**Arm, Inc.**
**Comments in response to:**
**National Institute of Standards and Technology (NIST)**
**"DRAFT Baseline Security Criteria for Consumer IoT Devices"**

## Background on Arm

On behalf of Arm, please find below Arm's feedback on the "DRAFT Baseline Security Criteria for Consumer IoT Devices".[1]

Arm is the leading global supplier of intellectual property (IP) to the semiconductor sector, licensing processor designs, security IP, system IP, software, and development tools, along with many other technologies that provide the essential foundation for modern computing.[2] Arm's products are licensed by more than 500 companies globally, including approximately 200 US companies. Designing a processor core is a costly and time consuming project; by utilizing Arm's processor designs, semiconductor companies can focus on developing their own IP to differentiate and customize their products, while still being able to leverage the wide range of compilers, code generators, debuggers, software, and other technology designed to run on Arm-based products.[3] Arm's microprocessor designs are found in every form of computing from the most powerful supercomputer in the world[4] to the most resource constrained applications[5], and everywhere in between. In 2020, more than 25B Arm-based chips were manufactured by our partners; that equates to nearly 900 Arm-based chips per second. This gives Arm immense reach into the earliest stages of developing secure products, and as such Arm believes secure computing starts with how we address security in our technologies. Arm puts the utmost importance on developing products with security as a primary focus, and delivering technologies and approaches that make it easier for our customers and others using our technology to develop more secure products. In 2017, Arm put out a call to action to the industry to do more to address security by releasing its first Security Manifesto, also discussing what more Arm itself could do to enhance security; in 2018 and again just this summer Arm released Manifestos that built on that vision and call to action.[6]

## Background on PSA Certified and previous work with NIST on NISTIR 8259A

Arm, together with eight other companies, have a security by design scheme called PSA Certified[7] that is aligned with NISTIR 8259A. It is supported by a large section of the electronics industry including most leading chip vendors. The cybersecurity baseline requirements of

---

[1] NIST, DRAFT Baseline Security Criteria for Consumer IoT Devices ("DRAFT Baseline")
*https://www.nist.gov/system/files/documents/2021/08/31/IoT White Paper - Final 2021-08-31.pdf*
[2] For more about Arm, see *www.arm.com*
[3] See Appendix 1 for Arm technology flow.
[4] See *https://www.top500.org/lists/top500/2021/06/*
[5] See *https://www.eetimes.com/darpa-research-advances-for-near-zero-power-sensors/*
[6] See *https://www.arm.com/resources/manifesto/iot-security*
[7] See *https://www.psacertified.org/*

NISTIR 8259A[8] reference PSA questions as IoT Reference examples and the PSA Certified questionnaire provides a mapping to 8259A.

The PSA Certified questionnaire has approximately 50 requirements and is split into three sections: chip, system software and device.[9] To make it easier and quicker for the OEM to answer the requirements the sections can be used in composition. The requirements originate from the PSA Security Model 10 goals that were established by doing a number of IoT threat models and determining the common aspects, the mapping to NISTIR 8259A and the mapping to the mandatory device parts of EN 303 645.[10]

Arm will soon be launching a web-based version of the PSA Certified Level 1 requirements for device, system software and chip that covers the NISTIR 8259A requirements. Arm believes this online questionnaire could serve as a vehicle for first evaluations and certification for the NIST IoT device labelling requirements. This online questionnaire will help developers by providing more extensive example answers that can be used as a guide and improved usability for those seeking to certify products.

**Comments specific to Questions from DRAFT Baseline Security Criteria for Consumer IoT Devices**

Arm proposes that NIST should initially focus on security by design criteria for the device as this is where a physical label is likely to reside and it reduces the complexity of evaluation. A product security label and/or label components are significantly more complex and could be addressed in a second phase of the labelling effort. As such, Arm's following comments are specifically focused on the device itself.

*NIST seeks comment on all aspects of cybersecurity labelling technical criteria for IoT devices. Specific areas for consideration include:*
*Whether these are appropriate criteria for a broad range of consumer devices*[11]

> The fact that PSA Certified requirements and NISTIR 8259A requirements mapped so well and that the PSA Certified work originates from original analysis of multiple IoT threat models indicates that the criteria are broadly appropriate (but see the next item for a proposed improvement).[12] PSA Certified is also mapped to the minimum device requirements of EN 303 645 (and therefore is additionally aligned to Singapore CLS).

