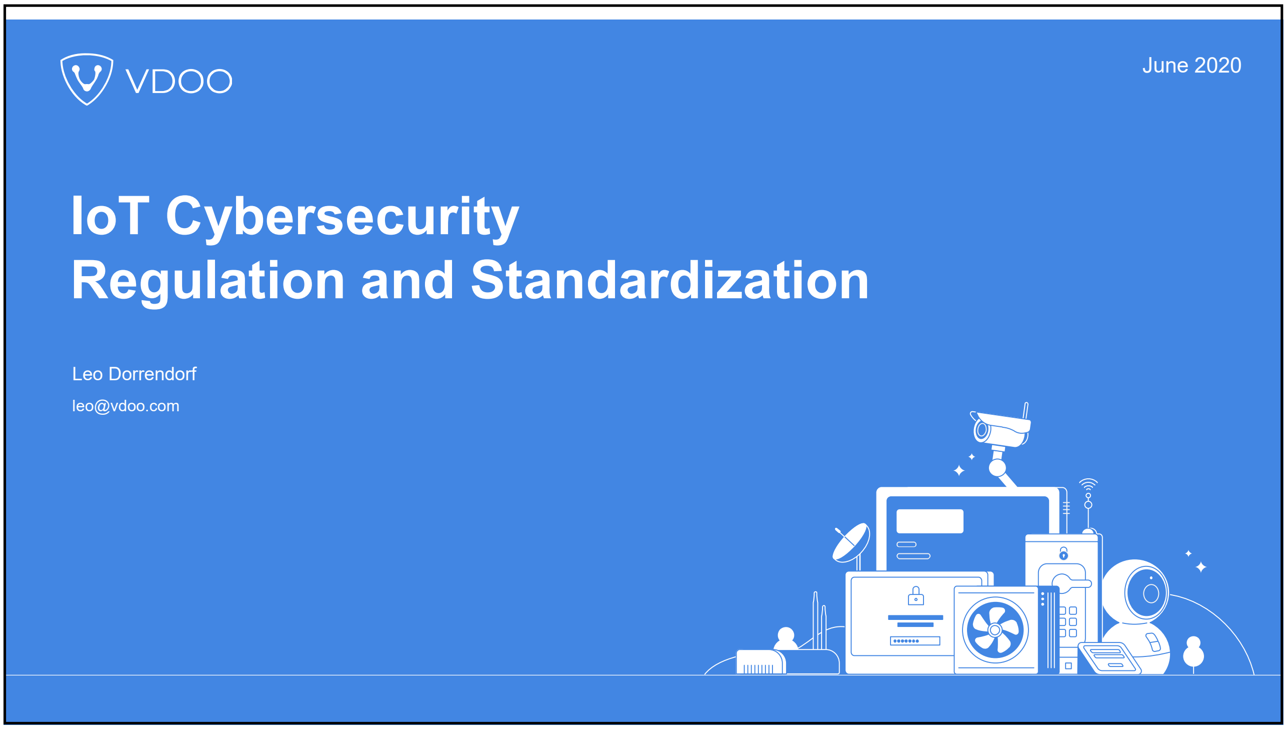
