Information on Current and Future States of Cybersecurity in the Digital Economy

Input to the Commission on Enhancing National Cybersecurity

Prepared for:

National Institute of Standards and Technology, U.S. Department of Commerce

September 9, 2016

Introduction

CA Technologies (CA) appreciates this opportunity to provide comments to the Commission on Enhancing National Cybersecurity (Commission) on current and future states of cybersecurity in the digital economy.

CA Technologies helps customers succeed in a future where every business is being rewritten by software. From planning to development to management to security, at CA we create software that fuels transformation for companies in the application economy.

The application economy is transforming the way organizations and governments interact with their customers and citizens. Applications are enabling organizations and governments to provide services in new ways that reduce costs, enhance efficiencies, and improve outcomes. Software has become the principal means through which organizations and governments 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 to end users.

The rapid growth of the Internet of Things (IoT) will exponentially expand the breadth and reach of the application economy, as more than 50 billion devices are expected to have internet connectivity by 2020.[1] Application Programming Interfaces (APIs) manage the connections between applications, data and devices. Broadly speaking, APIs make it possible for organizations to open their backend data and functionality for reuse in new application services. Organizations and governments that leverage open APIs can realize significant data-driven value creation.

However, the increasing volume and sophistication of cyber-attacks threatens to undermine this innovation and 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.

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. Critical infrastructure owners and operators are all experiencing sophisticated attacks, many of which include the possibility of catastrophic outcomes and swift marketplace reaction. Multiple financial institutions have experienced distributed denial of service attacks and the theft of customer information. 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 hackers infiltrated the control system of a small dam less than 20 miles from New York City in 2013[2].

[1] [1] http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

Cyber-attacks that disable vital 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.

In this new threat environment, CA Technologies believes that identity and access management and API management technologies are central to protecting systems, networks, devices and data, and enabling secure interactions with customers and citizens.

Identities constitute the new security perimeter and are the single unifying control point across all apps, devices, data and users. Identity and access management software authenticates individuals and services and governs the actions they are permitted to take. API management software authenticates devices and data and is fundamental to securing the IoT. API management software also secures and protects the APIs themselves from threats, and ensures authorized access to the APIs by the approved apps and individuals. As such, identities and APIs serve as the foundations of the application economy because they enable secure development, deployment and management of applications. They are how you protect access to apps and data, whether that be by human to machine or machine to machine.

CA Technologies' RFI response highlights the crucial role of identity and access management and API management technologies in the protection of both the public and private sectors over the short, medium and long-term future. We discuss the importance of building security into the development process. And we make short-term and long-term recommendations for policy makers to protect critical infrastructure, promote cybersecurity information sharing, strengthen Federal Government information security, and enhance national cybersecurity.

Identity and Access Management

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**.

Identity and Access Management (IAM) has always been about establishing, managing, and understanding the relationships between resources and those that need to access and interact with those resources. This serves as the basis for logical security, independent of the physical location of where the resource resides or where the subject that is interacting with these resources resides. IAM determines the policies by which appropriate access is defined, which requires an understanding of both the subject and the resource as well as the context through which they can and should interact. IAM also provides the opportunity for greater understanding of the subject, which enables organizations and governments to provide better quality and more tailored services.

IAM can best be described in terms of core operations:

- Authentication (including multi-factor and risk-based authentication) - a time of access operation that assures that the subject is in fact the real subject and not an impersonator;

- Authorization – a time of access operation that determines, given the current state, whether access should be granted;
- Privileged Access Management – a special form of Authorization with tighter controls and inspection around privileged accounts and operations (such as those of IT Administrators);
- Access Governance – a process for helping business leaders define and refine policies for determining appropriate access;
- Provisioning/Orchestration – a set of operations that happen at times of change facilitating the join/move/leave process and the coordination of change events between disparate connected resources;
- Analytics – providing insight into the changing nature of the relationships between subjects and resources; and
- Identity Repository – a persistent store for maintaining the current state and attribute values of subjects' profiles.

These fundamental elements of IAM – understanding and managing the relationships between subjects and resources –will remain relevant in both the short (12-24 months) and longer term (five to ten years) future. What will change is the scope of the subjects and resources involved and the types of policies that govern these interactions – moving more toward enterprises and governments leveraging IAM to better serve their customers and citizens while protecting their privacy.