[8] See *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf*
[99] See *https://www.psacertified.org/app/uploads/2021/09/JSADEN001-PSA_Certified_Level_1-2.1-REL2.pdf*
[10] See Appendix 1
[11] DRAFT Baseline, p. 2
[12] See NISTIR 8259A, Table 1, "IoT Reference Examples" column for PSA Certified mapping https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

*Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device*[13]

Arm proposes to add the ability of the device to use a hardware Root of Trust (RoT) to protect the integrity of the system and confidentiality of critical security assets. This criterion is widely used today by OEMs and Cloud Service Providers developing or specifying connected devices. Further, NIST has specifically discussed the importance of utilizing a RoT in its own work, noting "(r)oots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust."[14]

In "*Table 1: IoT Product Cybersecurity Capabilities Developed from NISTIR 8259A Using Informative References"* this could be introduced under "Product Security" with a new Potential Criteria of:

> *The ability of the device to use a demonstrably secure hardware Root of Trust to protect system integrity and confidentiality of secrets (e.g. The Root of Trust provided by a PSA Certified chip or equivalent).*

*Whether Tables 1, 2, and 3 have the right level of detail in the discussion of the criteria to ensure consistency in meeting the cybersecurity expectations*[15]

At launch it might make sense to have a smaller set of basic requirements to encourage OEMs to engage with the process and couple this with a self-declaration and publication level of assurance (This could be referred to as a "1 Star" label).

The baseline requirements set out in the white paper based on 8259A/B represent an extensive set of security by design requirements and could be coupled with independent lab based audit of responses (This could be referred to as a "2 Star" label).

This style of security tiers with increasing requirements and assurance translates to an easy to explain consumer message: "1 Star" represents basic security requirements that are claimed by the manufacturer; "2 Star" represents best practice security by design that has been audited by an indpendent laboratory. An example of a smaller set of requirements with simpler criteria is given in the next response (below).

[13] DRAFT Baseline, p. 2
[14] See *https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust*
[15] DRAFT Baseline, p. 2

*What might be the appropriate definitive text for these criteria be stated to facilitate conformity assessment*[16]

> To pass the "1 Star" Baseline Security Criteria for Consumer IoT Devices developers must provide written responses showing how the following abilities have been met:
>
> 1. Validated software updates for X years
> 2. Encrypted and authenticated communication
> 3. No default passwords
> 4. A vulnerability disclosure website and plan

*The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria*[17]

> Most MCU based systems should be able to meet the requirements of PSA Certified Level 1 and NISTIR 8259A. This is evidenced by the many MCUs that have been certified through the PSA Certified process.[18] A few older MCU chips with very limited resources might struggle to meet all the requirements.

*The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another*[19]

> Whilst a holistic product approach is desirable e.g. device + mobile app + cloud back end, it adds a lot of potential complexity to evaluating products for the labelling scheme. There may be a benefit from a "keep it simple" approach; keeping the initial focus at device level, with a few "organisational best practice" requirements, then extend over time. Keeping the assessments for cloud backend, hub and mobile app independent of device certification makes sense from a point of view that they can be phased in over time and kept compartmentalized from an evaluation point of view.

*…the labeling program must address multiple tiers of security achieved by various products:*
*• The bottom tier (or level) provides a minimum meaningful amount of assurance about the security of an IoT product.*
*• Each subsequent tier should provide additional security, assurance, and/or protection.*[20]

---

[16] DRAFT Baseline, p. 2
[17] DRAFT Baseline, p. 2
[18] See https://www.psacertified.org/certified-products/?_standard=psa-certified-chip-vendor
[19] DRAFT Baseline, p. 2
[20] DRAFT Baseline, p. 10

Arm agrees with the need for a label that demonstrates more robust approaches to security. It is proposed that:

- "1 Star" the first level uses self attestation/declaration of a small number of fundamental security requirements (see above for suggestion),
- "2 Star" uses evaluation lab audit of written answers to the more extensive NISTIR 8259A security by design requirements and
- "3 Star" requires a certified Root of Trust be used as well as meeting the Level 2 requirements.

The Singapore IoT Labelling scheme which was discussed significantly during the NIST Labelling Workshop on 14 and 15 September 2021 achieves this by utilizing "tiers" demonstrating more robust security features and device scrutiny.[21] PSA Certified achieves this as well by offering Levels 1, 2, and 3 Certifications, each with increasing security requirements and scrutiny.

**Conclusion**

Arm appreciates the opportunity to engage with NIST and comment on the proposed approach to developing an IoT labelling scheme. Arm shares the aim of improving IoT security, and consumer awareness about the need to consider security features in the purchasing process. By relying on NIST's significant past work around IoT security, and encouraging use of existing schemes such as PSA Certified to meet labelling criteria, we can collectively accelerate the roll out of a successful security labelling scheme that has value to consumers. Please contact us if we can answer additional questions or provide additional information on any of the comments provided.