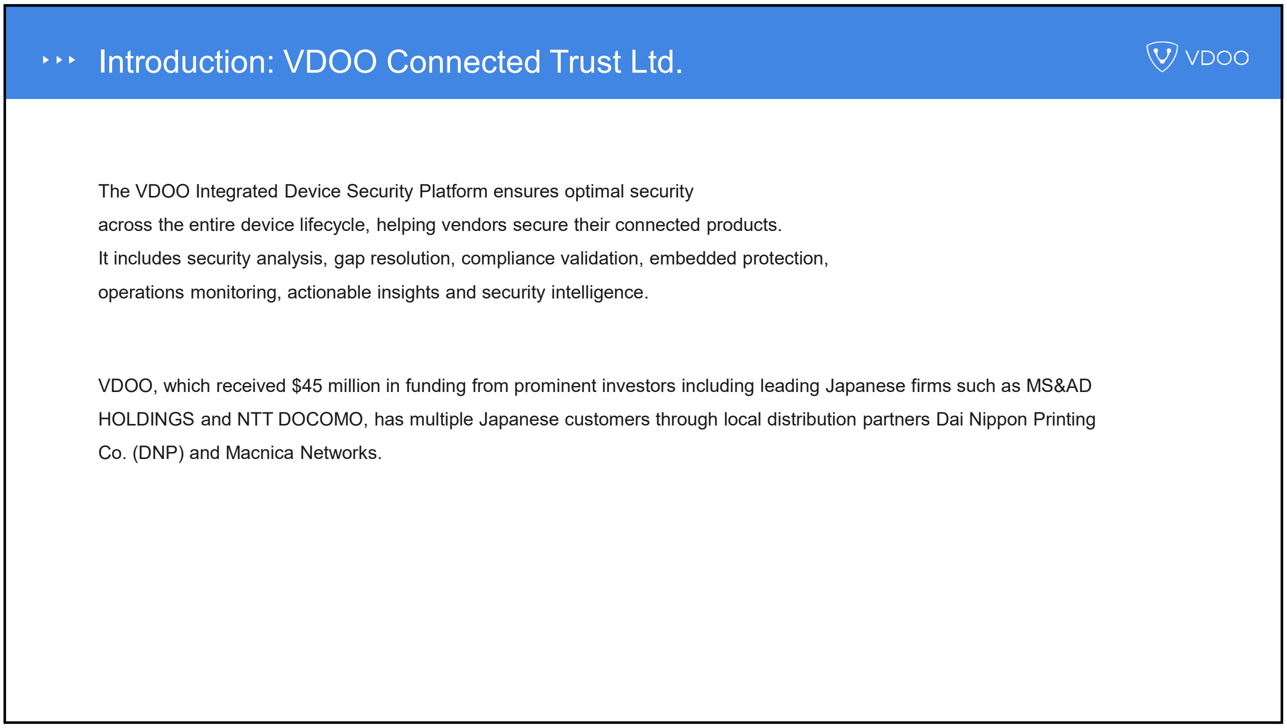


