Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

“Developing a Framework to Improve Critical Infrastructure Cybersecurity”

From The PCI Security Standards Council, April 8, 2013

Introduction

The Payment Card Industry (PCI) Security Standards Council, also referred to here as the PCI Council, appreciates the opportunity to provide feedback on this important initiative assigned to NIST. We support NIST’s assertion that the framework to improve critical infrastructure cybersecurity should provide flexible, scalable and technology-independent standards and guidelines, and that it incorporate a consultative and risk based approach. The PCI Council is pleased to support NIST efforts in partnering with the private sector on this framework, by presenting information relevant to our experience in the payment card data protection space.

Retail payment systems are not critical infrastructure. This can be demonstrated by volume and size of transactions. Retail payment systems can be distinguished from large-value payment systems, which have been historically owned and operated by central banks as part of their core mission of maintaining the flow of money through the economy. The volume of funds transmitted through large-value payment systems such as the Clearing House Interbank Payments System (“CHIPS”), Fedwire and the European Central Bank’s real-time gross settlement system are orders of magnitude larger than the volume of funds transmitted through retail payment systems. Furthermore, the individual payments processed by these large-value payment systems are orders of magnitude larger than the payments processed by retail payment systems, and often involve the settlement of large transactions in which the transaction counterparties are financial institutions rather than consumers and merchants. Also, there is substantial substitutability among retail payments – there are several retail payment systems, the ACH system, private label payment arrangements, checks, and cash – so that no one retail payment system is critical. For this reason the information given in this RFI response should be considered as best practice from an industry standards body that is focused on protection of very specific data assets as opposed to critical infrastructures.

As background, the PCI Security Standards Council was formed in 2006 by the five major payment card brands, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc. The Council guides the development of open industry standards and relevant best practices to protect payment card information, (such as the PAN or Primary Account Number, expiry date, magnetic stripe or chip data, and sensitive authentication data) across the transaction process and around the globe.

The PCI Council is but one example of the hundreds of private sector based entities that have been formed to develop voluntary consensus standards across virtually all branches of industry to serve new needs as they arise, thereby helping to ensure that businesses can conduct their operations responsibly at home, and competitively around the globe. As an industry initiative, the Council believes that other private sector industries with sensitive assets or critical infrastructure may be able to take parts of our successful model and adapt them for their own use. The Council encourages NIST to study it's, and other best of breed approaches to ensure that proven methodologies already deployed in the market are not superseded or adversely impacted by this NIST-led initiative. It is important not to reinvent the wheel where progress and expertise currently exist in the market.

The Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The latter is significant since the Council believes that providing a full suite of tools to support implementation is the most effective way to ensure the protection of payment card data. This response will provide detail on our holistic approach.

More than 670 companies worldwide participate in the Council's standards setting work. These Participating Organization members represent many different industries and backgrounds – from restaurants, banks, airlines, technology vendors, to universities and payment processors. Participants come from six continents, reflecting the global nature of the payment process and how multinational corporations and worldwide commerce depend on it; Participants have a range of titles and perspectives including IT specialist, risk manager, finance officer, security chief and head of business lines. As broad as this group is, they are singularly united in their desire to protect their customers and business partners' payment card data as well as their brand names and businesses from any potential harm. The Council believes its work is an example of a private sector industry uniting effectively around a common goal.

Council staff works closely with members of our various committees and our wider membership to develop PCI Standards. The PCI Standards are examples of a strong industry framework for protecting payment data. Although payment card data and payment systems do not qualify as sensitive assets or "critical infrastructure", nonetheless our approach to industry collaboration and standard setting could be applied to other sectors that would qualify under a critical infrastructure definition.

To support successful implementation of PCI Standards, the Council also maintains programs that certify and validate certain hardware and software products to support payment security. Additionally, the Council runs a program that develops and maintains a pool of global assessment personnel to help partner with organizations that deploy PCI Standards to assess their performance in using PCI Standards. The Council also focuses on creating education and training opportunities to build expertise in protecting payment card data in different environments and from the various viewpoints of stakeholders in the payment chain. Finally, we devote substantial resources to creating public campaigns to raise awareness of these resources and the issue of protecting payment card data. In short, the PCI Council's approach to securing sensitive payment card data across the payment transaction chain has been holistic. The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary – standards, products, assessors, educational resources and training - for stakeholders to successfully secure payment card data.

