One CA Plaza
Islandia, NY 11749

T +1 631 342 6000
F +1 631 342 6800
ca.com

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

To Whom It May Concern:

CA Technologies (CA) appreciates this opportunity to provide comments to the National Institute of Standards and Technology (NIST) on the development of a voluntary framework to enhance the resilience of critical infrastructure to cyber threats.

CA is the world's largest independent IT management software company. The company provides IT management and security solutions to the majority of the global Forbes 2000. By the very nature of what we do, we appreciate the complexity of cyber threats and the need for a sound framework to enhance the resilience of critical infrastructure to cyber threats.

Strong collaboration through partnership between government and the private sector is the best possible way to achieve effective security outcomes. In the areas where there is need for additional standards, government and the private sector must work collaboratively to create those standards and ensure that efforts to do so do not result in duplicative and unnecessary controls, add excessive cost, create unjustifiable market access barriers, or impede technological innovation.

An effective framework to improve critical infrastructure cybersecurity must be flexible, repeatable, performance-based, and cost-effective. These are fundamental elements to any effective approach to enhancing security in the cyber domain.

Our response to the RFI is provided in the enclosed attachment. As a company that is a committed partner to the government, we look forward to working with NIST and other agencies on the development and implementation of a successful cybersecurity framework. If you have any questions or comments, please contact Denise Zheng (denise.zheng@ca.com).

Sincerely,

Brendan M. Peter
Vice President
Global Government Relations

Risk Management

Enterprise Risk Management

CA Technologies (CA) has an enterprise risk management program to aggregate and report on management's response to significant risks affecting the business strategy, operations, financial reporting, and legal and regulatory affairs. Reporting is provided to company executives and the Board of Directors.

Cybersecurity Risk Management

Given the nature of the company's business, cybersecurity risk figures prominently within CA's overall enterprise risk management program. We have comprehensive cybersecurity policies and procedures covering a range of areas including acceptable use and access to IT systems and assets, data classification, malware, and incident response. All of our policies and procedures are reviewed regularly as a control to maintain the company's ISO 27001 certification. These policies and procedures drive the underlying security controls adopted across the company to provide defense in depth protection of our intellectual property and critical assets and to maintain business continuity.

All corporate information security policies and procedures are reviewed by senior management before publication and at time of modification. The policies are updated at a minimum annually and throughout the year as the threat landscape changes or if controls are modified. When new policies are created or if there are significant modifications, the relevant stakeholders are made aware through automated communications from our quality management system. Cybersecurity policies and procedures are also central to new hire and regular and continuous cybersecurity awareness training for employees.

Security Organization and Structure

CA Technologies has a centralized security model where the design, build, and operations of security controls source from one governing security body under our Chief Information Security Officer (CISO). To remain synchronized with senior leadership, we have a cybersecurity council that manages cybersecurity risks to the company. The objective of the council is to build, improve, and implement the company's cybersecurity roadmap and to assess progress toward objectives. The council meets quarterly and is comprised of senior executives across all relevant business units within the company. Each member of the council is responsible for implementing the policies and controls within their line of business and is held accountable for cybersecurity matters related to their department.

Risk Ranking and Prioritization

We have adopted a model wherein we risk rank our most critical assets and applications based on the information contained within. The ranking is done based on our data classification policy which defines what types of data are considered public, company record, confidential or highly confidential. Identification of our most critical assets enables us to take a risk-based approach when applying security controls. As weaknesses or vulnerabilities are identified, we prioritize remediation activities based on the asset risk level and criticality of the exposure. We use third parties to assess our risk periodically and provide us with a gap analysis and risk mitigation steps.

Understanding, Measuring, and Managing Risk

Managing cybersecurity risk is a top priority for the company. We take a measured approach to continuously improve our countermeasures and manage and reduce our overall risks over time. We leverage internally defined security control frameworks as well as industry recognized frameworks (ISO 27001 and COBIT) as part of our security governance model. Many of our policies and procedures include NIST, SANS, ISO, IEEE, and other industry best practices and recommendations. We have our own risk ranking methodology to assess the severity of cybersecurity risks and prioritize our action plans accordingly. We report security project and operational health metrics to executive management monthly to facilitate future investment considerations. Changes to and adoption of new technology follow a strong and mature selection process.

Business Continuity and Disaster Recovery

We have employee organizational and corporate level goals that are assigned to improve, measure, and ensure that risk related to business continuity is minimized. Various metrics are used by IT leadership to understand how the company is operating against its objectives and enables intelligent and timely decision making for future improvements.

Industry Cybersecurity Best Practices

CA provides IT management and security solutions to a majority of the global Forbes 2000 companies. While we work with a range of critical infrastructure sectors, our largest customer base is within the financial services sector, where we provide industry-leading identity management, authorization, access control, and data management and loss prevention solutions. Rather than providing an inventory of existing standards, our response is focused on identity and access management, which is one of the most critical and effective security practices and is applicable across all critical infrastructure sectors. We believe that robust identity access management must be a part of any framework to mitigate cyber risks to critical infrastructure.