VDOO

June 2020

IoT Cybersecurity Regulation and Standardization

Leo Dorrendorf
leo@vdoo.com

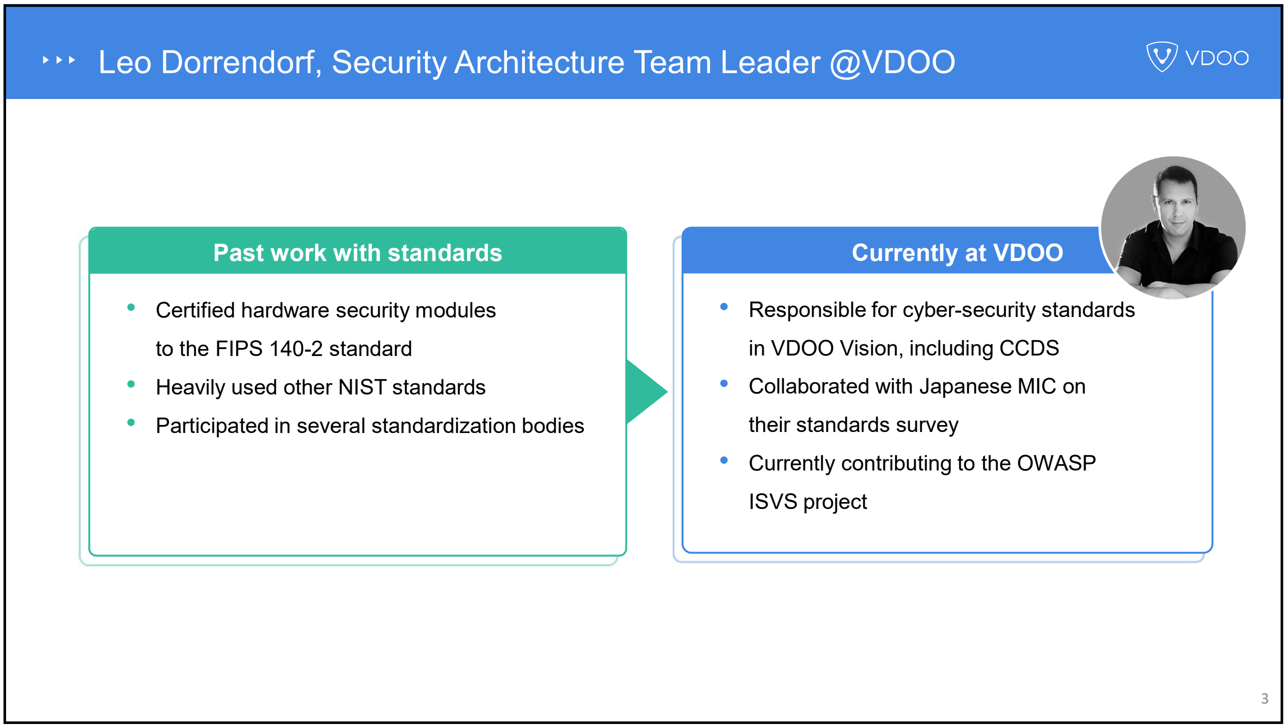


Introduction: VDOO Connected Trust Ltd.

VDOO

The VDOO Integrated Device Security Platform ensures optimal security across the entire device lifecycle, helping vendors secure their connected products. It includes security analysis, gap resolution, compliance validation, embedded protection, operations monitoring, actionable insights and security intelligence.

VDOO, which received $45 million in funding from prominent investors including leading Japanese firms such as MS&AD HOLDINGS and NTT DOCOMO, has multiple Japanese customers through local distribution partners Dai Nippon Printing Co. (DNP) and Macnica Networks.