The Council lends its perspective here to NIST through the prism of an organization explicitly focused on protecting payment card data. Not all questions are pertinent to our organization's experience or focus, and those that are not have been omitted in our response below.

Current Risk Management Practices

What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The greatest challenge for improving cybersecurity practices across all infrastructures is trying to stay current, through frameworks and standards, for a diverse group of technology, assets and processes. Part of staying current is the ability to not only monitor the threat environment, but also to design a framework that remains useful in spite of a changing threat landscape. Once appropriate best practices or standards are developed and implemented, maintenance and measurement of a secure posture, including educating and motivating those responsible for it, becomes the next challenge. It only requires one failure in diligence to lead to a compromise of controls.

What do organizations see as the greatest challenges in developing a cross-sector standards-based framework for critical infrastructure?

In the Council's experience in the payments space, developing a framework that meets the needs of a diverse set of stakeholders with different operating realities, risk profiles and business focus has been an evolutionary process. Through our standards lifecycle, community input opportunities and monitoring of the threat landscape, the Council has developed a set of standards that provide a balance between prescription and flexibility. They are a starting point for an organization to secure payment data. In a business environment any change to the ability to process card payments, while important, will only inconvenience the consumer to the degree they will have to use alternative payment methods. For a company operating in the critical infrastructure space, the impact of a cybersecurity incident will have deeper implications. Companies use security standards as both a high level "philosophy" on security and as a detailed "playbook" of controls. Finding a balance between prescription and flexibility in a framework that will apply across sectors is a key challenge. Establishing the right starting point that applies across environments is critical.

Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

The Council is focused on developing security standards for the protection of payment card data. Since the payment process involves a variety of stakeholders, it is necessary to get broad perspectives on the risk to payment card data. The Council does this by soliciting experience related to account data compromise, forensic examination, and innovative controls to help shape our views of cybersecurity risk. We believe PCI Standards and supporting resources are highly effective protocols by which any type of business can protect payment card data. Additionally they can offer a clear understanding of card data protection efforts to risk managers in a business. The PCI Standards are used by banks, retailers and any entity that stores, transmits or processes payment card data. Council staff develops and refines PCI standards in conjunction with Council committees and the broader participant membership and in accordance with a published lifecycle.

How do organizations define and assess risk generally and cybersecurity risk specifically?

It has been the PCI Council's experience, as an industry body that represents a diverse population of businesses, that assessment of risk varies significantly from industry to industry, company to company and professional to professional within those organizations. This starts with the fact that what is actually defined as a sensitive asset may not be consistent, and extends into how to protect those assets.

This was the case in the payment field before the PCI Data Security Standard codified what information is considered sensitive and requires protection, along with the outlining the controls and testing procedures needed to verify adequate security. The PCI Standards now provide a global approach to help align critical controls to mitigate evolving risks. The PCI Council also recently released guidance on the subject of performing risk assessment as part of a Special Interest Group initiated by our Participating Organization membership and driven primarily by merchants and security assessors from Europe, Australia and the United States

What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

The PCI Security Standards Council provides a suite of standards use by all entities that accept, transmit, or process data, as well as for the technology vendors and service providers that enable these activities. The Council also develops and distributes supporting materials that cover various domains within the payment transaction. These are outlined below:

- PCI Data Security Standard (PCI DSS): The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. For use by any entity that accepts or processes payment cards this comprehensive standard covers areas of physical and logical security and also includes components of employee awareness. Entities are able to assess their compliance with this standard through an annual assessment by a third party or by using one of the Council's self-assessment questionnaires (SAQs)

- PCI Payment Application Data Security Standard (PA-DSS): The PA-DSS is a set of security requirements for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. The standard ensures payment applications are securely designed and will support organizations PCI DSS compliance efforts. It governs payment applications that are sold, distributed or licensed to third parties, e.g. sold to merchants. Merchants have the opportunity to access the Council's public listing of validated payment applications to find information on products that will support their payment card data security efforts through PCI Standards.

