September 4, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
Computer Security Division, Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

By E-mail: nist800-163@nist.gov

Re: Draft NIST Special Publication 800-163 Revision 1 – Vetting the Security of Mobile Applications

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 draft special publication.

The NYSSCPA's Technology Assurance Committee deliberated the draft 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,

Jan C. Herringer

Jan C. Herringer
President

Attachment

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON

DRAFT NIST SPECIAL PUBLICATION 800-163 REVISION 1 – VETTING THE SECURITY OF MOBILE APPLICATIONS

September 4, 2018

Principal Drafter

Yigal M. Rechtman

NYSSCPA 2018–2019 Board of Directors

Jan C. Herringer, *President*
Ita Rahilly, *President-elect*
Anthony T. Abboud, *Secretary/Treasurer*
Charles Abraham, *Vice President*
Salvatore A. Collemi, *Vice President*
Iralma Pozo, *Vice President*
Janeen Schrann, *Vice President*
Joanne S. Barry, *ex officio*
Darcy Aldous
Dennis N. Annarumma
Sol S. Basilyan
Carnet Brown
Rumbi Bwerinofa-Petrozzello
Christopher G. Cahill
Catherine Censullo
Anthony S. Chan
Mitchell A. Davis
Harold L. Deiters III
William H. Dresnack
Edward F. Esposito
Mark L. Farber
Lynne M. Fuentes
Timothy Hammon
Douglas L. Hoffman
Kimberly G. Johnson
Jennifer Kartychak
Gerard LoVerde
Patricia McGrath
Candice R. Meth
Steven Morse
Tracey J. Niemotko
Kevin P. O'Leary
Thomas S. Pirro
Renee Rampulla
Brian M. Reese
Robert Rollmann
Michael M. Todres
Mark M. Ulrich
David Young

NYSSCPA 2018–2019 Accounting and Auditing Oversight Committee

Renee Mikalopas-Cassidy, *Chair*
J. Michael Kirkland
Jason M. Palmer
Rita M. Piazza
Victoria L. Pitkin
Joseph J. Puglisi
Robert M. Rollmann
Dominic J. Rovano
William M. Stocker III
Margaret A. Wood
Jonathan Zuckerman

NYSSCPA 2018–2019 Technology Assurance Committee

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

NYSSCPA Staff

Ernest J. Markezin

New York State Society of Certified Public Accountants

Comments on
Draft NIST Special Publication 800-163 Revision 1 – Vetting the Security of Mobile Applications

General Comments

We welcome the opportunity to comment on the National Institute of Standards and Technology's (NIST) Draft NIST Special Publication 800-163 Revision 1 – Vetting the Security of Mobile Applications (the Exposure Draft or ED).

The ED is both timely and appropriate. It includes many features, along with collateral risks, that Certified Public Accountants (CPAs) encounter as the advent and maturity of mobile computing has entered the business world, including in business application, tax matters, accounting and reporting, and attest and assurance. We believe this ED will become a helpful tool for CPAs to conduct their analytical and business-related services, with guidance for risks and a risk management approach that are unique to mobile applications, and is complimentary to existing topical literature of the American Institute of Certified Public Accountants (AICPA).

Specific Comments

We offer the following specific comments for consideration as the ED is finalized.

Compliance Risk

The description of the risk tolerance for mobile application (lines 426-429) proposes that risk tolerance for compliance should be assessed as low risk with multiple risk factors that should be strictly responded to. The ED correctly identifies the risk, but does not properly link it to compliance risk. For example, line 210 of the ED refers to "…personal health metrics or personally identifiable information (PII)…" as a reason for devices to have elevated risk, but this is somehow not linked to compliance risk.

In our view, compliance risk is one of the risks that has increased effect on an organization's operations and financial condition. Provided below are just two of many examples:

- The Health Information Portability and Accountability Act (HIPAA) is a compliance risk that is increasingly regulated by prescribed penalty, where discretionary and subjective penalties are not allowed. Accordingly, application security in mobile computing can expose an organization for both reputational and financial damages, increasing the impact. We believe that the compliance risk due to HIPAA is an example where the risk is **not** low.

