is to balance competing interests and meet very aggressive deadlines. While the initial guidance documents that DHS issued have raised some questions that we will address below, by and large we feel they provide good

clarity on the technical, legal, and practical considerations entities need to weigh when determining whether to participate in the program.

We are encouraged by DHS's openness to the feedback they have received from industry, civil society, and other actors in the cybersecurity ecosystem, and by DHS's consultative approach. DHS has indicated that they intend to address the majority of these questions in their final guidance documents. We look forward to reviewing those in detail when they are released later today.

We are committed to working with DHS to move implementation forward with active and constructive industry dialogue. Among other organizations, CA Technologies is a member of the Information Technology Information Sharing and Analysis Center and sits on the Executive Committee of the IT Sector Coordinating Council, which helps advise DHS and other Federal agencies on information sharing policies and public private partnerships.

I'd now like to turn to our views on specific provisions of the legislation and the issues we see at play and where some further clarity is needed in implementation.

*Liability Protection*

Organizations should have targeted liability protection for the data they share or receive. This protection will encourage greater participation in the program, leading to better cyber defense. Liability and regulatory concerns are powerful inhibitors of participation in information sharing agreements. Reducing these barriers through targeted protections helps organizations feel more secure in sharing, receiving, and acting upon cyber threat indicators.

The Cybersecurity Act included targeted liability protections, and DHS today is releasing updated guidance providing greater clarification on these protections and the requisite responsibilities of participating companies.

Cybersecurity information sharing is based on trust, and this trust needs to be underpinned by strong certainty for participating companies. While the preliminary guidance released by DHS in February began to provide greater clarity around processes and procedures to gain protections, it also left a great deal of uncertainty. Our understanding is that the updated guidance should provide more clarity and we look forward to exploring this in greater depth. Beyond the release of the updated guidance, we encourage DHS to actively engage with industry and legal groups to help them better understand the information sharing program, the responsibilities of participating organizations, and the liability protections that will be afforded participants.

*Preserving Privacy*

The Cybersecurity Act of 2015 requires organizations to take reasonable steps to remove PII of individuals not related to the threat from any cyber threat information they share through the program. It also requires the government to further scrub this information to ensure that PII is removed. This is vital to protect the privacy of customers and citizens.

The global IT industry is very sensitive to issues of protecting customer privacy and enhancing trust in the solutions we deliver. Therefore, we believe it will be helpful for DHS and the Administration to reassert that the purpose of cyber threat indicator information sharing is to protect networks. Any government exceptions to this purpose must be clearly defined and limited. In addition, CA and others advocated strongly that cybersecurity threat indicator information should be shared through a civilian portal under the legislation. We want to thank the Committee for pushing the National Cybersecurity and Communications Integration Center (NCCIC) at DHS as the portal for information sharing, and we encourage the Administration to continue to promote this portal as the principal mechanism through which to share.

While requirements to remove PII are important to protect privacy, it's also important to help organizations better understand how they can remove PII automatically. DHS's STIX/TAXII effort can help organizations understand what data to share, and how to share it, but companies will need further help to take the guesswork out of this process and automate the removal of PII before sharing. Myriad tools and capabilities exist in the commercial sector to enable automated PII removal. To the extent that organizations are able to effectively utilize these tools, it will lessen their concerns about liability and will heighten user confidence in the program.

We feel that the initial guidance released by DHS made strong commitments towards preserving privacy under this program, though participants will need greater clarity. We look forward to reviewing the updated DHS guidance in this space. Again, active stakeholder outreach and engagement throughout the policy implementation process can help lead to effective outcomes that address both security and privacy needs. DHS can work with sector specific agencies to convene workshops and other engagement activities where organizations can learn best practices on privacy protection as part of information sharing programs. Ideally, these workshops and programs can target different types of industries and can take place in different regions of the country.

DHS can also work to encourage greater participation in the information sharing standards development process, established under the President's Executive Order from February 2015. The Standards Development Organization, led by the University of Texas at San Antonio in partnership with LMI, is currently developing draft standards for Information Sharing and Analysis Organizations (ISAOs). This work should be as open and inclusive as possible, enabling multiple types of organizations, including both nonprofit and for-profit organizations to establish ISAOs.

*Automated Indicator Sharing*

Ultimately, in order to truly move the needle on improving cyber defenses in a significant way, organizations will need to leverage automated, real-time, actionable information exchanges. Cyber-attacks happen rapidly and without upfront notice. Once cyber threat indicators are discovered, this information must also be disseminated rapidly to allow organizations that are the subject of attacks to mitigate their impacts, and to help other organizations target their defenses against the newly discovered threat.