- PCI PIN Transaction Security Requirements (PCI PTS): The PCI PTS requirements apply to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions. Merchants have the opportunity to access the Council's public listing of approved devices that have been tested against the PTS requirements for physical and logical security and that will support their payment card data security efforts through PCI Standards.

- Point-to-Point Encryption: Point-to-point encryption (P2PE) solution requirements are focused on vendors, assessors and solution providers that play a role in developing, implementing or assessing products. The program defines requirements for applicable point-to-point encryption (P2PE) solutions, which are optionally deployed by organizations with the goal of reducing the scope of the PCI DSS assessment and providing an additional layer of security.

- PIN Security Requirements: This standard provides requirements for the secure management, processing and transmission of Personal Identification Numbers (PIN) at ATM and Point-of-Sale terminals for both online and offline authentication. The standard combines payment card-specific principles along with encryption key management requirements, that are cross-referenced from ISO, ANSI, EMV, NIST and FIPS.

The PCI Standards outlined above are written for both technical as well as business controls associated with the protection of payment card data. They focus on practical controls and also people and process orientated methods that businesses can put in place to protect cardholder data. These standards are revised, at a minimum, every three years with necessary updates in the interim if warranted. Please note that this list of standards is not exhaustive but an example of payment-centric work performed by the PCI SSC.

What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Deploying PCI Standards as a basis for protecting payment card data, and then assessing compliance with the standards on a quarterly-to-annual basis, is one measure that merchants, acquiring banks and others in the payment transaction process use to measure performance and ability to manage cybersecurity risk. For example, at a minimum, every quarter, entities validating PCI DSS compliance must scan their environment for new network threats and demonstrate corrective action to mitigate cybersecurity risk. To support this and other efforts to monitor progress against PCI Standards, the PCI SSC has developed an array of programs and resources to support the measurement of progress and security. These include but are not limited to:

PCI Qualified Security Assessor program: This sophisticated assessor program trains IT and payment security professionals to evaluate adherence to PCI DSS requirements. Each entity that receives payment card data is responsible for demonstrating adherence to PCI DSS annually and after significant changes to their environment. The Council maintains a quality assurance program to ensure a pool of globally available, high quality, assessment professionals able to support organization’s security efforts worldwide. A public listing of QSAs is available on its website. The Council uses a similar model for other assessor programs it manages such as those focused on validating payment applications or P2PE solutions.

PCI Approved Scanning Vendor program: Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers mentioned above. Joining the Council’s ASV program requires a rigorous remote test conducted by each vendor on the PCI Security Standards Council's test infrastructure, which simulates the network of a typical security scan customer. The Council has set up the test infrastructure in such a way as to deliberately introduce evolving vulnerabilities and misconfigurations for the vendor to identify and report as part of the compliance testing process. ASVs must pass an annual lab test to maintain their certification. The Council manages a public listing of ASVs on its website. Businesses can choose an ASV partner from the list to conduct a quarterly scan of their infrastructure to ensure it remains secure. Passing this scan may be one performance goal for an organization on its security journey.

Prioritized Approach to PCI DSS: This tool provides six security milestones that will help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance. The roadmap helps an organization to prioritize efforts to achieve compliance; establish milestones; lower the risk of cardholder data breaches sooner in the compliance process. It also helps acquirers objectively measure compliance activities and risk reduction by merchants, service providers, and others. The Prioritized Approach was devised after factoring data from actual breaches, and feedback from Qualified Security Assessors, forensic investigators, and the PCI Security Standards Council Board of Advisors.

Training programs for personnel: The Council firmly believes that technology resources alone are not sufficient to increase the level of security of payment card data. As a recent industry report noted, ”Employees are the first line of defense against physical and digital attack vectors. A lack of proper training and awareness can turn employees from assets into liabilities.” The Council offers a variety of education programs ranging from informal webinars available to members and the business community at large, to specialized instructor led and online training programs designed to build internal expertise in protecting payment card data through PCI Security Standards. These range from an introductory "PCI Awareness" course to a PCI Professional credential, which requires passing an examination. Our broad membership base provides input on market needs that can be addressed through education. Through this direct input the Council developed the Internal Security Assessor (ISA) Program for companies to develop assessment skills to partner effectively with QSAs. Similarly, the Qualified Integrator and Reseller (QIR) program was a response to industry feedback requesting a pool of integrators and resellers that can securely install and configure payment applications for merchants. This effort will introduce millions of new security touch points into the payment card ecosystem to confirm secure hardening wherever a QIR may sell payment application services. Organizations may have performance goals to develop a certain level of internal domain expertise in security matters. PCI Council training programs can assist in this regard.