Leo Dorrendorf, Security Architecture Team Leader @VDOO

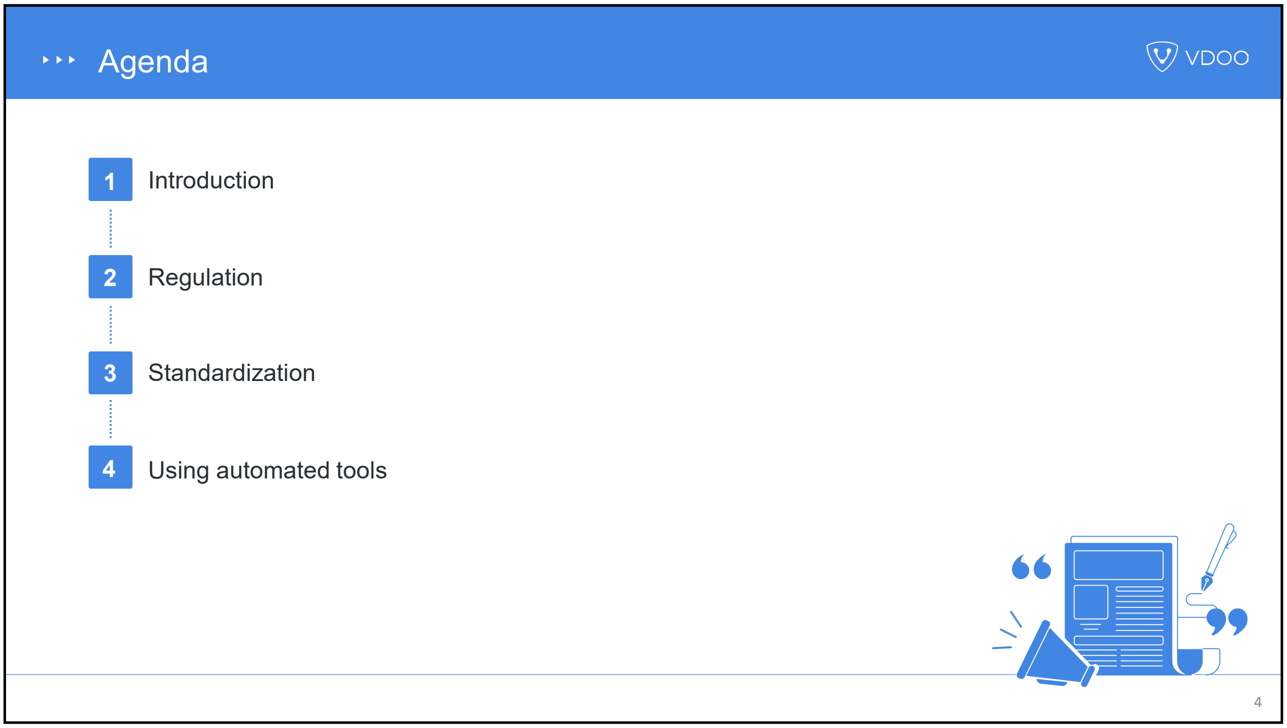
VDOO

Past work with standards

- Certified hardware security modules to the FIPS 140-2 standard
- Heavily used other NIST standards
- Participated in several standardization bodies

Currently at VDOO

- Responsible for cyber-security standards in VDOO Vision, including CCDS
- Collaborated with Japanese MIC on their standards survey
- Currently contributing to the OWASP ISVS project



Agenda

VDOO

1 Introduction

2 Regulation

3 Standardization

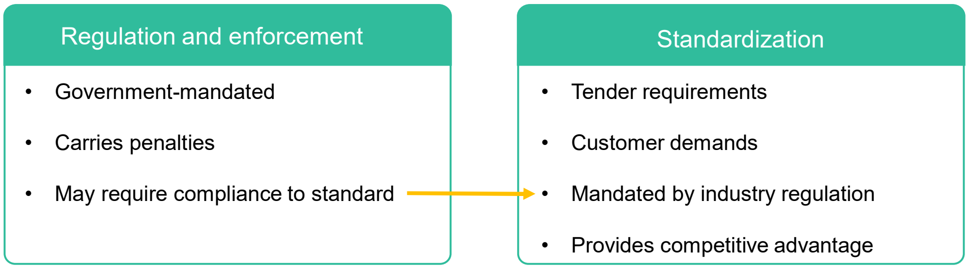
4 Using automated tools

1 ······· 2 ······· 3 ······· 4

Introduction

Motivation: Drivers to compliance

VDOO

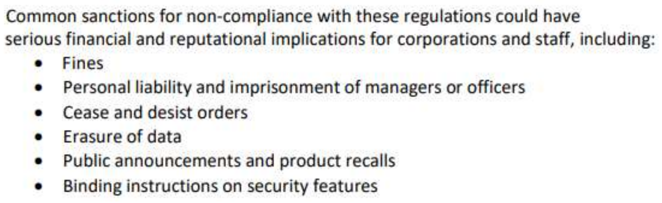


Regulation and enforcement

- Government-mandated
- Carries penalties
- May require compliance to standard

Standardization

- Tender requirements
- Customer demands
- Mandated by industry regulation
- Provides competitive advantage



