White House Strategic Discussion on
Internet of Things (IoT) Security Labeling

Strawman Concept for Discussion

By providing consumers with the ability to compare and contrast IoT products based on their cybersecurity protections, labeling programs have the potential to dramatically raise the bar for security across the entire IoT ecosystem. There are key elements that must be incorporated into any security labeling program, including one focused on consumer IoT products. These include, but are not limited to:

(1) A mark/label
(2) Conformity requirements
(3) Determination & attestation criteria
(4) A registry of certified products
(5) Encouragement & enforcement of adoption

In order to stimulate a fruitful conversation, and solicit participant feedback, the White House proposes an initial approach to address these elements:

(1) **Mark/label:** The U.S. Government will develop a single, national IoT security mark that may be applied to products meeting the established criteria for that particular class of product. While use of this mark does not preclude the use of other complementary marks – including those sponsored by a foreign government or industry consortium – a single U.S. national mark will aid consumer recognition and foreign government acceptance. The U.S. Government intends to issue and/or license the mark to one or more capable third parties to administer. The mark should be dynamic and updatable, providing manufacturers with the ability to update information about their products and consumers the ability to access the latest technical information available (such as through a QR Code). The U.S. Government will engage foreign governments to harmonize requirements and encourage reciprocal acceptance.

(2) **Conformity Requirements:** National Institute of Standards and Technology (NIST) Internal Report 8425 (*Profile of the IoT Core Baseline for Consumer IoT Products)* will serve as the foundation of a U.S. Government-endorsed IoT security labeling program. NIST will prioritize categories of high-risk consumer products for immediate attention, with initial consideration to (1) microprocessor-based endpoints (e.g., smart TVs, security cameras) and (2) network devices (e.g., consumer-grade routers). Thereafter, NIST will lead an effort to develop and tailor baseline criteria for the identified product categories.

(3) **Determination & Attestation:** A U.S. Government IoT security labeling program will be voluntary, but for those manufacturers seeking to label a product, the processes must engender trust and confidence in the product meeting conformity requirements. This would typically involve a combination of self-attestation, laboratory testing, inspections, and audits. Rigorous certification schemes with accredited laboratories will help ensure that product security is held to the highest possible standards.

(4) **Registry:** IoT products contain hardware and software components that may be secure now, but may become insecure if not properly patched and maintained. A product reaching its end of

service life must also be carefully considered. Consumers need a way to assess how and when their devices may become insecure, and clear mechanisms to update or replace those products at the appropriate time. A register of certified products should be maintained and updated continuously, ideally in a way that enables automated discovery (when authorized) and interoperability across reputable labeling programs. Given the number of existing and proposed platforms being developed by industry, the U.S. Government will aim to leverage these platforms to allow for maximum interoperability and usability.

(5) **Encouragement & Enforcement**: The U.S. Government will modify acquisition policy, consistent with the IoT Cybersecurity Improvement Act of 2020, to ensure Federal departments and agencies only procure those consumer IoT products with U.S. Government-endorsed labels. Where possible, the U.S. Government will incorporate similar requirements into Federal grant programs. The Biden-Harris Administration will ask the Federal Trade Commission (FTC), Federal Communication Commission (FCC), Consumer Product Safety Commission (CPSC), and other relevant regulatory agencies to consider how they may use their respective enforcement authorities to deter false product security claims or misappropriation of the U.S. Government mark. In coordination with such regulators, the Biden-Harris Administration will approach Congress regarding any identified gaps in authorities.

The White House Strategic Discussion on Internet of Things (IoT) Security Labeling aims to galvanize industry momentum on IoT security labeling. But there is still much work to be done. Manufacturers will need to begin to adopt these criteria into their products. Retailers will need to showcase to consumers those products that have met these criteria. And governments, regulators, and assessment bodies will all need to work collaboratively to avoid fragmentating the global marketplace, ensuring that security regimes and labels are widely recognized and accepted across borders.

Towards those ends, the White House is particularly interested in hearing stakeholder feedback on the following questions:

1. How can the U.S. Government harness existing and emerging industry efforts to advance the development of a national labeling initiative?
2. What is needed to ensure that manufacturers are able, and eager, to demonstrate baseline, as well as more advanced, cybersecurity protections?
3. How can all stakeholders work together to harmonize conformity requirements and ensure registry interoperability?
4. What steps are needed to raise awareness among consumers and retailers about the benefits of labeled products?

###