Respectfully Submitted,

Rob Coombs
Director, Architecture Technology Group
rob.coombs@arm.com

Rob Smart
Senior Principal Security Architect
rob.smart@arm.com

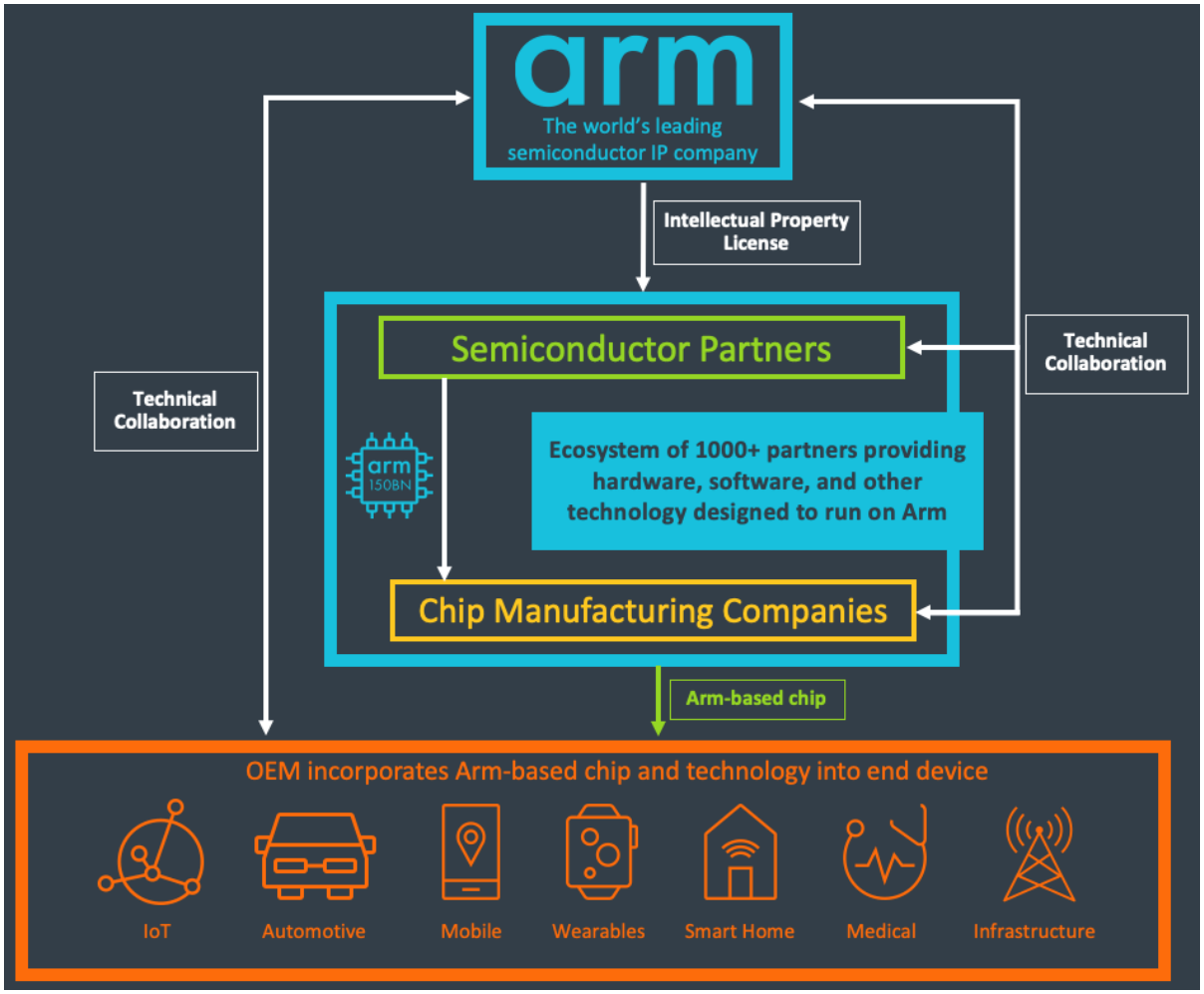
Anurag Gupta
Director, Architecture Technology Group
anurag.gupta@arm.com

Marcus Streets
Principal Engineer, Architecture Technology Group
marcus.streets@arm.com