Identity is the New Perimeter

Traditional cybersecurity command and control methods are no longer flexible enough to handle the demand for increasingly complex IT ecosystems designed to provide services anytime, anywhere, and to anyone with appropriate business need and access rights. As the popularity of cloud, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) offerings has grown in recent years, and with the explosion of mobility and new smart endpoints, more and more applications and users have moved outside of the firewall. Traditional control boundaries are eroding and in some cases are in jeopardy of being obsolete. We see this happening at a tremendous rate within the financial services sector, but the trend is also prevalent within other critical infrastructure sectors.

The traditional notion of network perimeter security is far less significant today. In the past, the network perimeter provided a hard outer shell around all of its data and applications. This approach kept everything contained, and security and IT teams could easily manage employee identities internally. As the number of remote employees has grown, VPNs became part of the perimeter. Today, the notion of the firewall and having an “inside the network” and an “outside the network” is less relevant, and therefore, organizations have to change how they manage security and user identities.

In this new landscape, identity is the new security perimeter; identities of individuals as well as the identities of things. The need to identify who or what is accessing a resource, what level of assurance is required, what constraints are placed on the usage and dissemination of data, and how the activity should be traced and potentially certified are all items that have identity as a common thread.

The following frameworks enable effective and adaptive security in this new environment.

Identity Management and Governance (IMAG)

All internal and external IT systems have multiple users with a range of roles and business needs. Identity management and the corresponding identity governance involve:

- On-boarding and off-boarding of users;
- Ensuring that different systems have consistent views of the same users (identity-linking);
- Managing user privileges and roles; and
- Ensuring that systems meet compliance requirements related to user creation, deletion, and management.

IMAG provides the foundation for trusted identities. It can either be centralized or distributed, and can encompass federated identity communities. The attributes/claims of identities can be of various strengths, ranging from information that is either provided by the individual to information that is provided by a higher level vetting organization that is able to deliver high quality attributes that have been verified through various third party systems or databases. As such, identities can also be of varying quality and strength. More critical and sensitive transactions need a higher level of assurance that the identity is really under control of the entity claiming ownership. This is where strong authentication provides benefit.

Strong Authentication

IT systems expose assets with differing levels of importance and sensitivity. Some have low sensitivity, such as websites that expose publicly available information, and often allow access to anonymous or low assurance users. Other systems are highly sensitive, and may impact the operations and resiliency of critical infrastructure. These systems require users to be identified prior to access, using progressively stronger authentication technologies as the value and sensitivity of the affected assets and data increases. A common approach is to use a variety of authentication technologies – both single and multifactor – where the specific technology used to protect a given system is selected based on its strength, balanced by usability and convenience. Multifactor authentication is becoming increasingly important as attacks on single factor (password) authentication increase. Another complementary approach is to augment strong authentication with risk analysis. In this approach the characteristics of a given authentication attempt are collected and used to generate a risk score that indicates the likelihood that the authentication is genuine, independent of whether the user authenticated correctly.

Access Management

Even single IT systems or small groups of systems may expose a wide range of assets with varying degrees of sensitivity. For example, a single web server might expose thousands of URLs that connect to many different infrastructure assets. There is a need for manageable ways to protect access to these assets such that only the appropriate users or roles can perform only approved operations on them. A typical approach is to use an access management system that centralizes the administration and enforcement of access policies applied to many endpoint systems. Identity is an element that defines access. The identity, its strength, and the context in which resources are being accessed are necessary to adequately control and secure sensitive information. As users expand their usage of cloud and mobile services, the only item that is consistent across these scenarios is the identity. There are a few categories of identities that need to be considered. Employees, partners, customers are all types of identities. Administrators of critical IT infrastructure are also another type of identity that can cause great harm. These accounts normally have elevated privileges that allow them to circumvent traditional command and control practices. To mitigate this particular category of elevated privileges and shared accounts, privileged user management has evolved as a new practice within IMAG.

Privileged User Management

Many IT systems, particularly legacy systems, do not have complex or fine-grained privilege management systems, where individual users are only given access to certain actions affecting specific assets. Rather, many have highly-privileged ("administrator" or "root") user accounts that must be used to perform a range of IT management tasks. Privileged account passwords are often shared between many people and may be lost or exposed. It is consequently hard to know which user performed a given management task, making audit and compliance difficult. This lack of accountability has proven to be a vector of attack for malicious entities. Company assets and operations are at great risk if a privileged user account is compromised because it is much easier to cause damage within administrative boundaries. An approach to solving this problem is to use a privileged user management system. Such a system provides additional controls on privileged accounts. Rather than the account passwords being widely known, single-user passwords are provided only as needed, under strict controls, and to specific users. This protects against loss of passwords, prevents unauthorized access, and provides an audit trail of which user performed which privileged operations. Privileged user management is even more important in virtualized environments, where the number of operating environments ("guest virtual machines") grows exponentially, and privileged users exist in both host and virtual systems. As organizations assemble applications and services from a combination of on-premise capabilities and evolving cloud environments, the control of these administrative accounts becomes more critical.