Newer IAM Developments

The overall user experience has become more important in the application economy because customers won't tolerate a poor experience for long – business requires a quality experience that will drive customer retention and loyalty. "Frictionless Security" becomes the business imperative for most organizations. However, the value of a quality user experience is not based solely on increased user satisfaction. Security interfaces that are inconvenient and cumbersome often force users into work-arounds, many of which end up violating security policy, even unwittingly. **In short, users need a convenient, intuitive experience that will enable them to easily conform to established security policy, rather than forcing them into violating them in order to get their jobs done**. Below are some components of what CA believes comprise a frictionless authentication experience.

Continuous authentication methods leverage behavioral and biometrics monitoring throughout a user session to determine if the session has been compromised. This provides a consistent level of assurance throughout the session rather than only checking at the beginning of the session.

Risk-based authentication has the benefit of not only facilitating the authentication of the identity but, because of the context that is provided under risk-based models, can also facilitate the recognition of the identity. This means that when there is a better understanding of the context around the identity, such as through geo-location data or purchasing behavior, the system may recognize the identity, determine that traditional authentication is unnecessary, and allow access. Conversely, if the system detects anomalies, such as logging in from a foreign country in the middle of the night after having a

few failed passwords, then this is a very high-risk operation and access will be denied absent additional authentication steps.

Privileged Access Management solutions provide the visibility, monitoring and control needed for those users and accounts that have the "keys to the kingdom." 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 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. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.

In addition, as requirements for cloud-based applications and cloud services increase, organizations will need to deal with tighter access management and security around privileged accounts. PAM capabilities protecting IaaS, PaaS, and SaaS services in addition to resources on-premises will become much more commonplace in cloud environments.

DevSecOps

IAM will also become an inherent part of securing the development of new applications under what CA has been referring to as "DevSecOps," an abbreviation of Development, Security, Operations. If proper security measures aren't applied early in the development of new services and applications, especially with the growth of the IoT, the opportunities for attack will only increase, costing us all much more in the long run. **As the government and commercial sectors look to create efficiencies through automation and modernization, they must build security into their systems on the front end and abandon the model of bolting security on afterwards**. If we as an industry start to build security in from the start, then interconnected capabilities will open up far fewer opportunities for attackers to abuse.

CA Technologies utilizes a secure software development lifecycle process to minimize vulnerabilities in its software. CA is a board member of the Software Assurance Forum for Excellence in Code (SAFECode), which is dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. CA is also a member of the Open Web Application Security Project (OWASP), which enables organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

Ultimately, the application economy is dependent on trust in the technology products and services, which enable its growth. Building security into the development of these products and services provides a strong foundation for this trust.

APIs and Securing the Digital Economy

Enterprise IT in the 21st Century has been characterized by a move towards opening up previously siloed databases and applications, so that data and functionality can be accessed across organizational boundaries or reused in new systems.

Building APIs is critical to all aspects of the digital economy including open government, as well as integration and interoperability in various industries like public sector, healthcare and finance. Each of these initiatives leverage APIs to connect enterprise data to mobile apps, cloud platforms, partners and IoT devices.

While building APIs can provide a wealth of business and service opportunities for organizations and governments, APIs also have the potential to open the enterprise to serious new security threats, by exposing sensitive backend systems and data to the outside world. APIs are vulnerable to many of the security threats that have plagued the Web plus a range of new API-specific threats. **Therefore, it is vital to deploy strong, API-specific security at the edge of an organization's API architecture**.

This need for strong security can conflict with a basic goal of API design—a well-designed API makes it easy for developers to create apps that provide seamless access to enterprise resources. Strong security is likely to impact this ease of access. **Deploying security in a centralized API architecture (rather than in the API implementation) will help mitigate this impact, as will enabling the use of flexible access management technologies like OAuth and OpenID Connect**.

The key component of an API management and security solution is the API Gateway which acts as the central enforcement point for security and other policies for APIs.