DHS has been working to promote its Automated Information Sharing (AIS) program, which leverages explicit protocols to identify and structure information on cyber threat indicators and to provide for a secure manner of exchanging this information. CA Technologies has been working with DHS and other industry partners to help enable this secure, automated exchange of information across a wide range of different organizations.

CA provides API management software that helps authenticate, authorize, validate, transform, and filter near real-time cyber threat messaging. We believe that any successful information sharing program must depend heavily on the authentication of the individuals and organizations that participate, and on the validity and integrity of the information and the data that is shared under the program.

CA would like to thank the Committee for promoting further development of automated information sharing mechanisms in the final legislation. While DHS's activity on automated sharing programs pre-dates the passage of the Cybersecurity Act, the inclusion of this program in the Act should boost confidence and encourage greater participation.

We recommend that DHS continue to leverage key outreach and partnership programs, such as the Critical Infrastructure Cyber Community or $C^3$ program, and partnerships with Sector Coordinating Councils to build greater awareness around automated information sharing, and to help organizations understand what technical and procedural steps they will need to take to participate. Industry can also play a significant role to build awareness. Sector groups can develop user guidance and promote this with their members.

In addition, we recommend that DHS and the Federal Government continue to promote the STIX/TAXII protocols with global standards development organizations. Ultimately, cybersecurity is a global challenge that doesn't recognize national borders. Global security solutions providers, including CA Technologies, seek to develop products that can scale for the global marketplace. The STIX/TAXII protocols are already commonly used to enable cyber threat information sharing across the Federal government and in the private sector, and we hope that this progress can be leveraged to improve cybersecurity internationally. DHS's recent decision to transition continued development of the STIX standard to OASIS is a positive development that will build international engagement and consensus around the protocol.

CA Technologies is not a current participant in the AIS system. Our internal security team currently utilizes multiple private-sector tools to identify, analyze and prioritize cyber threat indicators. However, CA recognizes the significant benefits that we can derive from participation in information sharing partnership programs in order to defend against cyber-attacks. Therefore, we are actively exploring participation. We welcomed the passage of the Cybersecurity Act of 2015 because of its authorization of activities and its calls for protections for participants. However, while we have strong interest, we are being very deliberate in making a determination on participation because we have outstanding questions associated with the program.

First, will the information we receive through this program be timely, accessible and actionable? Our security analysts must review and act on threat information from myriad sources in real-time.

Information shared through this program must help organizations to prevent, detect or mitigate attacks. Therefore, information needs to be shared in an expedited fashion. Information has to be understandable for participants in the program. And participants need to be able to act on the information, whether that be mitigating against specific ongoing threats, or re-deploying defenses for anticipated attacks. We continue to examine how we would need integrate AIS threat indicators into our overall threat management processes.

Second, how will DHS authenticate users who are receiving or sharing information in the program? Trust is vital to the success of information sharing and users must have confidence that the information they are sharing or receiving will not fall into the hands of adversaries and enable further attacks. Participants will want to know that the information they share will not be leveraged in a way that harms them. They will also want to know that the cyber threat indicator data they are acting on is valid. And, citizens and customers will want to know that participating businesses and the government are doing everything they can to protect their privacy under this program. Therefore, identity and access management will play a crucial role in protecting the underlying information sharing systems.

And third, will there be greater clarification and guidance around liability and privacy protections in the program? This includes clarification around liability protections for the sharing of information with other private sector organizations and for acting or not acting upon the receipt of indicators. It also includes greater clarification on privacy protection requirements.

To reiterate, CA Technologies believes that DHS has done an admirable job of early-stage implementation of the information sharing provisions of the Cybersecurity Act. CA looks forward to reviewing the updated guidance released by DHS today, which we hope will give us the certainty needed to become an active partner in AIS. We also encourage DHS to continue to conduct industry outreach, to help raise industry awareness of the programs, and to further provide clarification on associated liability and privacy protections.

We look forward to working with DHS and the Committee on continued successful implementation of these programs.

**Protecting Federal Information Systems**

A significant number of recent Federal breaches resulted from compromised identities, including those of privileged users. Title II of the Cybersecurity Act recognized this issue and authorized solutions to more fully address the vulnerabilities in government systems.

The EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs, when fully deployed will help government agencies acquire vital security capabilities and tools to better secure government networks and systems.

The EINSTEIN program is designed to detect and block cyber-attacks from compromising Federal agencies, and to use threat information detected in one agency to help other government agencies and the private sector to protect themselves.

The CDM program provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. CA has been an active participant in the CDM implementation.

