March 30, 2017

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, at (716) 851-8356, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

F. Michael Zovistoski
President

Attachment
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
Harold L. Deiters III, President-elect
John J. Lauchert, Secretary/Treasurer
Gregory J. Altman, Vice President
Susan M. Barossi, Vice President
Anthony S. Chan, Vice President
John S. Shillingsford, Vice President
Joanne S. Barry, ex officio

Edward L. Arcara
Paul E. Becht
Christopher G. Cahill
Salvatore A. Collemi
Mitchell A. Davis
Edward F. Esposito
Joseph M. Falbo, Jr.
Barnickel
Elliot L. Hendler
Patricia A. Johnson

Barbara A. Marino
Kevin Matz
Mitchell J. Mertz
Jacqueline E. Miller
Kevin P. O’Leary
Iralma Pozo
Brian M. Reese
M. Jacob Renick
Warren Ruppel
Denise M. Stefano
Michael M. Todres

NYSSCPA 2016–2017 Accounting and Auditing Oversight Committee

Robert M. Rollmann, Chair
Charles Abraham
Matthew T. Clohessy
Salvatore A. Collemi

Michael J. Corkery
Lourdes Eyer
Craig T. Goodman
Jan C. Herringer

Renee Mikalopas-Cassidy
Rita M. Piazza
William M. Stocker III

NYSSCPA 2016–2017 Technology Assurance Committee

Matthew T. Clohessy, Chair
Moises A. Brito, Vice Chair
Faisal Ali
Jeff Behling
Harvey G. Beringer
Michael Carroll
Xin Chen
Robert A. Cohen
David O. Daniels
James C. Goldstein

Heather Heale
Edgar Humantla
Jill Johnson
Dekedrian Johnson
Lucas Kowal
Jim Krantz
Joel Lanz
Michael Melcer
Shelly E. Mitchell
John Nasky

Joseph B. O’Donnell
Jason M. Palmer
Andrew Phillips
Karina Pinch
Michael Pinch
Michael A. Pinna
Yigal Rechtman
Clayton L. Smith
Thomas J. Sonde
Rebecca Stockslader

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.