If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

The PCI Security Standards Council's focus is to streamline and simplify the reporting process for any entity that is required to report on compliance with PCI Standards to third parties such as banks or payment card companies. The Council does this through the provision of reporting tools that are universally recognized by banks and payment card brands.   These templates include but are not limited to the PCI DSS Attestation of Compliance (AOC) and Self-Assessment Questionnaires. These reporting tools are available to download from our public website.

What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Specific to the payments sector and protecting the payment transaction process, the PCI Security Standards Council plays a role in both standards setting and, as outlined elsewhere in this response, in providing tools to help organizations drive and understand their conformity with these standards. We believe this model works in our sector and could be customized for other sectors or for critical infrastructure. The Council cooperates with many other international standards groups such as NIST, European Payment Council, EMVCo, Cloud Security Alliance, ATMIA, ANSI, ISO and others and looks to incorporate security best practices that are relevant to the payment security sphere.

Unlike most standards organizations, PCI standards (such as the DSS) do not mandate specific technical compliance details. Rather, they are practice and result oriented, allowing those that must comply with them to select their own approaches to compliance. Accordingly, those complying with PCI standards use techniques and systems that implement a large number of standards from many different national and international standards to achieve the required results. This provides greater flexibility to those that participate in the payment card environment to pursue robust security in a way that is most in line with their overall IT decisions, budgets, and priorities.

When it comes to assessment of adherence to the PCI Standards, the Council takes a sector specific approach to create assessment and reporting tools that relate specifically to meeting the needs of the business relationships and risk tolerance between banks and their merchant customers and payment card brands and their bank and merchant customers. This approach is proven to be effective for the payment space, which like every industry has its own unique operating environment. In principle, this holistic methodology could be applied to other sectors.

Although the card payments sector falls outside the realm of critical infrastructure, the Council believes that international standards bodies have a great deal of existing material and knowledge to contribute to standards development for critical infrastructure cybersecurity. Familiarity with the standards they have developed, and examples such as the Council’s holistic approach to providing tools necessary to drive conformity in the protection of payment card data, may mean international organizations are able to offer substantial input in the development of conformity assessment procedures too.

Use of Frameworks, Standards, Guidelines and Best Practices

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

What additional approaches already exist?

In the payment card industry, the PCI Standards provide a clear framework for securing payment card data wherever it is stored, transmitted or processed. PCI Standards have been adopted across industries from petroleum to hospitality, retail to airlines, and financial services. As outlined in previous responses, the PCI Council's framework of standards includes lab test requirements for terminals that accept payments and PIN data, lab evaluation for software payment applications, requirements and testing procedures for point-to-point encryption solutions and standards for effective security of how cardholder data environments should be implemented and including such tenets as encryption at the entry point of clear-text data to minimize the value of the data. Our holistic approach also includes tools for supporting and measuring the implementation of PCI Standards.

Which of these approaches apply across sectors?

The PCI Standards Council is focused squarely on protecting payment card data. The standards are focused on this asset and the environment which houses it. There are areas within PCI Standards that have incorporated other relevant publications and best practices from other sectors and areas such as NIST, ANSI, EMV, ISO and OWASP material. For example, encryption key management cross-references multiple best practices mentioned above within our PIN Security Requirements. Conversely, PCI Standards are referenced globally in a variety of international standards, best practices, legislation and other initiatives outside of the specific payment space. Data security best practices may apply across sectors. However, the Council believes that there are specific business practices and commonalities in the payment transaction process that demand a focused approach to securing customers' payment card data, as provided through the PCI Security Standards Council's industry wide standards development process. Initiatives and programs that support or report on the implementation of PCI Standards in a merchant, bank or other entity's environment, have also been crafted with input of payment card brands, forensic investigators, the assessment community, our elected Board of Advisors and other "front line" stakeholder groups. This input is crucial to incorporate the realities and needs of different stakeholder sets who feel the direct impact, challenges and benefits of standards implementation. This unitary approach to securing payment card data provides operating efficiencies to payment card brands, banks and merchants, and encourages effective communication among stakeholder sets. It also allows the payment card industry to enjoy high levels of standards adoption, a real-time ability to respond to emerging threats, and low levels of fraud as measured in basis points. The provision of standards and complementary resources through this streamlined approach is one that could be considered for other sensitive environments, including critical infrastructure protection.

