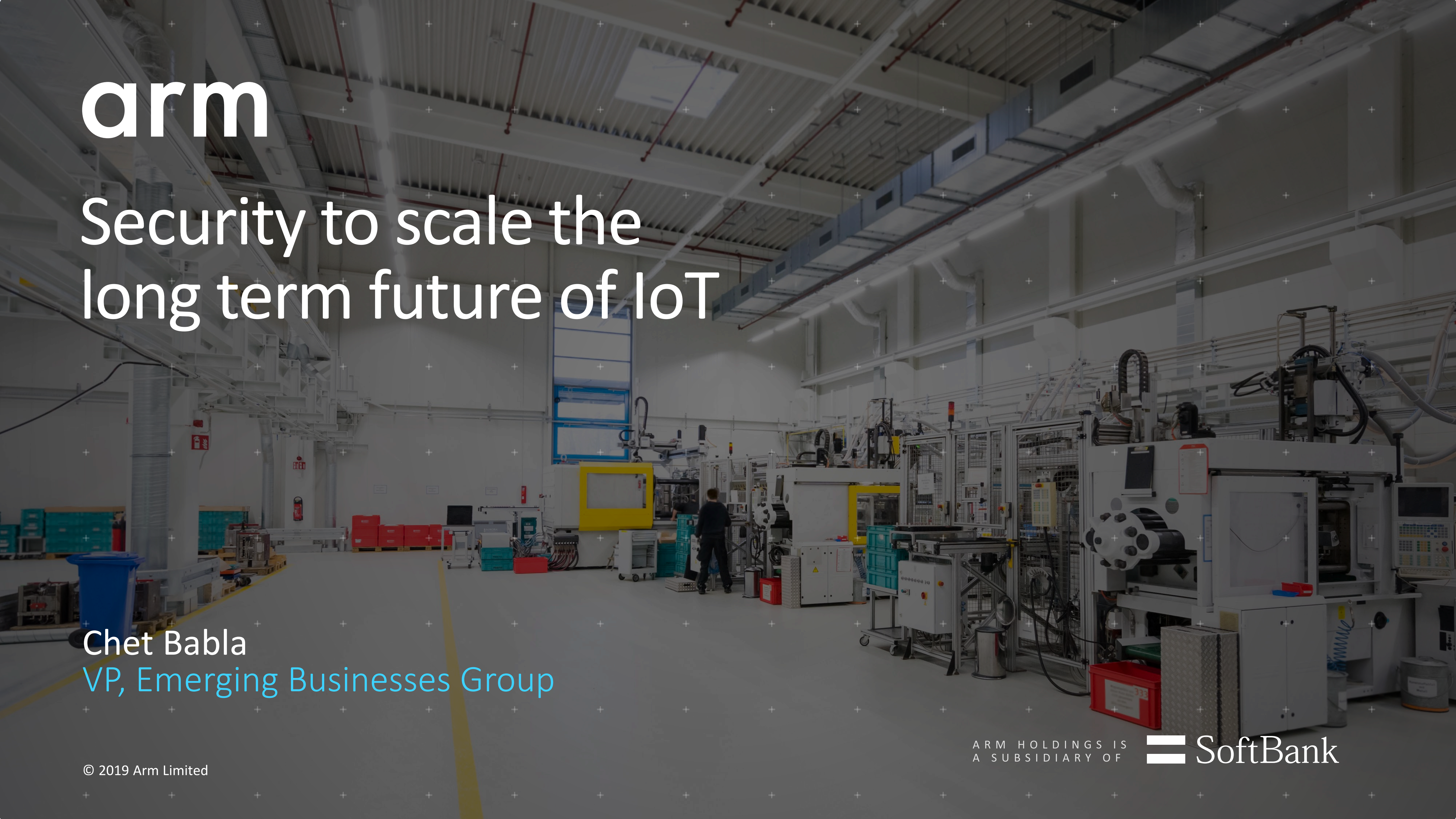


arm

Security to scale the long term future of IoT

Chet Babla
VP, Emerging Businesses Group

ARM HOLDINGS IS A SUBSIDIARY OF SoftBank

Arm - Architects of Global Possibilities

The global leader in the development of licensable semiconductor technology

Focused on freedom and flexibility to innovate

