Submission to the National Institute Standards of Technology

Response to the NIST Cybersecurity Framework Request for Information

Comments of Dell, Inc.

October 10, 2014

Via cyberframework@nist.gov

Ms. Diane Honeycutt

Secretary

Computer Security Division

National Institute of Standards and Technology

100 Bureau Drive, Stop 8930

Gaithersburg, MD 20899

I. Introduction

Dell appreciates this opportunity to provide comments to the National Institute Standards of Technology (NIST) on its preliminary observations regarding the NIST Cybersecurity Framework. Dell is a U.S.-based global company with more than 100,000 team members around the world. In recent years, Dell has expanded its cadre of services to support public and private organizations around the world. Dell customers choose Dell technology, services and software solutions to help them achieve unique business goals, improve competitiveness and better serve their customers while streamlining IT operations, increasing end-user productivity and securing data.

II. Framework Activity and Dell

Earlier this year, pursuant to Executive Order 13636 signed by President Obama, NIST released its first iteration of the NIST Cybersecurity Framework (the Framework) to help critical infrastructure owner-operators start a cybersecurity program or improve an existing one. The Framework was developed in collaboration with public and private organizations, including companies and trade associations.

The Framework features a number of steps that all businesses can take to assess and strengthen their state of cybersecurity over time. It also provides organizations—including their customers, partners and suppliers—with common language for understanding their current cybersecurity posture, setting goals for cybersecurity improvements and much more.

NIST and Dell, along with key partners and industry associations like the U.S. Chamber of Commerce and the Information Technology Industry Council (ITI), have participated in various public meetings to facilitate an ongoing discussion on the strengths and weaknesses of the Framework and how to promote greater awareness of the Framework. Dell has also supported interactions aimed at better understanding the scope and reach of the Framework with international government partners, critical sectors and medium and small businesses. In addition to closely evaluating the Framework's potential impact on Dell internal operations, Dell is committed to facilitating a dialogue with customers regarding the Framework and particular steps that they can take to assess and strengthen their state of cybersecurity.

Beyond attending formal NIST Cybersecurity working group sessions, Dell participated and hosted public discussions, complementing other efforts to promote the Framework and supporting a voluntary, flexible and evolving cybersecurity policy approach that identifies security goals and affords industry the flexibility to reach those goals through the use and application of various tools.

Some of these public discussions include:

- July 10, 2014 in Austin, TX, the Chamber of Commerce 2014 Cybersecurity Education & Framework Awareness Campaign: Matt Scholl, the acting director of the National Security Division of NIST; Jeanette Manfra, Director of Critical Infrastructure Cybersecurity at the White House; and Brian Engle, CIO of the State of Texas; Alan Daines, CISO Dell, Inc.
- September 25, 2014 in Washington, DC. Software & Supply Chain Assurance Forum: Improving Cybersecurity Through Acquisition: Jon Amis, Dell Supply Chain Assurance Program Director
- October 28, 2014 in Washington, DC, the Chamber's Third Annual Cybersecurity Summit: Paul Christman, VP of Dell Software
- November 4 – 6, 2014, Dell World 2014 – NIST's Dr. Ron Ross with DELL CSO John McClurg – NIST and the New Cybersecurity Framework
- Dell Software – Webcasts: "An Introduction to the New NIST Cybersecurity Framework" – Jack LeGrand, Federal Programs Coordinator
- Dell Software – Webcast: "Test Your Prepared NIST" –Jack LeGrand, Federal Programs Coordinator
- Dell Software – Webcast: "The NIST Cybersecurity Framework and Preparing for the Adoption of DHS CDM."

We commend NIST and our industry partners for looking beyond the initial target of IT security for large organizations and moderating discussions about opportunities for small to

medium-sized businesses to take advantage of the Framework as well. Below are a few select reflections on our experience to date with the Framework.

III. Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness; NIST solicits information about awareness of the Framework and its intended uses among organizations.

What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

We are starting to see traction from customers across sectors. Commercial Identity Verification (CIV) agencies are leveraging the Framework in security and strategic planning discussions (as would be expected). Agencies intending to utilize the Department of Homeland Security's Continuous Diagnostic and Mitigation (CDM) program are directed to measure their agency's security posture according to the Framework and where appropriate, prepare to fill gaps with CDM. Department of Defense agencies are starting to show interest, especially since the March 2014 announcement that the NIST Risk Management Framework will replace Defense Information Assurance Certification and Accreditation Process (DIACAP) in the next three years.

How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

Because the framework is relatively new, Dell is supporting existing customers through individual discussions on the Framework. This includes our standard security briefings with federal government customers, participation in events around this topic, continuing education courses at Armed Forces Communications and Electronics Association (AFCEA) conference & chapter events, and marketing collateral and certain media and advertising activities. Dell has not received many unsolicited inquiries about Framework support; however, is currently viewed as a "best practice" approach versus a compliance/governance concern. Dell has conducted multiple webcasts [for customers/suppliers] to accelerate the understanding and adoption of the Framework as an enterprise tool.

Is there general awareness that the Framework?

