ProteqsIT LLC
200 Vintage Circle, Suite 104, Naples FL, 34119
Tel 239-841-7585
info@ProteqsIT.com
WWW.ProteqsIT.com

PROTEQSIT

AUGUST 16, 2021

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

We would like to thank the National Institute of Standards and Technology (NIST) for the opportunity to file these comments in response to the "**Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers** ". President Biden's Executive Order 14028, targets improving the security of federal agencies, is ambitious, far reaching, and necessary. The objectives have been needed for many years with some becoming evident within the recent past. I as principal researcher at ProteqsIT remain committed to research and discovery of novel solutions to intractable problems such as cybersecurity using present-day leading-edge technologies. We look forward to working with NIST and other agencies toward a more secure future and would be happy as an expert in identity and access controls to speak to any of the topics outlined below:

We respectfully submit the attached paper on ProteqsIT LLC's initial position, and requests for clarity around the areas addressed.

Warm regards,

Richard Hallock

Principal researcher and owner

ProteqsIT response to call for papers on:

Cybersecurity Labeling for Consumers

Like the "UL" label infers having met certain objectives and goals, EO labeling should be no less informative. As such, it should indicate compliance with security measures and requirements as are published in response to this EO. It is on this basis I provide the following informative narrative:

Executive Order 14028 pertaining to cybersecurity is far reaching and all inclusive. Section 4 (a) presents objectives of "*Enhancing Software Supply Chain Security*". One objective in section pertains to software product security and reads "[t]he security and integrity of "critical software"—software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)—is a particular concern". Trust is the operative word, and that trust begins at the point of human access, the access point where a cyber incident results when an attacker breaches that trust. In addition, the EO speaks to user facing "product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices". These objectives especially apply to point of access security and consumer trust.

Trust is not a given; it must be earned for every access request. Affirmation of identity is imperative as anything less risks admitting a bad actor. Credentials alone provide no such affirmation of identity even when accompanied by demonstration of "intent".

In the alternative a registered and bound device with gesture-based demonstration of intent enabled by an identity affirmed subscriber delivers "trust" equaling that anticipated by the EO. Such a device when not in the subject's hands blocks availability and use of the gesture-based facility and underlying authenticator protocols.

A practical proof-of-concept mobile phone app demonstrating affirmation of identity as outlined is documented at ProteqsIT.COM website. By demonstrating four operational authenticators (OTP, FIDO, U2F, and Push) are accessible only by the original user of the POC app we establish applicant registration and subscriber authentication with assurance the subscriber is who they claim to be. Original user identity recognition by use of biometrics from their behavioral human traits allow for identity recognition and affirmation. This recognition of identity as a prerequisite gate to each authenticator prevents attacker impersonation of original user. Implemented by use of real-time neural networks eliminates need for biometric data storage thus blocking usable data acquisition by phishing or harvesting attack

Trust goals met by demonstrating a high confidence that the claimant in control of the authenticator is who they claim to be. We respectively suggest Cybersecurity Labeling for Consumers should confer this level of assurance at minimum so far as IoT devices and software development access security and trust are concerned.

ProteqsIT response to call for papers on:

Cybersecurity Labeling for Consumers

Labeling proposed in **Executive Order 14028** should reflect having met well documented goals and objectives. In support of such labeling, certifications carried out by an NGO should establish labeling software products and apps are authorized to display, if any. Participation should be optional but encouraged and perhaps incentivized by publication in a new register assembled, maintained, and published by government agency. Specific considerations include:

- Issue guidelines for instituting security practices and procedures by software development and deployment teams.
- Certification of said practices and procedures by independent NGO.
- Software labeling to indicate achieving certification goals, possibly at differing levels.
- Certification of authenticator adoption of practices and procedures as outlined in NIST Special Program 800-63-3 for standalone authenticator devices, mobile authenticator apps, and IoT device with self-contained authenticators,
- Certification of said practices and procedures by independent NGO,
- Labeling reflecting certification level probably in line with IAL and AAL recommendations, and
- Possibly a recertification regime as a result of labeling that is static while sophistication of cyberattacks are not.
- A review of certification processes employed by UL and PCI/DSS might provide additional guidance.