Partnership based culture & shared success business model

70%

Of the world's population use Arm technology

1000+

Arm ecosystem partners

130bn+

Arm-based chips shipped to-date

Previous Waves of Computing

WAVE ONE | MAINFRAME

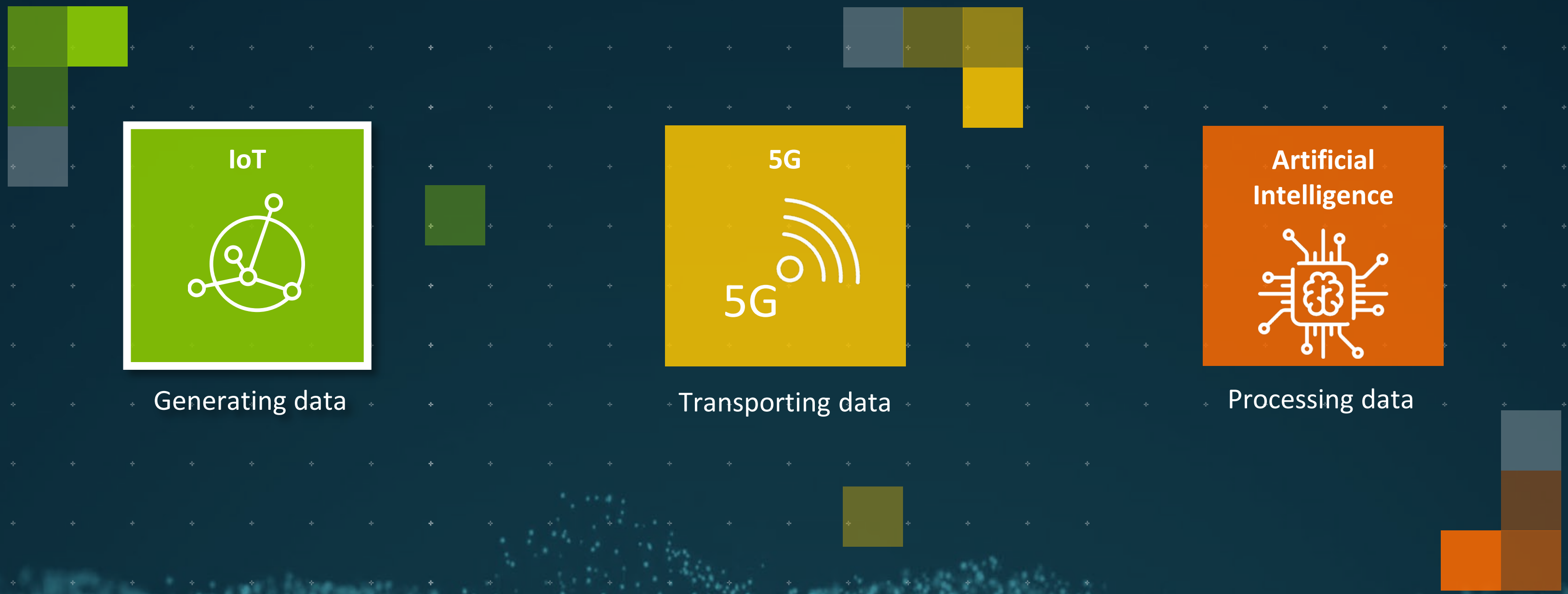
WAVE TWO | PERSONAL COMPUTING & SOFTWARE

