Contact: Carol Muehrcke

Organization: ISA Global Cybersecurity Alliance

Response to request for comments on DRAFT Baseline Security Criteria for Consumer IoT Devices, August 31, 2021

(Due October 17, 2021 to labeling-eo@nist.gov, cite "Draft IoT Device Labeling Criteria")

The following comments leverage a study of certification for Industrial Internet of Things components based upon the 62443 industrial automation and control system standards. The study was published in October 2021 by the ISA Global Cybersecurity Alliance and the ISA Security Compliance Institute.

1. **Scope.** The stated scope of the NIST paper is consumer IoT. It is recommended that the paper provide further definition of this scope, or alternatively, broadly characterize IoT devices and products that may be outside of the intended scope. It appears that significant editing and additions to the minimum capabilities described would be needed for industrial sensor and actuator devices, and for overall industrial IoT products such as cloud-based preventative maintenance or process control optimization.

2. **Consumer IoT and other IoT.** Add further insight on scope such as "Many of these minimum security capabilities are expected to be required beyond consumer IoT, such as in the industrial or enterprise IoT space. However, differences from consumer IoT in risk, scale, performance requirements, architectures, management model, and existing regulations/standards will drive distinct security requirements and assurance methods from those appropriate for consumer IoT."

3. **Product view and device view.** It is agreed that review of overall products (vs. devices) may remain the predominant practical approach for labeling of consumer IoT. For industrial or enterprise IoT, the drive for "best in class" is expected to drive the need for component level as well as product level evaluations. Cloud-based functionality will itself be a component subject to evaluation in these spaces.

4. **Example delta capabilities– consumer IoT vs. industrial IoT.** The following are provided as rationale for the above comments, and not proposed as content appropriate for the paper itself. These remarks are offered as examples of differences in capabilities for consumer vs. industrial IoT. They do not comprise a comprehensive evaluation of the paper for the industrial space.

   a) **Table 1 Data protection #1 Confidentiality.** Some data in industrial IoT devices requires confidentiality protection, but not all, as the potential criterion in the paper states. This is particularly the case for data at rest. An example of data at rest for which confidentiality protection may not be required, is short-lived process measurements. Cryptography protection impacts aggressive performance requirements and so is applied selectively in an industrial setting. 62443-4-2 in requirement CR 4.1 requires confidentiality protection for “data at rest for which explicit read authorization is supported.”

b) **Table 1 Data protection #3 Render data inaccessible.** For an individual to lock all others out of access to an industrial component or product would be an unusual action.

c) **Table 1 Cybersecurity state awareness #1 Detection:** The potential criteria discuss logging events, and the capability is about detecting incidents. These are related but different topics. In an industrial setting, some or even all logging and detection might be performed by the industrial IoT product itself. However, industrial asset owners in general require the flexibility to accomplish detection via export of logged events to other specialized software that can integrate and interpret events from many sources (SIEM, Security Information and Event Management). Therefore, export of logs using standard methods is a critical capability in the industrial space (62443-4-2 requirement CR 6.1). The need for this capability is not apparent if it is assumed that the product itself performs detection in all cases.

d) **Table 1 Product security #1 Maintaining operational capabilities.** In the industrial space, maintenance of operational capabilities upon loss of connectivity may or may not be desirable. The focus will be on maintaining capabilities where their loss could impact health, safety or the environment. A related requirement from IEC 62443-3-3 in sub clause 4.2 *Support of essential functions,* states *“*that essential functions … shall be maintained if zone boundary protection goes into fail-close and/or island mode.” The 62443 definition of essential function is “function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control.”

e) **Table 2 Non-technical supporting capabilities.** For the industrial space, the international standard IEC 62443-4-1 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements* defines requirements on secure product development lifecycle for control systems, as criteria for the capabilities listed in the NIST paper Table 2.

5. **Additional consumer IoT capabilities.** The following functional capabilities identified in the ISAGCA/ISCI study for industrial IoT mentioned above may also be appropriate for the consumer space.

a) **Table 1 Software update, security settings.** Update of software should preserve the user’s security settings.

b) **Table 1 Cybersecurity state awareness, monitor presence.** Require the ability to monitor presence/absence of a component from another component.

c) **Table 3 Logical access to interfaces, with external entities.** Require authentication and authorization for all digital entities communicating with the product, not only for communication between components of the product. This is required if there may be digital entities communicating with the product that are not part of the product.