In many commercial and public sector deployments, IAM is extended to the "modern" computing paradigm (mobile and cloud) via APIs. Digital transformation is driving modern computing adoption, and security plays a crucial role. API management technologies integrate standards-based security for Mobile and IoT using SCIM, OAuth, OpenID Connect and PKI to orchestrate a secure context between clients and server side. Automated client registration and secure channel creation requires no specific implementation of security protocols by the app developer, but results in an end-to-end protocol and data-level security posture. API management solutions can be configured to provide end-to-end security between the client and secure data (including dynamic secure data storage on mobile clients), as well as protecting against many web-based threats and OWASP vulnerabilities.

APIs and the Internet of Things

Security plays a critical role to the development and deployment of IoT technologies, tied closely to identity, privacy and/or personal safety. Healthcare sensor/device failure can have fatal consequences for the involved party. Personally identifiable health and financial information can be extracted from wearables and sold. Rapidly approaching autonomy provides a security challenge to the automotive industry, but even traditional vehicles can have potentially dangerous results from breaches. Industrial Internet applications (smart grid, aerospace, robotics) can affect large populations if compromised. Transportation systems also have potentially high consequences for failure.

The exponential growth of data and events generated and processed by IoT systems will be hard to govern and maintain. From a security perspective, the data must be secured from end point, through all integration nodes in transit, to backend systems (and potentially back out).

Endpoint security is also a massive challenge that depends greatly on the Things in question, which range from massively expensive machines to small smart bulbs and embedded systems.

APIs are in the center of any IoT solution. APIs provide a way to connect computer software components and data. 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.

APIs are like windows into an application—a direct conduit that leads straight into the core functionality and data residing in the heart of the app. **APIs will be critical to the interfaces between sensors, devices and applications in the emerging IoT ecosystem. Leveraging APIs and securing them will be vital in enhancing trust in the IoT.**

APIs represent a great opportunity for the enterprise to integrate applications quickly and easily. But APIs can be a double-edged sword: promising agility, while at the same time increasing risk. Organizations will need to address API security as an architectural challenge long before any development takes place; if they can do so, the IoT will reap the rewards of this technological breakthrough safely and securely.

CA's 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. To extend this to the IoT, CA adds a layer of security on top of MQTT (the communications protocol for the IoT) to enable end-to-end security in these implementations.

The IoT will enable organizations to operate systems and supply chains more efficiently by generating actionable insights combined with automation and integration of business processes. IoT solutions also can enable the automation of dangerous or tedious activities (such as transport, mining, warehouse management, and property surveillance.) This extension of traditional IT functions also introduces new challenges: it expands the cybersecurity attack surface, it exposes new privacy challenges, and it greatly increases the load on IT infrastructure and service support. API Management technologies will continue to play a critical role in securing the data, devices and transactions under the IoT.

There is significant risk that global governments and US Federal regulatory agencies will develop multiple, distinct and overlapping compliance regimes around the IoT. This policy fragmentation can lead to organizations dedicating scarce resources towards compliance exercises and away from innovation and development.

The Department of Commerce can help lead inter-agency IoT policy alignment initiatives, and can also work with global partners to promote policy alignment, where possible. The development of a National IoT Strategy, which incorporates both Federal agencies and independent regulatory agencies, can help drive this alignment and coordination.

CA Technologies also believes that policy makers should embrace international, market-driven standards rather than country-specific technology mandates for the IoT. International standards are

vital to vendors' ability to deliver secure, resilient and cost effective solutions that meet truly global performance requirements. Local standards fracture markets, increase cost and may weaken security.

Leveraging the Cybersecurity Framework to Protect Critical Infrastructure

The Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") provides owners and operators of critical infrastructure with a risk management-based, flexible approach to addressing cybersecurity threats. CA Technologies values the Framework because it provides a common language for us to discuss cybersecurity risks and priorities across our entire enterprise, and with customers and suppliers.

CA Technologies is utilizing the Framework to assess, prioritize, and improve our own cybersecurity program. We contracted with a major third party consulting firm to assess our controls against the categories and subcategories of the Framework. Our leadership team felt it was important to conduct an independent assessment, as this would help provide an objective picture of our overall cybersecurity posture.

Our use of the Framework reaffirmed and validated a number of the controls and processes that we had in place, and it also aligned with areas where we were investing to improve technology processes. Our plan is to use the Framework to continuously evaluate and measure how the enhancements we implement are improving our overall posture in a continuously changing cyber threat landscape.

