October 18, 2021

National Institute of Standards and Technology
By email to: labeling-eo@nist.gov

Re: DRAFT Baseline Security Criteria for Consumer IoT Devices

Thank you for the opportunity to provide feedback on the National Institute of Standards and Technology draft baseline security criteria for consumer Internet of Things ("IoT") devices. The draft is thorough and provides an excellent standard from which to evaluate security criteria. To further strengthen the document, we recommend more clearly specifying the following elements:

- **Period for which an IoT device will receive functionality and security updates and support.** While page 5 states "Expected lifespan, anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and term of support" as an element of internal documentation, the security criteria should be clarified to state that information about the duration of support for security updates must be transparent and available to the consumer prior to purchase. Indeed, minimum length of support should be a prime candidate for inclusion on an IoT security label, as that would likely be one of the most important factors for a consumer to consider when purchasing an IoT device.
- **Multi-factor authentication.** Certain language on page 9 could be interpreted as specifying multi-factor authentication ("MFA") (e.g., "The ability to participate in a secure authentication mechanism with other product components (e.g., help gather authenticators, assert authorization based on authentication)" and/or "The ability to verify and authenticate an update on behalf of another product component") but the standard could more clearly state that the use of MFA may be a criterion for assessment.
- **Automatic security updates**. The standard should specify that in many cases security updates should happen by default without requiring users to take action (and such automatic updates should not be paired with functionality updates that a user may not wish to install).
- **Password strength.** The standard should specify password complexity as a criterion for evaluation.

- **Resistant to brute force authentication attempts.** The standard should identify rate limiting and other tactics to limit the effectiveness of brute force attacks as relevant criteria.
- **Fails dumb and/or gracefully.** The standard should state that products should retain functionality unrelated to connectivity or smart features if those are compromised or no longer supported. If however the fundamental operation of the device is compromised by a security incident, the device should shut down rather than allow use in an unsafe fashion.
- **Openness to third-party testing.** The standard should encourage the use of bug bounty programs and discourage legal threats to security researchers who responsibly report vulnerabilities.
- **User notifications.** The standard should specify that users should be notified out-of-band when an IoT device's configuration or security settings are changed.
- **Internal access controls.** The standard should specify that companies should have proper policies to ensure user data is not accessible from employees who do not need access to that data.
- **Support for associated mobile and desktop applications.** The standard should specify that companies have an obligation to consider the security of any applications available to control, access, or otherwise interface with the IoT device.

Sincerely,

Maria Rerecich
Senior Director, Head of Product Testing

J. Glen Rockford
Program Manager, Product Testing - Privacy

Cody Feng
Senior Test Project Leader - Digital Lab Testing

Justin Brookman
Director, Technology Policy