- New York State regulations for cybersecurity, as well as other cybersecurity requirements from other states and countries, create a prescriptive, compliance exposure for cyber

security developers, hosts, applications, and users. New York State regulation 23 NYCRR 500 is a prescribed regulation that similar to HIPAA has substantial requirements that could lead to reputational, commercial and financial compliance risks. We believe that the compliance risk due to 23 NYCRR 500 is another example where the risk is **not** low.

App Vetting Process

Appropriate attention is given in the ED to the App development and App vetting processes, however we have some specific comments regarding the development and vetting.

We believe the App Vetting Process, described in lines 468-470, is overly simplistic. According to the flow chart diagram, the rejection of the App Deploy leads back to the App Acceptance process. This could be misleading and possibly lead to a higher acceptance of risks and misapplication of software code, because the issues and challenges that are raised in the App Vetting process may not be considered by the designers and users.

Accordingly, we propose that the input from users and designers be considered a required step in the re-application or re-configuration of the App, once it is rejected. The App Vetting Process, as well as the App Development process that appears in line 496, describes a "water fall" development process. However, it fails to describe a more commonly utilized, and a more effective method of "agile development," whereby the entire development team, including users, are creating inputs and expectations at any stage of the development process.

Appendix A: Threats to Mobile Applications

Appendix A is referred to without any qualification and appears to describe a currently known and comprehensive list of threats to information technologies, with a focus on the nature of the threat to mobile computing in particular.

In our view, the ED should refrain from including Appendix A without any discussion of its appropriateness and usefulness as a guide and not as a definitive tool. For example, in 1996 when HIPAA was created, virus attacks were the main class of threats that were known. The authors of that law responded by requiring anti-virus software to be present. By contrast, ransomware was not present until several years ago, and HIPAA thus failed to consider or even apply regulations to this class of threats, except to include it in the generic "risk based" response. Similarly, although this ED lists a robust set of threats that are currently known, the absence of qualifying language that other threats may exist could lead CPAs and others to conclude that if the threat is not reflected in Appendix A, then the ED does not fully apply to a new, yet to be discovered class of threat.

We recommend that language be introduced into the ED that suggests that Appendix A is an illustrative list, and emphasize that future, yet to be known classes of threats could manifest that would require unique and possibly different responses than exist for all other currently known threats.

Network Infrastructure

Underlying network terminology and the use of networks is peppered throughout the ED. However, there is no comprehensive discussion of underlying network infrastructure (NI) which is germane to the understanding and security of mobile Apps. For example, the ED states,

starting in line 525 that "…a score that estimates the likelihood that a detected vulnerability or behavior will be exploited and the impact the detected vulnerability may have on the app or its related device or *network*." (emphasis added) without discussion of NI.

Throughout the ED, the concept of a network is referred to. For example, virtual private network is mentioned in line 751, wireless networks are mentioned in line 212, and the "device's network" is referred to in line 666. Though unrelated to infrastructure and more term of art, "enterprise network" is mentioned in line 732 and voice over IP is referred to in line 1032.

Accordingly, we make note that neither the text of the ED nor the related appendices include discussion of this prevailing infrastructure and its modality.

We suggest that a thorough description of NI is appropriate in this ED. For example, a network can be, as the ED points out, a "Wi-Fi" network. But other networks could pose a greater or lower level of reliability and security such as a mesh network (sometimes known as "Meshnet"), high-frequency radio network (also known as "Ham Radio"), or satellite or ground-based repeaters. Further, Ham Radio networks cannot by law (FCC, Part 97) encrypt its communications, and depending on the frequency range of Meshnet, Wi-Fi, or WiMax, such encryption could also be prohibited, or allowed. All those networks are relevant to the level of security of the NI. It would be helpful then for the users of the ED to be able to have a full discussion of NI, along with the features and threats unique to that type of infrastructure.