CA continues to support Federal Government efforts to promote critical infrastructure cybersecurity guidance alignment with the Framework.

CA Technologies also believes that one of the best steps the U.S. Government can take to increase the sharing of best practices is to promote alignment of federal information security practices with the Framework Core. A majority of information security vendors service both the public and private sectors. Aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework, will enable more vendors to compete in the public and private sector information security marketplace, driving further innovation and improving security capabilities.

In addition, **NIST should continue to support public and private sector efforts to align state cybersecurity requirements with the Framework**, so as to avoid a patchwork of cybersecurity compliance requirements across multiple states. We are encouraged by the work of the National Governors Association to help states utilize the Framework.[3]

Further, **NIST and its Federal agency partners should expand their promotion of these approaches with their global government partners**. International acceptance of industry-led, global cybersecurity standards allows for even greater competition and innovation in the marketplace. International

[3] http://ci.nga.org/cms/home/ci1617/index.html

adoption of the Framework approach to critical infrastructure cybersecurity establishes a common lexicon across a range of stakeholders, yet allows for technology flexibility to address unique threats and priorities. While CA recognizes there may be a need for distinct national policies at the margins, these should build off of an aligned approach exemplified by the Framework, and should not create alternative and potentially contradictory approaches.

Effective Implementation of Automated Cyber Indicator Sharing

Cyber threat information sharing helps organizations improve collective cyber defenses by enabling them to prioritize and deploy resources against current and anticipated attacks. Ultimately, though, **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.

The U.S. Department of Homeland Security (DHS) has been working to promote its Automated Information Sharing (AIS) program, which was authorized in legislation signed by the President last year, and 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 is working with DHS and other industry partners to help enable this secure, automated exchange of information across a wide range of different organizations.

CA's API management software 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**.

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.

Protecting Federal Information Systems

A significant number of recent Federal breaches resulted from compromised identities, including those of privileged users.

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.

Both identity and access 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.

Our primary recommendations in this space are the need for deployment, 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 inconsequential without deployment. There is a distinct risk of a moral hazard where agencies will fail to prioritize cyber funding in the short term, leaving them susceptible to risk of a significant breach in the interim.

Further, DHS partners with the General Services Administration (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.

Most departments and agencies have already deployed a variety of authentication and authorization solutions as part of both their internal and citizen facing applications. **CA Technologies recommends that any government-wide solution add value and not create disruption and unintended expense by replacing the existing work that has been done**. The applications that have been built and secured with these existing FICAM solutions are servicing millions of people today. Agencies should be encouraged and funded to do what is best for meeting their business requirements: leveraging APIs to further extend their baseline solutions and adding additional safeguards like privileged account and shared account management. Any new policies coming out of this program and our new administration should consider and augment the investments and the services already being provided, not direct them to new platforms and distract them from the ancillary opportunities.

In the wake of the OPM breach, government officials worked tirelessly 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.

Conclusion

The world of cybersecurity is undergoing significant changes and many companies are undergoing a "digital transformation" in which they need to create new business channels, engage with their customers and citizens in new ways, and increase overall efficiencies – all while protecting corporate, customer and citizen data from breach and misuse. Identity and access management and API management technologies will be vital to securing the applications, data sets and devices of the application economy. Identity is the attack vector of choice for cyber criminals in the application economy. It is therefore crucial to properly authenticate and authorize individuals, devices and data.

The public and private sectors should continue to focus on deployment of robust IAM and API management technologies to secure applications and devices.

From a policy perspective, the Federal Government and industry should continue to focus efforts on promoting the use of the Framework for Improving Critical Infrastructure Cybersecurity, both in the private and public sectors, and with global government partners. In addition, the government should support continued implementation and promotion of the Automated Indicator Sharing program to support broad cyber situational awareness. Further, the government should accelerate deployment of technologies to support the EINSTEIN and CDM programs. And the government and industry should continue to promote the use of international, market-driven standards for securing both the Internet of Things and the broader IT ecosystem.

CA Technologies appreciates the opportunity to provide input to the Commission for Enhancing National Cybersecurity. We look forward to partnering with the Commission, its members and its staff as you develop recommendations for enhancing public and private sector cybersecurity for the near term future and over the next decade.