From: Markezin, Ernest
Sent: Thursday, January 18, 2018 1:24 PM
To: cyberframework <cyberframework@nist.gov>
Subject: NYSSCPA Comments on NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (2nd Draft)

Please find attached the New York State Society of CPAs comments on the National Institute of Standards and Technology's proposed draft update - Proposed Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework Version 1.1 Draft 2
If you have any problems in opening the attachment, please contact me at 212-719-8303.

Sincerely,

Ernie Markezin

Ernest J. Markezin CPA CGMA
Director
New York State Society of CPAs

[*Attachment copied below*]

January 18, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

By E-mail: Cyberframework@nist.gov

Re: Proposed Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework Version 1.1 Draft 2

The New York State Society of Certified Public Accountants (NYSSCPA), representing more than 26,000 CPAs in public practice, business, government and education, welcomes the opportunity to comment on the above-captioned proposed framework enhancements.

The NYSSCPA's Technology Assurance Committee deliberated the proposed framework enhancements and prepared the attached comments. If you would like additional discussion with us, please contact Jason Palmer, Chair of the Technology Assurance Committee, at 631-300-1710 or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

Harold Deiters

Harold L. Deiters III
President

Attachment

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON

PROPOSED FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY – CYBERSECURITY FRAMEWORK VERSION 1.1 DRAFT 2

January 18, 2018

Principal Drafters

Matthew T. Clohessy
Joel Lanz
Jason M. Palmer

NYSSCPA 2017–2018 Board of Directors

Harold L. Deiters III, *President*
Jan C. Herringer, *President-elect*
Anthony T. Abboud, *Secretary/Treasurer*
Paul E. Becht, *Vice President*
John B. Huttlinger, Jr. *Vice President*
Mitchell J. Mertz, *Vice President*
Candice R. Meth, *Vice President*
Joanne S. Barry, *ex officio*
Dennis N. Annarumma
Edward L. Arcara
Sol S. Basilyan
Christopher G. Cahill
Jack M. Carr
Anthony S. Chan
Salvatore A. Collemi
Mitchell A. Davis
William H. Dresnack
Edward F. Esposito
Mark L. Farber
Lynne M. Fuentes
Jennifer R. George
Craig T. Goodman
Elliot L. Hendler
Douglas L. Hoffman
Patricia A. Johnson
Kimberly G. Johnson
Barbara A. Marino
Tracey J. Niemotko
Kevin P. O’Leary
Thomas S. Pirro
Iralma Pozo
Renee Rampulla
Brian M. Reese
Steven A. Stanek
Denise M. Stefano
Janeen F. Sutryk
Michael M. Todres
Mark M. Ulrich
F. Michael Zovistoski

NYSSCPA 2017–2018 Accounting and Auditing Oversight Committee

Robert M. Rollmann, *Chair*
Renee Mikalopas-Cassidy, *Vice Chair*
Charles Abraham
Michael J. Corkery
Craig T. Goodman
Jan C. Herringer
J. Michael Kirkland
Rita M. Piazza
Victoria L. Pitkin
Joseph J. Puglisi
Dominic J. Rovano
William M. Stocker III
Margaret A. Wood

NYSSCPA 2017–2018 Technology Assurance Committee

Jason M. Palmer, *Chair*
Faisal Ali
Jeff Behling
Harvey G. Beringer
Moises A. Brito
Michael Carroll
Xin Chen
Matthew T. Clohessy
Robert A. Cohen
David O. Daniels
Maureen P. Downing-Cilano
Christopher Gagliardi
Anthony J. Girard
James C. Goldstein
Zachary Gordon
Heather Heale
Jill Johnson
Dekedrian Johnson
Jennifer A. Kartychak
Lucas Kowal
Jim Krantz
Joel Lanz
Shelly E. Mitchell
John Nasky
Bruce H. Nearon
Yossef Newman
Joseph B. O’Donnell
Benjamin Parlato
Robert Patterson
Florence G. Pavalow
Andrew Phillips
Karina Pinch
Michael A. Pinna
Yigal Rechtman
Clayton L. Smith
Thomas J. Sonde
Rebecca Stockslader
Christopher J. Zingalli

NYSSCPA Staff

Ernest J. Markezin
Keith Lazarus

New York State Society of Certified Public Accountants

Comments on
Proposed Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework Version 1.1 Draft 2

General Comments

Overall, we support the proposed enhancements to the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

In response to NIST's request for comment on whether the revisions in Version 1.1 Draft 2 (Draft) reflect the changes in the current cybersecurity ecosystem (first question, line 30 of the Draft), we recommend that the 'Framework Implementation Tier' definitions incorporate guidelines to benchmark an organization's sophistication in managing legal and regulatory risks.