Which organizations use these approaches?

The PCI Standards and supporting programs and resources are widely used by all organizations that store, process or transmit cardholder data worldwide. These include global banks, many types of merchants (e.g. retailers, hotels, and airlines), payment processors and service providers. In the United States, publicly available statistics show that 97% of the largest merchants are using PCI Standards. The PCI Qualified Security Assessor community includes more than 1700 professionals. Over 1400commercially available payment applications have been validated in accordance with the PA-DSS Standard, and over 600 PIN transaction security requirements approved devices are also listed on the Council's website and used in the payments ecosystem.

What, if any, are the limitations of using such approaches?

The PCI requirements are intended exclusively to protect against the compromise of payment card data. They do this through providing a layered approach to security, with PCI controls helping to prevent, detect and react to threats to payment card data. While some industries and organizations have cited the PCI requirements as useful in defining their own data security policies the design and intention of the requirements are drafted and evaluated specifically to protect payment card data.

What, if any, modifications could make these approaches more useful?

Cybersecurity threats are continually evolving. Similarly advancements in technology are impacting traditional card payments in areas such as cloud computing and use of consumer-grade mobile devices for payments. Standards organizations such as the PCI Council strive for a balance that ensures standards remain as current and as strong as possible, but also introduces change in a way that does not jeopardize security efforts for organizations that rely on PCI standards to enable their business relationships and protect their customer data. The PCI Council does this through exhaustive feedback effort and planned three-year lifecycle process with defined opportunities for industry input. This is coupled with continuous evaluation of PCI requirements and frequent FAQs publications to provide clarity to any emerging changes. This is the approach that works for the payments sector. In a critical infrastructure environment a different update cycle or lifecycle process might fit, with the scope to mandate use of specific standards in some circumstances.

How do these approaches take into account sector-specific needs?

The PCI Council brings together a diverse set of stakeholders from across the payment process that all have the aim of protecting their customers' payment card data and their own business and reputation. PCI SSC membership encompasses representation from the payment networks and financial institutions that monitor fraud and data compromise events, to the merchant that accepts payments cards to the vendors that supply secure, PCI lab-evaluated products and the security professionals that evaluate environments across different industries. Through a planned lifecycle for PCI Standards that invites feedback from across the various industries that play a role in the payment chain, a variety of sub-sector needs and opinions are reflected. This holds for other Council initiatives beyond standards setting too. For example, the Council supports an annual open submission process for the Community to propose Special Interest Group (SIG) projects. Anyone within the PCI community can propose or be involved in SIG work. A SIG's goal is to produce guidance on a specific area of security payment card data through PCI Standards that reflects the learning and experiences of a variety of industry verticals using the standards. Additionally, every two years the Council holds an open election for a 21 member Board of Advisors whose specific task is to represent their industry vertical and global geography in the Council's work. Any Participating Organization (PO) member company can nominate and vote in the Board of Advisor elections. Information on the Council's current Board can be found here.

When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Based on the previous points discussed, specific to the payments space, it is the PCI Council's opinion that globally applicable payment card standards are best developed through a community of representatives from across industry, geographical region and incorporating a diverse set of experience. Any framework developed should be able to satisfy and react to all stakeholders that may be impacted by such requirements and not unintentionally create an advantage for any set of stakeholder over another. Although there are a variety of broadly applicable security standards available, there is great value in sector specific approaches that encompass the specific needs and perspectives, and unique operating environments of a particular industry.

