VMware, Inc. Response to RFI
Citation Number 78 FR 13024
Document Number 2013 – 04413

Background

VMware is the world's leading virtualization, data center consolidation, and cloud computing infrastructure software company. With approximately 300,000 global customers and about $5 billion in revenues for 2012, VMware currently supports 100% of Fortune 100 and 99% of Fortune 1000 companies. VMware was founded and built upon the success of virtualization software that is easy to install and use, resilient, and extremely cost efficient with rapid ROI that regularly exceeds 25%. Due to the significant and rapid payback of investments in our infrastructure software solutions, VMware captured about 80% share of the virtualization technology market.

Building upon this success, VMware expanded into a comprehensive portfolio of virtualization and cloud computing software solutions that encompasses: virtualization and physical management, data center consolidation, private/hybrid cloud management, virtual security, virtual configuration management, and end user computing environments. As a result of this success and the considerable adoption of our infrastructure software, VMware has a unique perspective pertaining to advanced data center operations and management that spans virtually every industry. As such, VMware welcomes the opportunity to contribute to this effort on an ongoing basis.

Commitment to Standards

VMware applauds this effort by NIST to gather input and suggestions from industry. In fact, VMware has demonstrated a strong corporate commitment to the use and advancement of standards across the industry. VMware has provided resources to support the efforts of the Distributed Management Task Force (DMTF), including the current DMTF President, who is also a VMware employee. Through these efforts, VMware has worked across the industry to facilitate the establishment of various standards including the Open Virtualization Format 2.0 and open API based Cloud Management Standards. VMware has also been adhering to the Common Criteria standard to certify a number of our core products at the EAL 4+ level. Thus, VMware is supportive of the approach and objectives associated with a standards-based approach to cyber security and protection of our Nation's Critical Infrastructure. VMware has taken an international approach to standards that includes coordination and participation with numerous standards bodies including IEEE and ISO. As a global company, it would be our preference for the cyber security standards framework to have global applicability. However, we also recognize that such a global approach could take time to unfold and each respective standards body might not work on the same timeline.

Challenges

One of the most significant challenges that VMware anticipates with an effort to improve cyber security practices across critical infrastructure is the very disparate and often independent nature of these various sectors. The organization challenges that stand in the way of the development of a framework that meets the cyber security needs of such a disparate group will be significant. With such a broad constituency involved, reaching a consensus could prove to be a formidable task. In addition, a delicate balance is required to ensure that any framework is general enough to provide benefits to all critical infrastructure sectors while also remaining flexible enough to meet potentially unique requirements that any individual or small number of sectors may need. Achieving such a balance is a critical success factor for this effort. It can not be overemphasized how important it is for this cyber security framework to avoid being overly prescriptive, which

could drive up costs and complexity across the entire critical infrastructure ecosystem – and would be counterproductive to the primary objective of improving cyber security.

Risk Management

Current risk management frameworks such as FISMA, DIACAP and the new FedRAMP process are good examples of processes that are supported by standards that address the three inter-related aspects of a comprehensive risk management approach: managerial, operational, and technical control environments. Both FISMA and DIACAP are very mature frameworks for ensuring that a comprehensive approach to risk management is adopted and institutionalized. Since FedRAMP is based upon these proven processes, it will also gain from the years of experience and lessons learned across the government through their use. The primary challenge associated with these legacy approaches is to steer away from the historical tendency to take a "check-the-box" approach to managing risk. In today's highly dynamic and threat filled environment, a truly risk based approach to cyber security is required.

Due to the extensive capabilities in data center management, virtualization and cloud computing provided by our software based solutions, VMware has a broad and unique perspective within the risk management ecosystem. First, VMware virtualization technology has enabled a massive consolidation across the server and infrastructure layer within data centers. At the same time, through policy driven automation and multi-site fail over, VMware has developed considerable expertise in the components necessary to manage risk at the management level. In addition, VMware technology has helped to combine IT roles in a manner than increases efficiency but at the same time includes features that enable the largest and most complex organizations to maintain, log, and manage separation of duties.

In a similar manner, VMware technologies have become a major component of modern, agile data centers from an operational perspective. Operationally, VMware software enables a very dynamic and agile operating environment. In no small way, this very dynamic nature of applications and data running on our infrastructure software can be made inherently more secure. Moreover, VMware has continued to drive our research and development activities towards the expansion and extension of a security "defense-in-depth" architectural model into the virtual and cloud computing environment. As a result, we have learned how our infrastructure products, features, and capabilities can be integrated and enacted within a broader solution that is substantially more secure than the legacy alternatives. For example, we are aware of one Federal agency customer that is using a number of our products to implement an "auto-quarantine" capability that balances the need for increased automation and security without impacting operations and users.

From a technology standpoint, VMware software enables a considerable consolidation at the infrastructure level. Through this consolidation, and the significant reduction of basic footprint exposure, many data centers have been made to be more secure. Our automation technology enables customers to configure security approved baselines at the virtual server level, virtual firewall level, and even the virtual data center level and leverage the automation features of our management software to ensure real-time configurations remain in

compliance with approved security baselines. Through this combination of shrinking the size of the physical infrastructure, policy driven automation, and adherence to proven security based protocols, VMware has identified emerging best-practices that should be considered within the cyber security standards framework.

Critical Infrastructure Interdependencies

VMware recognizes that many critical infrastructure components may be related. At the same time, legacy methods for the integration and management of interconnected systems are brittle as well as complex. These characteristics can work in tandem to present a higher risk profile than would otherwise be necessary. In addition, the emergence of cloud computing has introduced another variable into the data center and infrastructure equation. Through experience, VMware has learned that it is not only the underlying technologies such as virtualization and operations management that present the opportunity to add resiliency and security. It is how the underlying solution is architected, configured, and integrated that also makes a significant difference from a resiliency and security standpoint. VMware specializes in the ability to share physical infrastructure, abstract access and environments through software, and protect the integrity of the environment to meet robust service and performance levels. Through this experience, VMware has developed a comprehensive set of products, reference architectures, and intellectual property that together enable a range of best practices and capabilities to be brought together in a secure but shared, hybrid cloud model.

Closing

VMware is highly supportive of this effort by NIST to include input from industry as it explores a cyber security standards framework. As described herein, VMware believes our industry leading infrastructure products and experience have led VMware to develop considerable expertise and best-practices that can help this effort to succeed. We also caution against an approach that is overly prescriptive that could potentially undermine the objectives of this effort. For example, specific technology products or solutions should not be prescribed as the government should not be in position to provide an advantage or disadvantage in the marketplace. In addition, while transparency is important, it is more important for the government to share specific information with industry about cyber security vulnerabilities. It is not in the best interests of competition, efficiency or security for trade secrets, supply chain, or other intellectual property of industry to be shared. Ultimately, it is the purview of the Congress to provide the Federal government with the statutory authority and clarity to share government information with industry.

Again, VMware is very supportive of this effort. We would very much appreciate the opportunity to work with NIST, the Administration, and the Congress to address the critical need for enhanced cyber security going forward.