WAVE THREE | INTERNET

WAVE FOUR | MOBILE & CLOUD

The Fifth Wave of Computing

The data driven era



IoT

Generating data

5G

Transporting data

Artificial Intelligence

Processing data

1 trillion connected devices opportunity

IoT Delivers Value Through Digital Transformation

Productivity gains – automation, sensor driven insights, smart manufacturing

New business models – from a ‘product sale’ to ‘as a Service’ revenue

Enhanced customer experience – access to real-time data, agile support

USD$11 trillion global economic value by 2025*

*McKinsey Global Institute, 2017

The Complexity of IoT

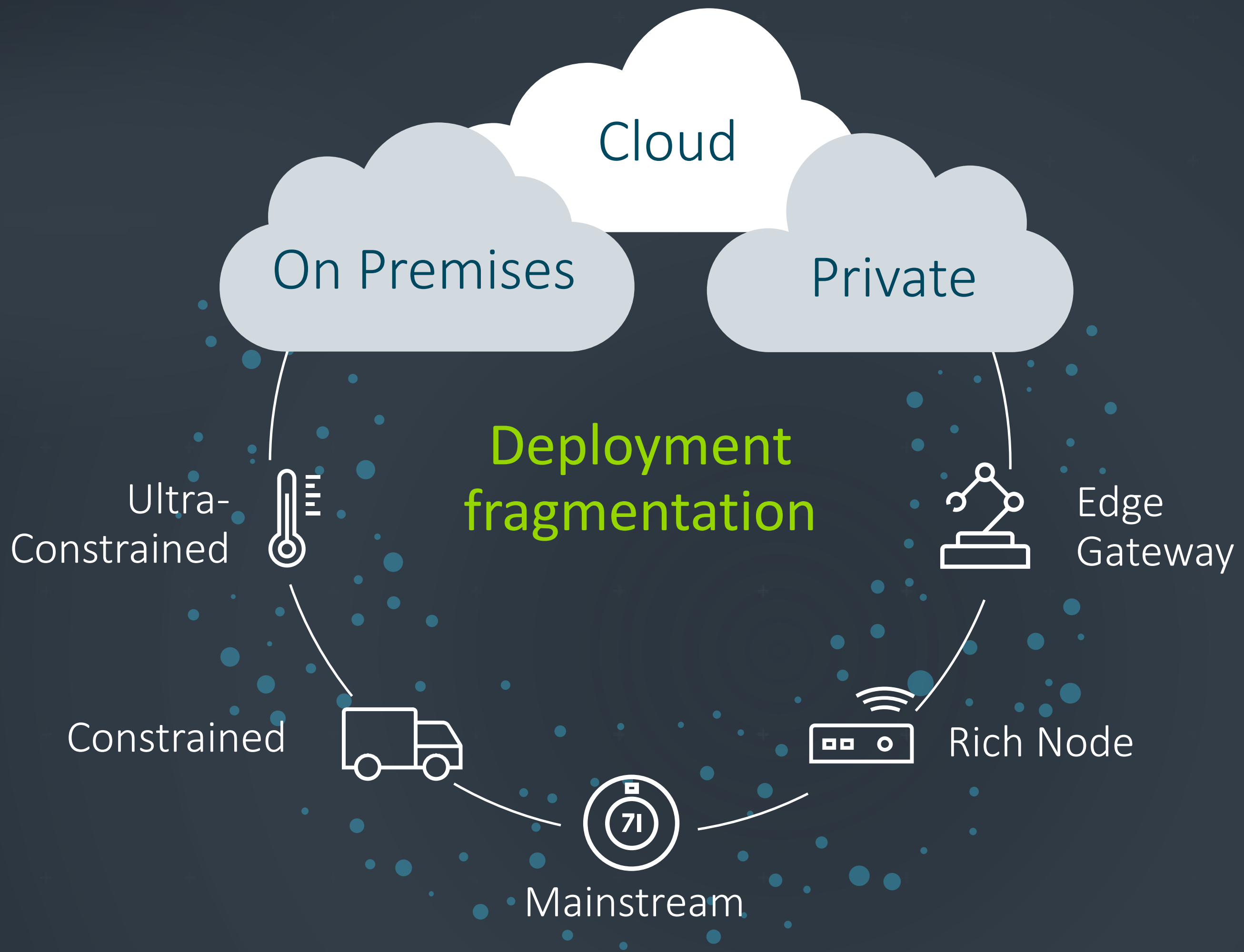
Security is needed end-to-end

Connect

Provision

Manage

Develop devices



Can the data be trusted?

Is my application vulnerable?

Is my business vulnerable?

Security

Making IoT Devices Secure

Security cannot be an afterthought

Analyze
Threat modeling

Architect
Hardware & firmware architect specs

Implement
Firmware source code

Certify
Independently tested

Security threats to be analyzed

Physical attacks

- Non-invasive
- Invasive

Software attacks

- Buffer overflows
- Interrupts
- Malware

Communication attacks

- Man-in-the-middle
- Weak RNG
- Code vulnerabilities

Lifecycle attacks

- Code downgrade
- Ownership changes
- Unauthorized overproduction
- Debug hacks

Fundamental Device Security Goals

Secure Storage

Secure Boot

Isolation of Root of Trust

Secure update process

Validation of updates

Attestation

Unique instance ID

TRNG services

Security lifecycle

Anti-rollback feature

Platform Security Architecture (PSA)