Data Protection

As an entity's network and applications transition into a hybrid environment, the next area of concern is protection of intellectual property or other sensitive information. Content or data is like water. It finds the most efficient way out of a container. Attempts to keep it contained have proven flawed in the new bring your own device (BYOD) and cloud environment. To deal with this concern, data protection and content-aware solutions need to be deployed. Data protection must also maintain the relationship of the policy and identity as it transitions through the various containers such as email, disk, SharePoint, etc.

Data is a key IT asset that is particularly difficult to protect, because it must be available to users in order for it to be valuable. Yet by making data available there is a risk of it being lost or exposed to attackers, either through malicious attack or simple innocent mistake. An approach to protecting against these situations is to implement systems that classify data, monitor its access, and automatically implement controls according to policy. For example, an attempt to copy a sensitive file to a memory stick might be blocked. An email with sensitive data might be intercepted before being sent and encrypted. Moving from manual user intervention to automated policy enforcement and assuring that the content policy is part of the payload are critical components of protecting sensitive information from cyber threats.

Cloud Security & Integrated Systems

The approaches discussed above apply to different threat areas, and they also complement each other. Integrating these approaches into a broader security solution provides natural synergies. For example, the management of users; creation of their authentication credentials; assignment of roles; and management of access policies all naturally go together and can be presented to an IT manager as an integrated solution. This makes the overall IT management process both more scalable, as well as more secure. Management of the integrated solution itself can be made easier by providing it as a cloud service. This provides centralized, integrated security, with the ability to standardize on important aspects like SLAs and audit requirements.

Threat Detection

In addition to the security controls identified above, threat detection (e.g., antivirus, intrusion detection, malware detection) is used to try to identify any malware or malicious users who have bypassed existing security controls or exploited weaknesses in the attacked system. These systems are a last line of defense in a complete security implementation. A related threat detection approach is that of penetration testing.

Audit

Security Information and Event Management (SIEM) software allows for auditing capabilities of log files in order to detect malicious usage that has not been detected through either data protection or threat detection capabilities. We are seeing a movement in this area to combine traditional SIEM approaches (using specific log files) with Big Data in order to provide more accurate detection and a better view into an organization's processes.

Cross-Sector and Cross-Organization Applicability

The approaches listed above are generic best practices for cybersecurity that apply to all sectors. The intersection of identity, applications, and data needs to evolve for an ecosystem that spans both public and private sectors but allows for mixing and matching of approaches to maximize enterprise business opportunities, while minimizing cybersecurity exposures.

Identity management, authentication, and access management are used to some extent in all organizations, from small to large, although some organizations will have better documented, more controlled, and/or better automated processes than others. Privileged user management is typically used in larger organizations with stricter controls (e.g., financial institutions) and recently within hosted IaaS and PaaS services. Data protection is typically used in larger organizations and organizations that are subject to regulatory control (e.g., healthcare). It is also used, although inconsistently, by medium sized businesses. Cloud security/integrated systems are in the initial stages of adoption by industry. Some threat detection systems are widely adopted across the industry (e.g., antivirus). While log examination is common in most organizations, formal audit control software tends to be adopted only in larger organizations.

Sector-Specific Needs

The approaches identified above represent generic security best practices and are not sector-specific. Regardless of the sector, all critical infrastructure entities should implement each of the identified security controls identified above. However, sector-specific needs will dictate details within each of the controls (e.g., such as proper configuration of access control, appropriate risk models, etc.). We believe that the cybersecurity framework should also build upon efforts that are already underway to harmonize and accelerate adoption of risk-based identity controls and federation, such as the National Strategy for Trusted Identities in Cyberspace. There is significant and meaningful work being done through pilots and the Identity Ecosystem Steering Group to define standardized identity controls, interoperability scenarios, and mechanisms to elevate trust based on the risk of the transaction and the identity attributes required to enforce authorization.

Potential Modifications

Identity management, authentication, and access management are reasonably mature technologies, although they are still evolving and improving. For example, research is currently being done on continuous authentication (e.g., based on biometrics such as typing patterns), and better forms of mobile and biometric authentication. Improved models for risk analysis of allowing access to information and devices are being developed. In terms of access control, large organizations tend to have difficulties in controlling access to information due to the proliferation of people (identities), roles, and information. In these organizations, the principle of least privilege (users having access only to that data they need and no more) is typically not followed. Better access control models (e.g., based on social networking analysis to inform risk models) are being investigated. Data protection models will improve as advancements are made to automatically classify information and determine who has legitimate access and for what purposes. Threat detection also needs improvement. Current threat detection approaches lead to large numbers of false negatives, and they are unable to address zero-day attacks. While there is ongoing research aimed at detecting zero day attacks (e.g., anomaly detection, behavioral analysis), these approaches suffer from large numbers of false positives, which in turn leads to significant resources spent on manual analysis and human response. In the area of audit, further investigation is needed on how to better incorporate multiple data sources to provide analysts with a complete picture of their organization, coupled with intelligence to help the analyst detect any malicious activity.

In summary, more research is required to continually improve existing security controls.