

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**

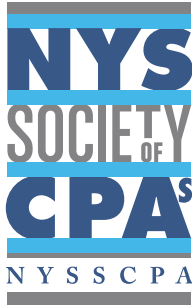
The New York State Society of Certified Public Accountants (NYSSCPA), representing more than 26,000 CPAs in public practice, business, government and education, welcomes the opportunity to comment on the above-captioned proposed framework enhancements.

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

NYSSCPA 2016–2017 Accounting and Auditing Oversight Committee

Robert M. Rollmann, <i>Chair</i>	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, <i>Chair</i>	Heather Heale	Joseph B. O’Donnell
Moises A. Brito, <i>Vice Chair</i>	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.