VISA

Russell W. Schrader
Chief Privacy Officer
Senior Associate General Counsel
Global Enterprise Risk

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899
(Delivery via e-mail to cyberframework@nist.gov)

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

Visa is encouraged by the White House's effort to better secure our nation from cyber attacks through increased public-private collaboration. The attention to cyber security is helpful, timely, and critical, and Visa appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST) Request for Information (RFI). We hope that our perspectives may help guide government and industry efforts to better cooperate on a national cyber security framework. As Patrick Gallagher, U.S. Under Secretary of Commerce for Standards and Technology and Director of NIST, recently said:

> "This multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested. The approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace."

Industry participation is vitally important in understanding the different requirements that exist across business sectors and individual companies within those sectors. And although a "one size fits all" approach will not work, there is one unifying goal shared by all stakeholders: protecting consumers and the economy, by maintaining a secure infrastructure in the face of threats like cyber attacks.

Visa is one of many organizations operating in a complex, diverse financial services sector. Within this sector, government already plays a valuable role in maintaining a secure infrastructure, and we must continue to build on these public-private partnership successes. For example, the Federal Financial Institutions Examination Council (FFIEC) continuously assesses financial institutions' controls for cyber and physical security, business continuity and operations management. For companies like Visa with operations around the globe, the ability to globally scale an effort like cyber security is important to avoid confusing, duplicative or contradictory standards.

This submission provides Visa's perspectives on building a strong, public-private cyber security framework, including:

- An overview of Visa's current risk management practices;
- Feedback on the use of frameworks, standards, guidelines and best practices; and
- Specific industry practices.

Current Risk Management Practices

Cyber security will always be a top priority for Visa. Our company has helped build the electronic payments ecosystem over more than 50 years, and that ecosystem is founded on the promise to consumers, merchants, and financial institutions that transactions will be securely and efficiently processed. In recognition of this trust placed in us, Visa is relentless in fortifying the security of our own systems and the broader payment ecosystem through partnerships with industry organizations, governments and law enforcement officials. Below are five broad examples of our work:

Protecting System Data

Recognizing that there is no "silver bullet" to protecting payment data, Visa uses a coordinated, defense-in-depth approach to cyber security, which relies on concentric layers of security controls that prevent data theft and fraud and are more impenetrable than any one control alone. In addition, we apply the concept of "least privilege," which ensures that users of any system are granted the least amount of privilege necessary to perform the duties of their jobs.

Maintaining Compliance Among Contractors and Other Vendors

Participants in the payments ecosystem are entering into ever more complex outsourcing arrangements with contractors, their sub-contractors, licensees and others. Visa responds to this complexity by setting clear standards and then enforcing them through a variety of techniques, including targeted site inspections to confirm continued adherence to established security standards.

Implementing Secure Technology in Our Products and Services

Visa maintains leading security technologies and processes in our processing environment and for every product and service we offer, strengthened by standardized, well-tested security governance that protects our customers. We also invest heavily in workforce training and development to ensure that our people are equipped with the knowledge and skills necessary to maintain security secure payments network, because just as important as the technology is the human power behind it.

Eliminating and Devaluing Sensitive Data
Beyond Visa's efforts to build a strong perimeter defense, our organization works with stakeholders throughout the payments ecosystem to eliminate unnecessary, sensitive data from systems wherever possible. For example, Visa partnered with the U.S. Chamber of Commerce on the "Drop the Data" campaign, which educates small merchants on the importance of securing their systems and eliminating unnecessary data. We also regularly share best practices and guidance on the use of encryption and tokenization to help organizations devalue vulnerable payment data. Visa also recently announced updates to our plan to drive EMV chip adoption for debit and credit cards in the United States. Chip technology, which is used extensively in other parts of the world, introduces dynamic elements into each transaction message, making payment data less attractive to thieves – and thus less susceptible to cyber attack – by rendering it useless for card-present fraudulent transactions if stolen.

Coordinating with Law Enforcement
The increasing sophistication of cyber-attacks and intrusions by hackers demands coordination between public- and private-sector organizations, but finding and bringing these criminals to justice is often difficult. Visa partners closely with law enforcement and government on the investigation of many cases and maintains relationships with the U.S. Secret Service, Federal Bureau of Investigation, Department of Homeland Security, Department of Defense, National Security Agency, Interpol and other federal and state agencies. Visa provides training as well as the *"Resource Manual for Prosecutors and Investigators"* to help law enforcement better understand the payment system and financial crimes. Additionally, we maintain a 24-hour hotline for law enforcement agents to call for assistance in investigations.

Although international cooperation has improved, some nations are still reticent to collaborate on prosecution. More troubling is the reported involvement of some governments themselves in perpetrating cyber-attacks against businesses.