What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

One important role that various sector agencies and similar councils can play is the development of a comprehensive communication and information sharing strategy. Such a strategy could help foster support and knowledge of cybersecurity threats that may not have an immediate impact on one potential sector but allow for the other sectors to gain valuable intelligence that may allow them to modify their recommended security postures. Information sharing is most successful, valuable and effective when it includes liability and confidentiality protections for providers and receivers. Sector specific agencies and their stakeholders represent a valuable communication channel for NIST in the promotion of any developed framework. In the case of PCI Standards there are clear business incentives to minimize risk, and protect reputation that spur adoption across the global payment chain. Sector specific agencies may have a similar role to play as the Council in incentivizing adoption of the framework in their respective oversight areas.

What other outreach efforts would be helpful?

As outlined above, information sharing forums, when they include protections for participants, provide an opportunity to bring together a variety of perspectives on addressing common risks. In the PCI Council and other voluntary consortiums, regular working groups, Special Interest Group projects and Community Meetings facilitate engagement with the entire community. This type of frequent interaction facilitates knowledge sharing across geographies and vertical industries.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

The PCI Council will comment below where these practices appear in PCI Standards. and provide commentary on broader applicability.

• Separation of business from operational systems;

While PCI DSS does not require that business and operational systems must be separated, it does recommend using network segmentation to isolate systems that store, process or transmit cardholder data (or systems that are connected to such systems) from those that do not. Additionally, PCI DSS requires implementing only one primary function per server to prevent functions that require different security levels. Segmentation when properly implemented may allow an entity to reduce the scope of their PCI DSS assessment making PCI DSS adoption efforts more manageable by allowing the entity to focus associated personnel, security resources, etc. on a smaller, more well-defined environment.

• Use of encryption and key management;

The PCI standards (including PCI DSS, PA-DSS, PTS, P2PE and the PIN Security Standard) require use of encryption to protect payment data as well as robust key management processes to protect the cryptographic keys. While encryption plays an important role in the protection of sensitive information such as payment card data, key management is a critical function of encryption that if improperly implemented may provide a false sense of confidentiality. The PCI Council would encourage a high-level of integrity for critical infrastructure so that the lowest common denominator for key management does not become common practice for data and systems of high sensitivity. .

Importantly, PCI Council standards also prohibit the storage of sensitive data at all except where subsequent access is justified, thereby decreasing both cost and risk. A similar emphasis could be useful in some critical infrastructural areas as well.

• Identification and authorization of users accessing systems;

PCI DSS requirement no. 8 requires that all users be uniquely identified and properly authorized to access any system in the cardholder data environment. Such identification and authorization is necessary to ensure that only authorized users access cardholder data, that every access can be traced to a unique individual for accountability, and that such access can be tracked and monitored. Strong access controls are recommended for any framework developed.

• Asset identification and management;

Asset identification is a critical component to understanding what could negatively impact the security of critical systems and associated data. Regular asset identification should be part of all security frameworks to confirm no intentional or unintentional changes have been made. This becomes even more important when entities acquire other multiple organizations with differing systems. This is common practice in the private sector. PCI standards require organizations to identify and document all their locations of cardholder data within their environment, create a datagram or inventory of their locations of cardholder data, and confirm that all those locations of data are included in the scope of their assessment efforts. This includes all the systems or assets that may store, process or transmit cardholder data. This is essential in the payment sector to ensure all cardholder data is adequately protected; simply put, if an entity doesn't know where its sensitive data and systems are, it cannot protect them. The PCI Council encourages clear direction on what data and systems would be identified under critical infrastructure for consistency in the identification of what is of value.

• Monitoring and incident detection tools and capabilities;

PCI DSS Requirements nos.10 and 11 require logging of access and activities related to cardholder data, as well as vulnerability scanning, penetration testing, and intrusion detection/prevention capabilities. Comprehensive logging and monitoring is critical so that entities know who is doing what and when, and is invaluable as a source of information in understanding any suspicious incidents (e.g., unauthorized access) that may occur. To be most effective across critical infrastructure monitoring must be active, with real-time response and possibly run as an independent procedure to that of administrators responsible for daily security duties.

• Incident handling policies and procedures;

PCI DSS requirement 12.9 requires a detailed incident response plan that allows for immediate response in the event of a system breach and is reviewed at a minimum annually or after any significant change. The PCI Standards ask that the plan include among other elements, assignment of specific roles and responsibilities, response procedures, business recovery procedures, coverage for all components in the cardholder data environment, inclusion of or reference to response procedures from associated business partners. The plan must be not only reviewed but tested annually and include training for responsible staff. It must be a living document. The presence of a well-thought out and periodically tested incident response plan can be a critical part of defense in depth.