Open security framework & certification scheme

psacertified™

www.psacertified.org

arm PSA

Building trust in devices & data

A PSA Methodology Example – Smart Meter

Process flow

System description

↓

Assets

↓

Threats

↓

Security Objectives

↓

Security Requirements

Outcome

Asset: Metering data integrity & confidentiality

↓

Threat: Remote SW attacks

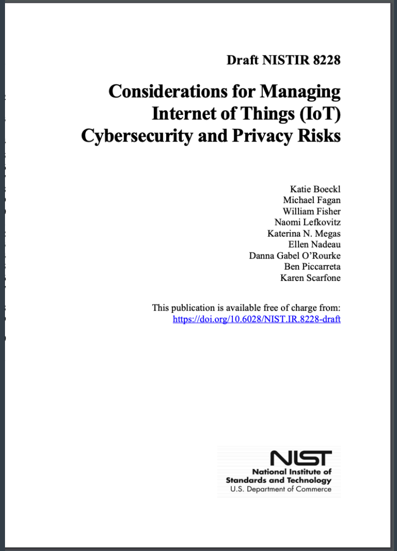
↓

Security Objective: Strong Crypto

↓

Security Requirement: Hardware-based key store

Governments and Industry Organizations are Waking up to the IoT Security Threat



Draft NISTIR 8228

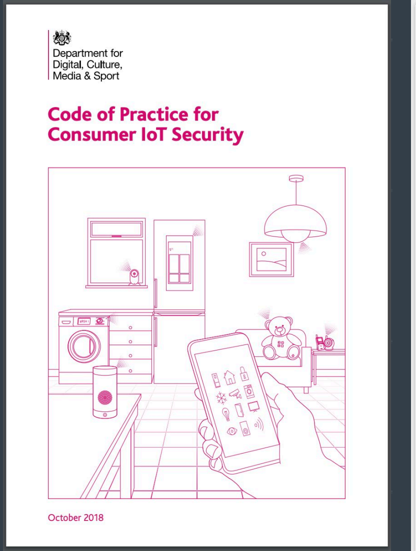
Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228-draft

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

US: NIST

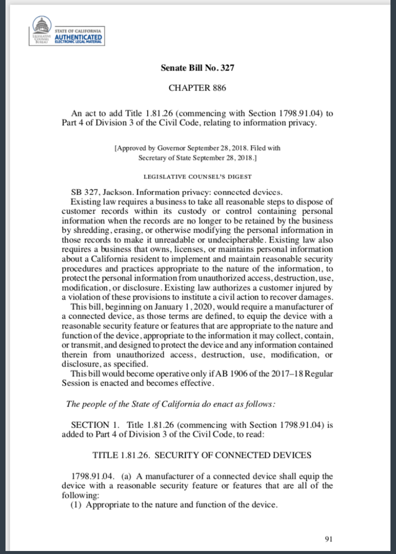


Department for
Digital, Culture,
Media & Sport

Code of Practice for Consumer IoT Security

October 2018

UK: DCMS



STATE OF CALIFORNIA
AUTHENTICATED
ELECTRONIC LEGAL MATERIAL

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with
Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. SECURITY OF CONNECTED DEVICES

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

91

US: California

enisa

Baseline Security Recommendations for IoT

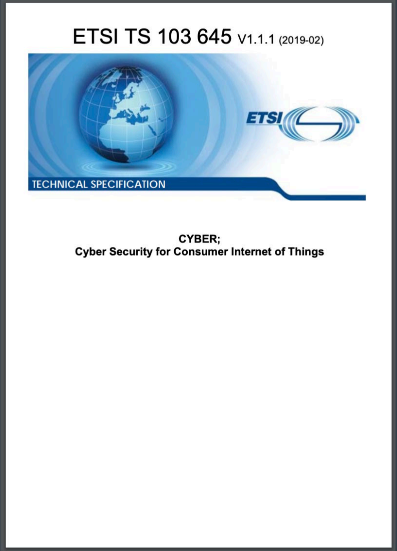
in the context of Critical Information Infrastructures

NOVEMBER 2017

www.enisa.europa.eu

European Union Agency For Network And Information Security

EU: ENISA



ETSI TS 103 645 V1.1.1 (2019-02)