Use of Frameworks, Standards, Guidelines and Best Practices

Visa recognizes that securing our own network is not enough. Payments take place in an ecosystem that includes financial institutions, other payment networks, processors, vendors, merchants, and consumers. In order to improve security best practices across this complex system, Visa has collaborated with stakeholders to set clear, *centralized* standards that can be implemented in a *decentralized* fashion.

Without clear, mutually agreed-upon standards, it is impossible for participants in any system to know if their security practices are sufficient. Although the establishment of such standards requires extensive collaboration – since no single entity can keep the entire system secure or has the complete knowledge to set standards for all other participants – Visa is proud to participate in a number of very good cyber security standards that exist today:

- Payment Card Industry Data Security Standards (PCI DSS)
- EMVCo Standards
- International Organization for Standardization (ISO) Standards – ISO 27001 and ISO 27002
- Accredited Standards Committee X9 – Financial Services Standards
- FFIEC / National Institute of Standards and Technology Requirements – NIST SP 800-53
- Financial Services Information Sharing and Analysis Center (FS-ISAC) Best Practices
- Sarbanes-Oxley and Gramm-Leach-Bliley Requirements
- Control Objectives for Information and Related Technologies (COBIT)
- Federal Information Processing Standards – FIPS 140-2
- Global Platform Specifications

These standards and requirements are thorough and cover logistical, physical, technical and operational elements of security. They have been developed over many years and are constantly being reviewed and updated. The PCI DSS standards are of particular interest because they were developed with input from a wide range of stakeholders, are updated to reflect new threats and developments in payments, and are scalable to both the largest and smallest users of payment information.

Beyond industry standards and best practices, there is an opportunity for government and industry to coordinate public education and awareness efforts on cyber security. The Department of Homeland Security's partnership with the National Cyber Security Alliance to promote the education campaign "Stop. Think. Connect." is a good example of how the government's credibility and resources can be deployed to educate consumers. Visa is proud to support this effort, as well as the U.S. Cyber Challenge, which aims to significantly reduce the shortage in our country's cyber workforce through accessible, compelling programs for students.

Specific Industry Practices

As government seeks to enhance cyber security by centralizing *best practices*, it is important to avoid centralizing *implementation* of security measures across a diverse economy. Mandating specific technologies or solutions can have unintended consequences and inhibit innovation. Suitable, effective security controls in one environment may be unworkable, unnecessary, or even counterproductive in other environments.

Government is uniquely able to encourage transparency and improved information sharing regarding threats, vulnerabilities and controls: with private industry, between government agencies and even across international institutions that may have differing views and requirements. Since improved information sharing is core to the success of enhancing cyber security across industry sectors, Visa supports the White House objective to improve and broaden the sharing of confidential information to help thwart cyber attacks. We also support a legislative solution that affords appropriate legal and privacy protections for information sharing between government and the private sector. These protections will allow government and businesses to exchange specific threat information and defense strategies, secure the nation's cyber assets and mitigate emerging threats in real time, all with appropriate liability, antitrust and freedom of information protections.

Once cyber threat information is readily shared between the public and private sectors, it will be necessary to expand existing threat-informed risk management and mitigation efforts, as well as sector-coordinating councils and government operations centers. Such steps will better position public- and private-sector officials to collaboratively oversee cyber security efforts in the future.

Conclusion

Securing America's critical systems is a shared responsibility and must be a top priority of government and the private sector. Public-private collaboration is necessary to build a comprehensive national cyber security framework – one that adopts best practices, facilitates better information sharing, and expands cyber security education and talent recruitment efforts.

However, in order for any of these efforts to ultimately be successful, governments must increase law enforcement capabilities to investigate, disrupt, apprehend and prosecute cyber criminals in the U.S. and abroad. Visa supports the Administration's recent comments at the highest level about the crisis of international cyber crimes, and we welcome a renewed effort to establish international cooperation to apprehend and prosecute cyber criminals and establish consequences for countries that harbor cyber crime rings. We support efforts to eliminate havens for cyber crime through improved extradition agreements, aggressive prosecution and implementation of international treaties that pursue a common criminal policy against cyber crime. Indeed, stopping cyber crime at the source – frequently outside the U.S. – remains the surest and most efficient path to mitigating the threats we face.

Visa will host its fifth Global Security Summit in Washington, D.C. on October 2, 2013, which brings together hundreds of representatives from the worlds of commerce, banking, government, academia and law enforcement to explore how payment system professionals can work with merchants and government officials to protect cardholders and businesses against current and emerging security threats. We will extend an invitation to NIST in the coming months.

Visa looks forward to working with the Administration and Congress to combat growing cyber threats in a manner that serves the interests of consumers, businesses and our entire country.

Sincerely,