In the private sector, annual evaluation can be neglected unless it's part of an organization's ongoing commitment to security. Companies often make significant changes without updating policies and procedures for future employees that assume security responsibilities for their organization. The PCI Council, within our standards framework, encourages not just annual assessment of the incident handling policy but also after significant changes to the architecture such as after a merger of business units or organizations with heterogeneous operations.

• Mission/system resiliency practices;

PCI Standards do not specifically require mission or system resiliency practices (beyond the reference to it in the above-mentioned incident response plan). This is because PCI DSS focuses mainly on the security of cardholder data, whereas mission or system resiliency practices typically focus on availability of data and address an organizations ability to remain operational after a variety of incidents.

• Security engineering practices;

Many of the PCI Standards were designed based on fundamental security engineering best practices, as they focus on secure payment terminals, payment applications, encryption solutions, and cardholder data environments. For example, PCI PA-DSS requires secure coding techniques for applications, and secure access control systems and user authentication that follows fundamental security principles.

The Council would assert that the framework should advocate use of a secure development lifecycle throughout the implementation and management of the critical infrastructure. The

Council would also encourage NIST to recognize that engineering practices will vary by industry based on their understanding of acceptable risk management.

Are these practices widely used throughout critical infrastructure and industry?
As indicated above, many of these practices are used in the payments space through PCI Standards. As previously outlined, publicly available statistics. indicate that 97% of the largest merchants in the United States are compliant with PCI DSS, for example.

How do these practices relate to existing international standards and practices?
The PCI Security Standards are a globally applicable framework and are broadly used throughout the world wherever payment card data is stored, processed or transmitted. Users of PCI Standards would be familiar with the security practices outlined above. The PCI Standards take a layered approach to security with controls to prevent, detect and react to threats to payment card data.

Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?
Asset identification and agreement to which assets qualify is possibly the most critical first step, as all controls cannot be implemented until the appropriate scope has been agreed upon. Identification is often much more difficult in the execution, compared to the theoretical description of behavior in most frameworks.

Which of these practices pose the most significant implementation challenge?
The process of asset identification will only grow in complexity as private sector organizations become more dependent on business partners to help manage and secure assets. Being able to actively and successfully monitor the appropriate access to a wealth of different data and systems will become a more sophisticated task.

How are standards or guidelines utilized by organizations in the implementation of these practices?
While PCI Standards have a broad reach with respect to the payment card information ecosystem, they also relate to only a narrow, specific set of criteria related to payment card data. The explicit focus of data that requires protection allows businesses to more easily identify, monitor and protect against threats related specifically to the exposure of such

information. As outlined, the PCI Standards reference many of the practices above. Companies use security standards as both a high level “philosophy” on security and as a more detailed “playbook” of controls. NIST may also want to consider the balance between demonstrating the objective or intent of a control versus specifying a prescribed way to achieve the control.

Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

The PCI Security Standards Council brings together representatives from over 670 global companies that through their membership have made a commitment to having their industry, geography and specific business’ perspectives reflected in the creation of PCI standards. Membership in the PCI Council and participation in standards setting and other activity is entirely voluntary. Membership for the vast majority of those companies involves only a modest fee. It is therefore encouraging that so many global companies are actively participating. In addition, many larger companies that use PCI standards are investing in PCI education for their staff. This ensures they have the personnel resources to use PCI standards to protect payment card data through maintaining a secure infrastructure. For example, over 650 companies have invested in the Council’s ISA training for their staff. The PCI Standards ecosystem encompasses much more than IT standards. In formulating the holistic approach discussed throughout this response, and to ensure the successful adoption of PCI Standards through the payment transaction process, the Council draws on input and expertise from testing laboratories, assessment experts, forensics investigators, risk specialists, technology vendors and business professionals from financial services and merchant backgrounds.