ETSI

TECHNICAL SPECIFICATION

CYBER;
Cyber Security for Consumer Internet of Things

ETSI

GSMA

IoT SECURITY GUIDELINES

Overview Document

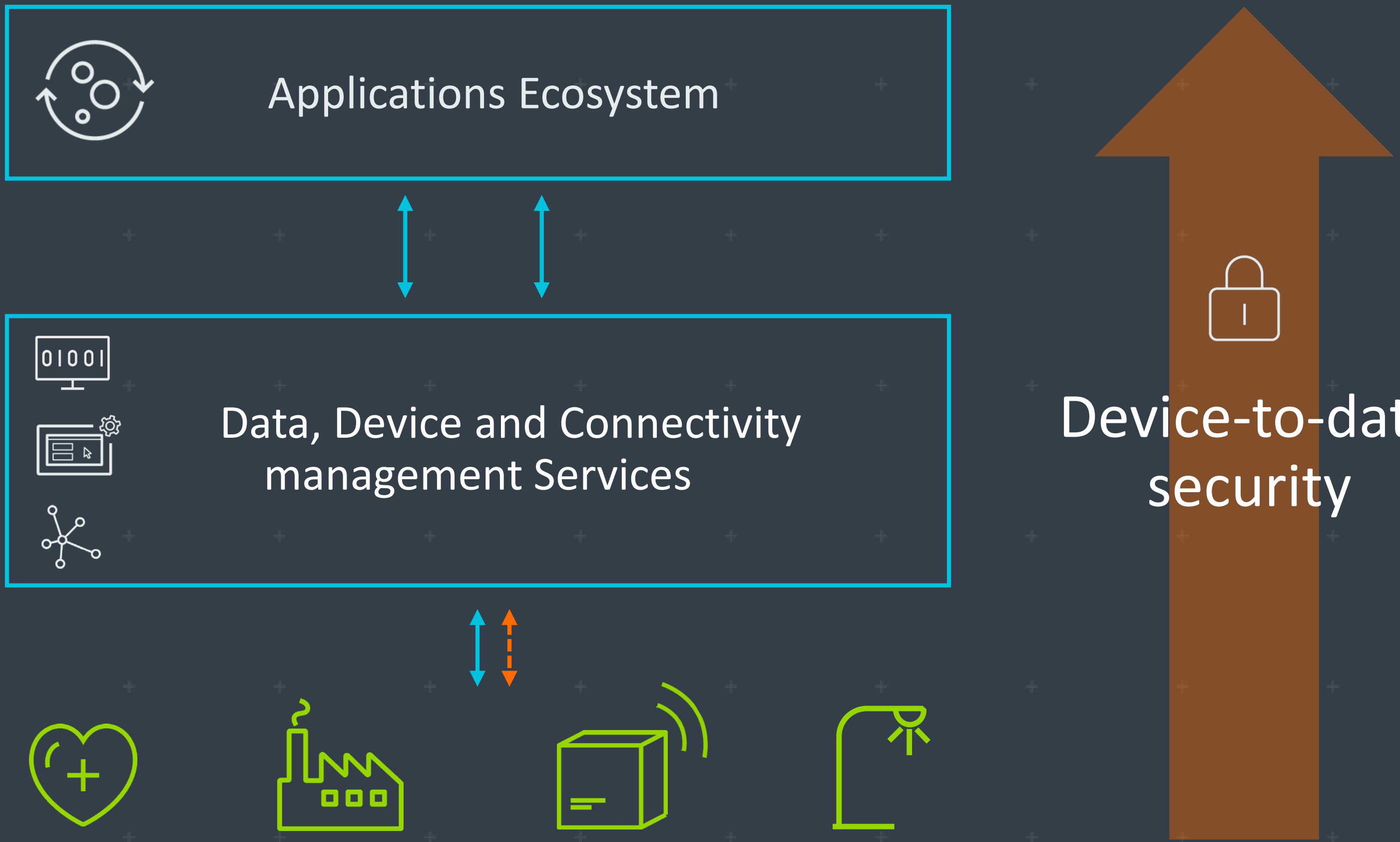
Supported by

GLOBALPLATFORM GSA IoT WORLD ALLIANCE oneM2M simalliance Security | Identity | Mobility

GSMA

IoT Security Must Be End-to-end

Security is only as strong as the weakest link


Applications Ecosystem

Data, Device and Connectivity management Services

Device-to-data security

arm

Thank You

Danke

Merci

谢谢

ありがとう

Gracias

Kiitos

감사합니다

धन्यवाद

شكرًا

תודה