> ***a. Is intended for voluntary use?***
> ***b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?***
> ***c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?***

Risk, security and IT management professionals seem to understand that DHS has released new cybersecurity guidelines. However, the questions often begin with the relevance of these guidelines. Because government is driven by compliance mandates; private sector concerns vary by industry. Once Dell explains and supports the Framework as a best practice to prioritize needs and resources (instead of a compliance checklist), the concept is usually well-received.

Is intended for voluntary use?

Dell believes that the structure and intent of the Framework is for voluntary use as a collection of best practices and dynamic guidelines based on risk. Unlike other NIST standards which become requirements for agencies to follow, the Framework is an adaptive tool that helps agencies identify and classify enterprise systems by criticality. It is not a requirement for agencies to utilize it.

Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

Yes. In the past, IT and Risk were often operationally part of two separate activities (technical requirements and business/mission requirements) though IT risk is a component of a broader risk strategy. Cyber threats have now become a risk so great that it has a profound effect on national security and economic stability, leading to a need for resources to support cybersecurity activities. Cybersecurity is becoming more important in the overall risk strategy.

Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

The Framework outlines points to multiple existing references which can be used to define/validate recommended best practice areas.

What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

NIST should consider leveraging security associations (i.e. The International Information

Systems Security Certification Consortium (ISC2), ISACA (previously known as Information Systems Audit and Control Association), Information Systems Security Association (ISSA) and IT industry experts (i.e. Gartner, International Data Corporation (IDC)) to continue the Framework discussion and raise its awareness. These types of organizations tend to drive IT trends in both the government and commercial sectors. Because the application of the Framework is intended to be risk-based, there is a significant amount of interpretative range in the agencies' measurement of similar target systems. NIST, in consultation with industry, should provide guidance on reducing these potential differences so that the remedies for deficiencies in similar circumstances do not also have a corresponding range of quality. In addition, common questions arise about the correlation and utilization of FISMA and the use of the new Framework. NIST should provide guidance with regard to the utilization of the Framework (subjective) with FISMA (objective).

Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

Dell has extensive experience in education and outreach on cybersecurity risk management. The integration of Dell (Quest) Software and Dell SecureWorks capabilities into the Dell portfolio of customer offerings has significantly increased our proactive efforts toward cross-industry education on cybersecurity risk management.

Since its release in February, Dell has been discussing the Framework with federal agency customers and providing formal training (webinars, AFCEA CEU training, etc.)

- Dell Software – Webcasts: "An Introduction to the New NIST Cybersecurity Framework" – Jack LeGrand, Federal Programs Coordinator

- Dell Software – Webcast: "Test Your Prepared NIST" –Jack LeGrand, Federal Programs Coordinator

In addition, the Dell Software Marketing team created an online questionnaire that provided an output of high-level cybersecurity gaps.

What more can and should be done to raise awareness?

- Market the framework as Cybersecurity best practices for all businesses and agencies, not just for critical infrastructure.
- Develop opportunities to inform senior management across industry sectors how to combat cyber threats. With recent high profile breaches, cybersecurity is top of

mind in the executive suite.

- Solicit more IT-related professional organizations and industry analysts to actively discuss the pressing need for more common cybersecurity practices, touting the framework as a starting point and a common language. This could lead toward greater awareness and adoption with key IT influencers.
- Keep the message simple, direct and as a best practice. The core table (five functional areas) is a simple concept that is relatively easy to grasp. DHS should be transparent and use it more to stimulate a broader discussion, leveraging the simple graphics to quickly relay the key value proposition.

IV. Dell's Experiences with the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

Has the Framework helped organizations understand the importance of managing cyber risk?

The Framework has supported key discussions that have allowed some sectors more than others to make progress in understanding the importance of managing cyber risk. Dell's experience is that organizations aware and fluent in the Framework are security, risk, or audit organizations; these organizations are in the process of socializing the Framework and the importance of managing cyber risk to other companies at large.

What benefits have been realized by early experiences with the Framework?

The Framework has provided a structure and common language to think about and communicate cyber risk consistently. As security, risk and audit organizations begin to socialize the Framework, companies have benefitted from having the built-in credibility of an industry-standard framework which companies may research more fully if they wish.

What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

For those aware of the Framework, it is useful and informative, providing clarity on important aspects of cybersecurity. But as the Framework focuses on cybersecurity, readers may be influenced to believe that "cyber risk" is equivalent to "IT risk", which includes cybersecurity risk. It would be helpful if the Framework discussed the scope more clearly and explicitly in the introductory sections, acknowledging that there are other aspects of IT risk besides cybersecurity risk.

Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

The Framework Core is one of the most useful aspects to Dell. As the Framework continues to be institutionalized in our organization and with others, the Tiers and Profile may become more used and useful. The Framework Core outlines high-level components that should be considered as part of a cybersecurity risk management program. The Profile and Implementation Tiers add a critical attribute which is contextual information – are those applicable components ad-hoc or adaptive, etc.? It would be useful to gain greater clarity from NIST in this area. Also the Implementation Tiers helps baseline where an organization currently stands and helps articulate where it wants to be and how to get there. Overall the three components provide a common sense approach to cybersecurity risk management, and will be extremely beneficial in helping drive a long-term cybersecurity strategy.

* * *

Dell appreciates the opportunity to submit these comments to NIST. If you have any questions about these comments, please contact Marisela Salayandia, Dell Government Affairs, at Marisela_salayandia@dell.com or via cell at 202.733.7136.