The payments ecosystem is complex. With millions of merchants worldwide accepting payment card data, there is a population of smaller merchants that focus their resources on running their core business as opposed to having a security methodology or playing an active role in Standards setting and related activity. Representation of their interests is gleaned through association members and other entities (payment service providers, resellers, banks and vendors) that interact with this community.

Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

PCI Security Standards Council requires the ongoing monitoring and risk identification for emerging threats either directly within our standards or the basis for new requirements.

Additionally, any organization that stores, transmits or processes payment card data is required, at a minimum, to thoroughly scan their environment by using an Approved Scanning Vendor (ASV) at least every three months to detect threats that may have gone undiscovered. The PCI Council uses the risk rating developed and maintained by the National Vulnerability Database and FIRST. The Council monitors cybersecurity risk in a number of ways. This includes through regular meetings with participants in the PCI Forensic Investigator program , our laboratory testing partners and many other industry stakeholders involved with cybersecurity activity.

What are the international implications of this framework on your global business or in policymaking in other countries?

In formulating the PCI Security Standards Council approach, we recognize that payment networks and their users transcend national borders. As such, the PCI Council invites stakeholders worldwide to join us in our work. The Council works to provide a global standard with international support and collaboration that can be monitored and assessed against, that reflects and balances the business realities of our US headquartered Participating Organization members as well as our many international participant members.

The PCI ecosystem of standards and associated tools provides businesses globally with a consistent way to demonstrate adherence once to a comprehensive set of requirements in whatever regions they do business and store, process or transmit to payment card data. This streamlines their reporting requirements to global business partners such as to banks and card brands. The Council recommends any framework for critical infrastructure give due consideration to the international operating realities of any business that will be subject to its use.

In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

Any framework should aim to provide multi leveled layers of protection. For example, to protect payment card data the PCI Council takes a security-in -depth approach. PCI Standards are multi-layered and provide security controls to prevent, detect and react to threats to payment card data.

Security awareness training is another critical component for any successful framework. Having security policies provides limited value unless those professionals responsible for performing the duties described are aware and appropriately trained. Policies will only be effectively implemented if those responsible have the awareness and appropriate skill to execute identified cybersecurity controls.

Additionally, the requirements will only be enforced with demonstrative assessment and an ongoing system for validation. In the private sector, technology and its use evolves quickly, companies are sold or acquired and processes merge on a regular basis. We encourage NIST to consider these dynamic changes in an environmental approach, and support regular auditing or assessment of critical infrastructure environments by organizations qualified to do so.

Conclusion

The Council supports the Executive Order's recommendation to create a framework for critical infrastructure cyber security, and looks forward to supporting NIST in this process. Many standards and proven constructs exist to help support NIST in the process of establishing the first draft of this framework. The challenge ahead is to identify and recognize at what level existing voluntary standards can be leveraged, and how to incentivize private sector entities to use any proposed framework or standard.

Similar to the role that the PCI Council plays within the payment space, NIST must find a way to facilitate collaboration from a diverse group of participants while not dictating a myopic way forward for any one industry. All impacted stakeholder groups should have a seat at the table, and NIST should ensure the discussions focus on the framework's intent and not on specific technology agendas. Similar to the Council's holistic approach, NIST may want to take an environmental approach to achieve its objectives. Will presenting an IT framework alone be sufficient to drive improved security in the critical infrastructure market? Or will the creation of assessment protocols, product validators or other supporting tools also be necessary in order to spur adoption and advance the cyber security agenda? In addition to removing barriers to adoption, there must be a clear business case to understand and agree to validate against this framework.

The PCI Council would encourage building mechanisms for frequent diagnostics and protected information sharing into the framework. There must be ongoing threat evaluation and a methodology to share and react to findings. Many such constructs exist in the financial services sector and it is important to study these to ensure that this process does not “reinvent the wheel.” This information sharing may stimulate innovation for security mechanisms to address new threats. Within payment networks the return on security investment has generated improvement in the development of advanced encryption, sophisticated removal of sensitive data via tokenization and spurred acceptance of evolving technology such as mobile payments. Finally, any framework must not only understand the changing threat landscape, but also reflect an understanding of the unique operating environment of organizations responsible for managing critical infrastructure.

The PCI Security Standards Council stands ready to share any further expertise with NIST and supporting agencies in the development of this framework.