While CDM Phase 1 focused on asset discovery and management, Phase 2 is titled "Least Privilege and Infrastructure Integrity" and has prioritized both identity management and privileged access management. One of the most important areas of IT risk relates to privileged users. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and on the overall security and privacy of organizational assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that are essential for their role—enabling "least privileged access" for reduced risk. Privileged Access Management solutions provide the visibility, monitoring and control needed for those users and accounts that have the "keys to the kingdom." This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.

Both identity management and privileged access management positively affect operations, putting security activity in the background to make sure security is not seen as a barrier, but instead as an enabler to more secure business operations.

CA would like to thank the Committee for authorizing these programs under the Cybersecurity Act. In particular, we believe that legislative language calling on the head of each agency to assess access controls to sensitive and mission critical data will help protect against the threat of improper use of privileged credentials.

Finally, on behalf of our IT industry partners, we would like to thank the Committee for its help in conference negotiations to ensure that the EINSTEIN program would be designed to promote the security of Federal networks without jeopardizing multitenant cloud environments. In addition, we welcome continued Committee oversight of DHS implementation to improve effectiveness and accountability.

Overall, our primary recommendations in this space are the need for procurement flexibility and improvements in the workforce development process. Currently, Federal agencies recognize the value in deploying CDM solutions. However, they recognize that these deployments could be paid for by DHS in the following appropriations cycle. Agility and speed are very important in this context. Ultimately, a plan and a strategy are worthless without deployment. There is a distinct risk of a moral hazard where agencies will not prioritize cyber funding in the short term, leaving them susceptible to risk of a significant breach in the interim.

Further, DHS partners with GSA on the development of contract vehicles for these programs, and there is a need for more trained contracting personnel to accelerate deployment of these new contract vehicles. We think this should be a key focus for implementation of Title III of the Cybersecurity Act.

In the wake of the OPM breach, we saw government officials working around the clock to improve systems. These are committed individuals, and the sense of urgency following the breach resulted in quick and decisive action to resolve significant challenges that became immediately apparent. However, the long term success in implementing those decisions may be hamstrung by backlogs in the procurement process.

Reacting to specific events to shore up defenses is different than proactive planning. As we look forward, we believe there is opportunity for DHS and its partner agencies to leverage the lessons learned in the cyber sprint and apply them proactively to enhance overall cyber posture across the federal government.

I would mention two things in particular that we think warrant further consideration by this committee. First, we believe it is critical for the federal government to align its own cybersecurity practices with the NIST Cybersecurity Framework that is quickly becoming the standard for private sector information security management efforts. Ensuring that the same approach is being used across the public and private sectors will standardize terminology and ensure that the government is walking the walk when it comes to the approach evangelized in the Cybersecurity framework. We want to commend the Committee for favorably reporting the "Improving Small Business Cybersecurity Act of 2016" last week. As this legislation moves forward in the House and ultimately, we hope, to enactment, we would recommend that an explicit requirement be included directing DHS and the Small Business Development Centers to also leverage the NIST Framework in maturing their cybersecurity programs.

Second, we recommend the Committee maintain focus on the unique cyber threats emanating from the compromise of digital identities. As we note above, the attack vector of choice in today's threat environment remains identity. CA believes that any conversations about cybersecurity threats and solutions must keep a strong focus on shoring up identity protections and enabling organizations to protect themselves from sophisticated identity-based attacks.

**Conclusion**

Cybersecurity represents a significant challenge for industry officials, and for state, national, and global policy makers. At the same time, the application economy is unlocking a multitude of opportunities to provide new services and value to customers and citizens. State, national, and global governments must work with private sector, academic and public stakeholders to develop and implement cybersecurity policies that improve security, enable innovation, and build public trust.

The Cybersecurity Act of 2015 recognizes the crucial role of public-private partnerships in enhancing cybersecurity by authorizing and promoting active cyber threat indicator information sharing across the private and public sectors. It also recognizes the national imperative to protect Federal information networks and systems.

Ultimately, the success of this legislation will depend on stakeholder engagement, agility and inter-agency cooperation and buy-in. CA believes that DHS has made great strides in partnering effectively with the private sector on the implementation of information sharing provisions and we encourage DHS

to continue to improve in this regard. The Title II provisions of this Act, in combination with last year's updates to the Federal Information Security Management Act, further enhance DHS's position to play the lead operational role in protecting Federal information civilian systems.

CA Technologies applauds the efforts the Committee has taken in tackling these key issues. We stand ready to continue partnering with the Committee, DHS, and our industry colleagues in the effective implementation of the Cybersecurity Act of 2015.

Thank you very much for the opportunity to testify today, and I look forward to answering any questions you may have.