# Comments to NIST Regarding IoT Security Criteria & Labeling

DEVICE SECURITY LEVEL AGREEMENT

This paper, from the Device Security Level Agreement (DSLA) program provides feedback and suggestions in response to the NIST request for input regarding "Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software."

The following points are respectfully submitted to NIST and the community for further consideration in the ongoing development and guidance of IoT security criteria and labeling initiatives:

1. A security controls model should not be confined to IoT classed devices but should be broadly designed and implemented to support most embedded systems used in the IoT, ICS, and general IT industries, network-appliance type devices for example. While consumer IoT is a security concern, it could be said to be the least of concern relative to the broader range of devices insecurely operating in various industries and businesses.

2. A security controls model should be able to accommodate all levels of "device" complexity; with security controls being relative to technology existence in the device.

3. The security controls model should be multitiered. But not have minimal levels for ease of understanding. An ideal system seems to be 3 or 4-tiered at most. To do the job properly, there is no escaping the value of a tiered level or class model.

4. Security controls should be crafted to be broadly applicable to any industry class and usage based upon a technology threat and system criticality rating system. Such a system would then place a given device into a required security controls class.

5. The problem is too complex to be adequately addressed by self-attestation as the sole or entry level of a model. Self-attestation promotes and perpetuates an inferior "lowest-bar" model. For the most part, having proper security levels is not an operational or functional requirement immediately impacting potential sales of the manufacturer. Conversely, building-in and testing security is not an insignificant time and cost endeavor for the device manufacturer. This will always promote an approach of least effort, and "launch first, secure later – and if required" by device makers in industry. Technology security is not a new thing. And there is a problem in industry with proper levels of security being implemented for a reason. For sure, adequate resources also do not exist with device manufacturers to properly determine security in their technologies and implementations. Unfortunately, without an adequate incentive mechanism – mainly in the form of a substantial penalty – the device manufacturers will not adequately and honestly comply with a self-attestation model. Additionally, a post-problem detection penalty is not a model that supports adequate security being established in the market for end-users. Self-attestation is a paper tiger that will not meet intent and will do more harm than good.

6. The security controls model should be verified by a framework of third-party labs specialized in embedded systems security testing. While the field of embedded security is a specialized area of security, there are many qualified security testing companies available to perform needed conformance testing and audit work. The problem is in requiring and starting a process for device manufacturers to follow. The needed capabilities in industry will adjust and balance as necessary.

7. Covering only a small subset of security controls, such as passwords and updates is a wasted effort for all involved. The potential threat surface on varying types of devices, and thus the problem scope, is too large. This is also not just a consumer electronics problem; and arguably, consumer electronics is the least of the worry in terms of consequences. Any security controls model should cover the complete technology surface of the device and device solution-set, and service a broad range of security control categories – for example:
    - Access Controls
    - Communications Security
    - Configuration Security
    - Connected Services
    - Credentials Security
    - Data Privacy
    - Data Security
    - Firmware Security
    - Hardware Security
    - Software Security
    - Security Updates
    - Trusted Computing
    - Vulnerability Testing

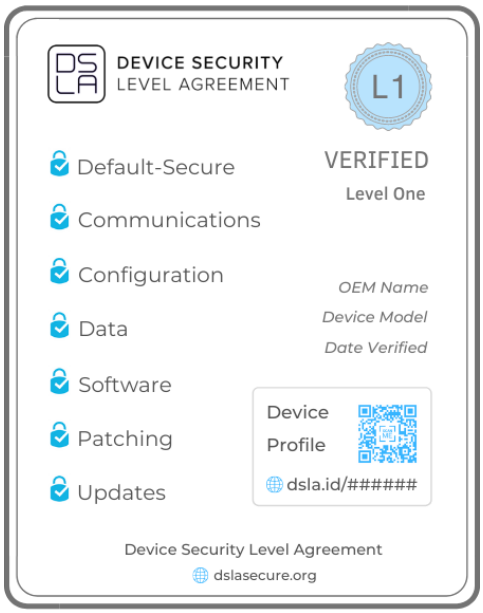
8. Validation of a device's security posture cannot be a one-and-done event. Some degree of device retesting or vulnerability monitoring should be part of the model to confirm ongoing attention to security and conformance to a security controls model by the manufacturer. Device manufacturers often have multiple software release cycles in a year. Additionally, almost all manufacturers incorporate open-source software. New vulnerabilities are discovered and issued daily to monthly for commercial and open-source software, which then necessitate patching by the developer and downstream updating to the end-user. The primary hurdle for device manufacturers is identifying there is a problem to be addressed. The primary hurdle for industry and end-user is ensuring timely patching and downstream updating to the device occurs.

9. A device security label could be seen as being more important for informing the purchasing decisions of businesses in industry than the consumer – though a label would also be useful to the consumer for informing conformance to a security standard as well. And both would rely on an element of awareness and education, or at least inference, as to what the label is and how it works. Having "security" or "trust" related terminology would assist any label effort with initial understanding of focus and intent. Today, labels on devices have a myriad of various certification marks on them that provide no relevance to the end user whatsoever.

10. The security controls model should correspond with a security labeling model. The intent of the label should be to both immediately inform about a security level or class the device conforms too, as well as give direction for greater details on the security conformance provided by the device and manufacturer. For a label to be a useful in an immediate sense upon viewing it, beyond merely leading to more information, the label must identify some aspect of ranking or class. Grading and medal schemes (gold, silver, etc.) are viewed as limiting because of their association with quality being further inferred for the item overall. Stars are too simplistic and vague.

11. The labeling model should accommodate both digital and printed labels optimized for use on device casing and packaging, as well web, and other marketing collateral.

12. Any device security label should support being multiformat. A basic form should exist that could accommodate small print areas, while still informing of security class/level, and an URL in some form for further contextual information and current compliance status. A larger label would accommodate larger display areas and provide more, key contextual information. Both labels should give direction to more detailed digital information displayed from the internet so they could work together and standalone. The larger secondary label should only try to communicate a minimum of security related details given the non-security-oriented audience needing to use it. The primary objective is to show conformance to an established program criteria and communicate secondary profile location for checking conformance status and details. The DSLA dual label mockups for this approach are shown below:


## About DSLA

The Device Security Level Agreement, or DSLA, is an open-security-initiative creating a new approach for how device security is established and communicated. DSLA is a comprehensive, security best-practices-driven framework built in and for the security industry – in support of device manufacturers. In its ongoing, quiet evolution, DSLA has been used to validate security (not attestation) of well over 100 devices (basic to robust) from many major device OEMs. DSLA is focused on IoT/M2M embedded system devices and modules but is designed to support almost any standalone computing system. The DSLA security validation controls establish a minimum-viable security posture for device operation and use; and was created as a comprehensive, multi-tiered model for applying progressive and pragmatic device-security grounded by device-capability and threat context. Further information on DSLA can be found at http://www.dslasecure.org/