Regarding the two other specific questions, we do not believe that the proposed changes would impact the use of the framework either by a current user of the framework (second question, line 33 of the Draft) or those currently not using the framework (third question, line 35 of the Draft).

As a "one size fits all" framework there are naturally areas of compromise that will need to be made. We are especially sensitive to the needs of small and mid-size entities that are challenged in finding reputable guidance in managing their cyber risk programs. For these entities we recommend the following enhancements that we believe would facilitate the use of this tool with other reputable tools.

1. In the Informative References of Table 2 Framework Core consider providing references to "NISTIR 7621 Revision 1 Small Business Information Security: The Fundamentals." As a related NIST publication this cross-reference would facilitate the administrative burden of small businesses having to reconcile recommended practices between two NIST publications.

2. Consider providing a risk priority to the framework's requirements. For example, can results from the NIST and General Services Administration (GSA) sponsored project, "The Cyber Risk Predictive Analytics Project," be used to identify critical risks and actions?

Specific Comments

We concur with the importance of considering legal and regulatory risks as a part of assessing the risk management practices of an organization as described within Section 2.2 (Framework Implementation Tiers) of the proposed framework.

While legal and regulatory requirements are cited as a consideration, the framework's subsequent definitions for Tier 1-4 risk management practices do not provide measurements for organizations to assess how their legal and regulatory risk management practices align to specific Tiers.

The cybersecurity legal and regulatory landscape is becoming increasingly more active, with new regulatory requirements originating from activities such as the New York State Department of Financial Services Cybersecurity legislation (23 NYCRR Part 500) issued in March 2017 and the "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" Presidential Executive Order issued in May 2017.

In light of this recently increased volume of cybersecurity specific regulations that are being issued for organizations to assess, and potentially comply with, the gaps in organizations' cybersecurity regulatory risk management practices may become more noticeable. The varying degrees of risk management practices to manage existing regulations; incorporate recently issued regulations into risk management practices; and be properly prepared to incorporate additional new regulations; could be categorized to align with the existing Implementation Framework Tier 1-4 definitions. For example:

- Partial (Tier 1) – Regulatory and legal requirements are not formally integrated into an organization's risk management practices.

- Risk Informed (Tier 2) – Regulatory and legal requirements are established and integrated into an organization's risk management program, but are not consistently monitored for compliance or enhanced when errors or corrective actions are identified through monitoring activities.

- Repeatable (Tier 3) – Regulatory and legal requirements are established and integrated into an organization's risk management program and are consistently subject to monitoring for compliance and adequately responds to errors and corrective actions identified through monitoring activities.

- Adaptive (Tier 4) – Regulatory and legal requirements are established and integrated into an organization's risk management program and are consistently subject to monitoring for compliance and adequately responds to errors and corrective actions identified through monitoring activities. Monitoring of potential changes to legal and regulatory requirements are actively monitored and integrated into other organizational risk management practices, are discussed with senior management and adjustments to adherence monitoring programs are adjusted timely to address new and changing legal and regulatory requirements upon their implementation dates.

Given the increased activity in the cybersecurity legal and regulatory landscape, we recommend integrating criteria specific to legal and regulatory risk management practices, such as the above example, into the Framework Implementation Tier 1-4 definitions. This will allow organizations to better assess what Tier their legal and regulatory risk management practices align to and the incremental activities needed to align to higher quality Tiers.

Other Comments

The line references for our other comments are those as reflected in the NIST Draft with markups.

Line 254 – Given the popularity of the CMMI model in various industries and technology-dependent sectors, would it be practical to compare the Tiers to CMMI maturity levels (e.g., we understand the disclosure in line 410, but it may still be confusing to business leaders)?

Line 521 – We suggest including a sample framework profile that business executives can use as a model in implementing the framework.

Line 570 – By starting with the “design” phase, some business executives may assume that cybersecurity requirements are a “technical” rather than a “business” requirement. Perhaps a more tradition lifecycle that includes “feasibility and analysis phase” should be included so that cybersecurity requirements can be included as part of the system selection process.

Line 615 – As regulatory issues are typically mandatory, these might be better preformed in Step 1 of the establishment of a cybersecurity program.

Line 650 – Consider adding Step 8 that would focus on ongoing monitoring, maintenance and periodic reporting to stakeholders (including boards and executive management).

Line 660 – Specify the responsibilities of those responsible for governance.