From: **Markezin, Ernest**
Date: Thu, Mar 30, 2017 at 12:37 PM
Subject: NYSSCPA Comments on Draft Update of NIST Framework for Improving Critical Infrastructure Cybersecurity
To: Cyberframework@nist.gov

To: Mr. Edwin Games

Please find attached the New York State Society of CPAs comments on the National Institute of Standards and Technology's proposed Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

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
14 Wall Street, 19th Floor, NY, NY 10005

www.nysscpa.org | **Facebook** | **Twitter** | **LinkedIn**

--

[Attachment Copied Below]

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

By e-mail: Cyberframework@nist.gov

Re: National Institute of Standards and Technology
Proposed Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework Version 1.1

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 Matthew Clohessy, Chair of the Technology Assurance Committee, or Ernest J. Markezin, NYSSCPA staff.

Sincerely,

F. Michael Zovistoski
President

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROPOSED FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY – CYBERSECURITY FRAMEWORK VERSION 1.1

March 30, 2017

Principal Drafters

Moises A. Brito
Matthew T. Clohessy
Joel Lanz

NYSSCPA 2016–2017 Board of Directors

F. Michael Zovistoski, President
Edward L. Arcara
Sol S. Basilyan
Barbara A. Marino
Kevin Matz
Harold L. Deiters III, President-elect
Paul E. Becht
Christopher G. Cahill
Mitchell J. Mertz
Jacqueline E. Miller
John J. Lauchert, Secretary/Treasurer
Jack M. Carr
Salvatore A. Collemi
Tracey J. Niemotko
Kevin P. O'Leary
Gregory J. Altman, Vice President
Mitchell A. Davis
Edward F. Esposito
Iralma Pozo
Renee Rampulla
Susan M. Barossi, Vice President
Joseph M. Falbo, Jr.
Rosemarie A. Giovinazzo-Barnickel
Brian M. Reese
M. Jacob Renick
Anthony S. Chan, Vice President
Elizabeth A. Haynie
Warren Ruppel
Steven A. Stanek
John S. Shillingsford, Vice President
Elliot L. Hendler
Jan C. Herringer
Denise M. Stefano
Janeen F. Sutryk
Joanne S. Barry, ex officio
Patricia A. Johnson
Jean G. Joseph
Michael M. Todres
David G. Young

NYSSCPA 2016–2017 Accounting and Auditing Oversight Committee

Robert M. Rollmann, Chair
Michael J. Corkery
Adam S. Lilling
Charles Abraham
Lourdes Eyer
Renee Mikalopas-Cassidy
Matthew T. Clohessy
Craig T. Goodman
Rita M. Piazza
Salvatore A. Collemi
Jan C. Herringer
William M. Stocker III

NYSSCPA 2016–2017 Technology Assurance Committee

Matthew T. Clohessy, Chair
Heather Heale
Joseph B. O'Donnell
Moises A. Brito, Vice Chair
Edgar Huamantla
Jason M. Palmer
Faisal Ali
Jill Johnson
Andrew Phillips
Jeff Behling
Dekedrian Johnson
Karina Pinch
Harvey G. Beringer
Lucas Kowal
Michael Pinch
Michael Carroll
Jim Krantz
Michael A. Pinna
Xin Chen
Joel Lanz
Yigal Rechtman
Robert A. Cohen
Michael Melcer
Clayton L. Smith
David O. Daniels
Shelly E. Mitchell
Thomas J. Sonde
James C. Goldstein
John Nasky
Rebecca Stockslader
Yossef Newman

NYSSCPA Staff

Ernest J. Markezin
Keith Lazarus

New York State Society of Certified Public Accountants

Comments on

The National Institute of Standards and Technology Proposed Framework for Improving Critical Infrastructure Cybersecurity – Cybersecurity Framework Version 1.1

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 there are any topics not addressed in the draft framework that could be addressed, we recommend that board of director governance and audit committee oversight requirements also be addressed within the updated framework.

Specific Comments

We recommend that the Framework Implementation Tiers' Integrated Risk Management Program requirements be expanded to incorporate explicit requirements for board of director involvement in providing governance and approval of organizations' cybersecurity risk appetite levels. These enhancements will further promote an appropriate tone at the top of organizations to manage cybersecurity risk within the organization.

We recommend that the Framework Implementation Tiers' Integrated Risk Management Program requirements be expanded to incorporate audit committee oversight requirements. Explicit requirements to incorporate independent internal control reviews subject to audit committee reporting and oversight will allow for board members to have objective and reliable assurance over the effectiveness of controls that manage and report on cybersecurity risk within their organization.

We recommend that the Framework's Measuring and Demonstrating Cybersecurity guidance be expanded to include objective and subjective measures that are intended to provide management with a score of the state of its cybersecurity program. Incorporating both objective and industry and company specific subjective results will aid management and relevant governance committees in identifying areas of weakness in their cybersecurity programs.