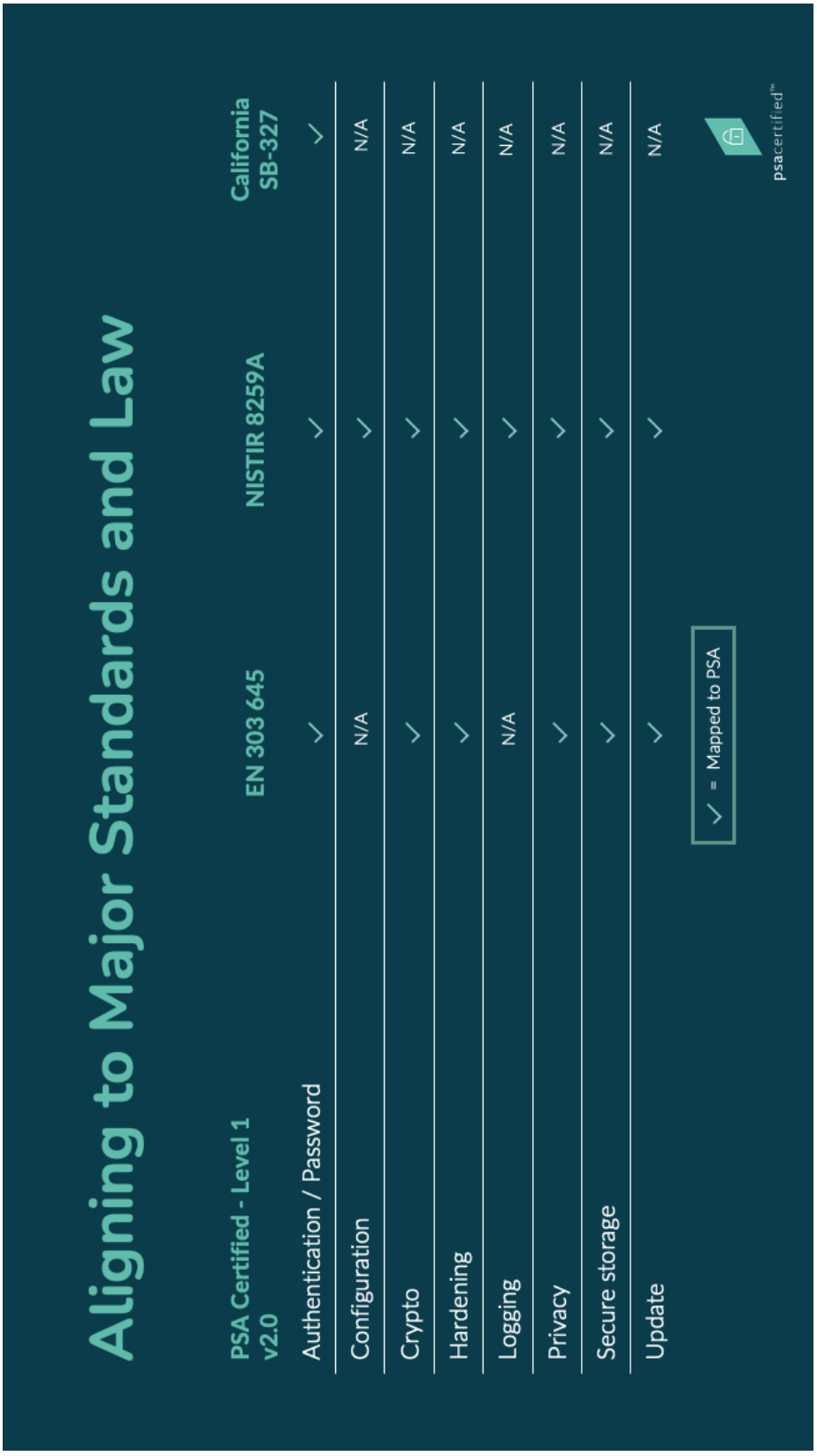
Vince Jesaitis
Senior Director, Government Affairs
vince.jesaitis@arm.com

15 October, 2021

Appendix 1


arm
The world's leading semiconductor IP company
Intellectual Property License
Semiconductor Partners
Technical Collaboration
Technical Collaboration
arm 150BN
Ecosystem of 1000+ partners providing hardware, software, and other technology designed to run on Arm
Chip Manufacturing Companies
Arm-based chip
OEM incorporates Arm-based chip and technology into end device
IoT
Automotive
Mobile
Wearables
Smart Home
Medical
Infrastructure

Appendix 2


Aligning to Major Standards and Law
PSA Certified - Level 1 v2.0
EN 303 645
NISTIR 8259A
California SB-327
Authentication / Password
✓
✓
✓
Configuration
N/A
✓
N/A
Crypto
✓
✓
N/A
Hardening
✓
✓
N/A
Logging
N/A
✓
N/A
Privacy
✓
✓
N/A
Secure storage
✓
✓
N/A
Update
✓
✓
N/A
✓ = Mapped to PSA
psacertified™