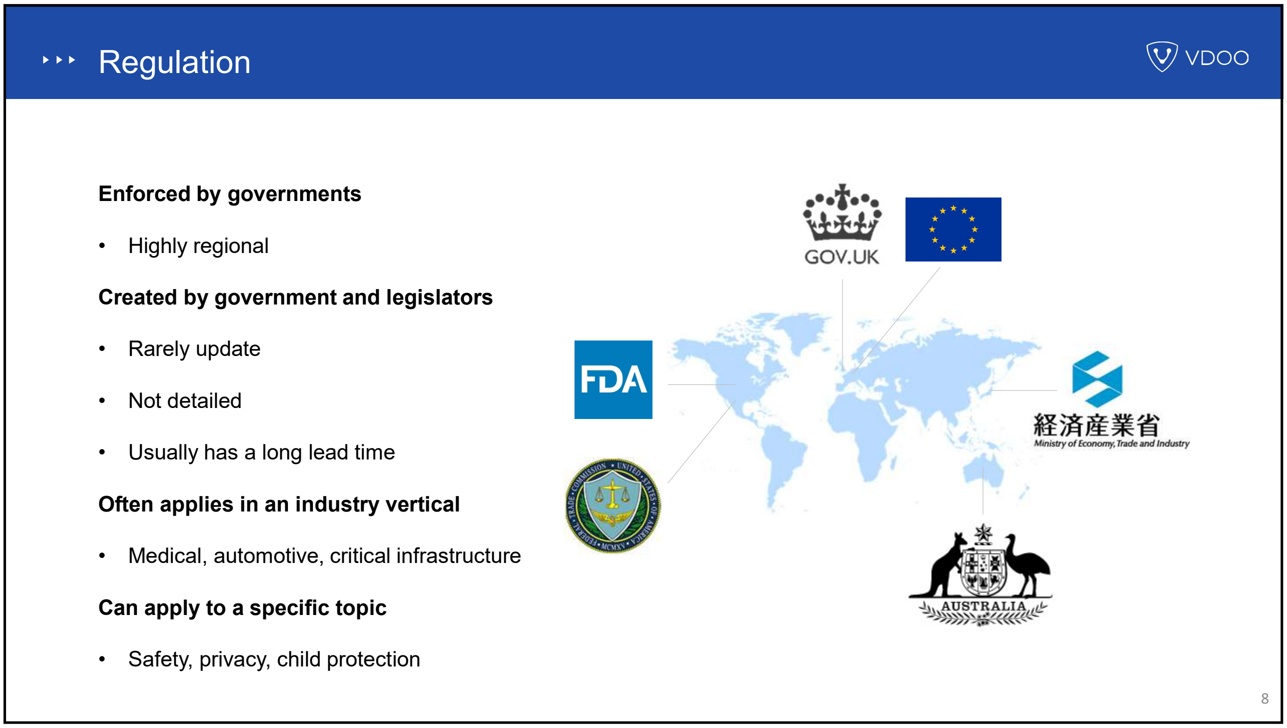
Common sanctions for non-compliance with these regulations could have serious financial and reputational implications for corporations and staff, including:

- Fines
- Personal liability and imprisonment of managers or officers
- Cease and desist orders
- Erasure of data
- Public announcements and product recalls
- Binding instructions on security features

https://www.iotsecurityfoundation.org/best-practice-guidelines/

1 ······· 2 ······· 3 ······· 4 ······· 5 ······· 6

2. Regulation



Regulation

Enforced by governments

- Highly regional

Created by government and legislators

- Rarely update
- Not detailed
- Usually has a long lead time

Often applies in an industry vertical

- Medical, automotive, critical infrastructure

Can apply to a specific topic

- Safety, privacy, child protection

Recommended source

Overview paper from the IoT Security Foundation

BEST PRACTICE USER

IoT Security Foundation

IoT Cybersecurity: Regulation Ready

A Landscape Report – Concise Version

BEST PRACTICE USER

IoT Security Foundation

IoT Cybersecurity: Regulation Ready

A Landscape Report – Full Version

https://www.iotsecurityfoundation.org/best-practice-guidelines/

Example regulation: FDA

FDA regulations only apply if the device intends to:

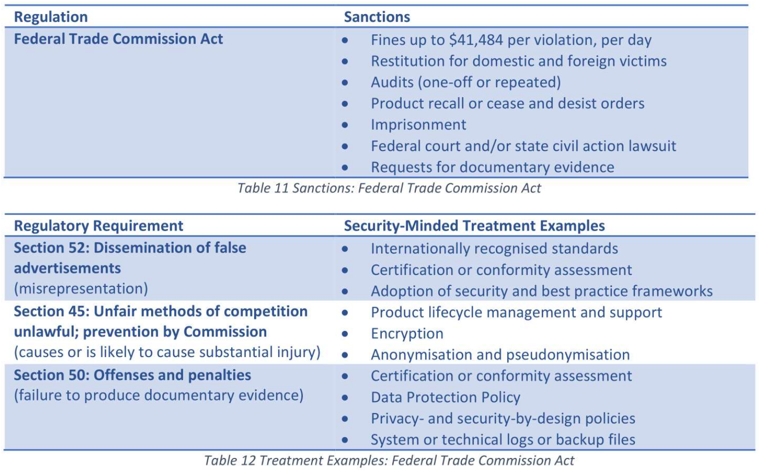
- … Diagnose, prevent, cure, mitigate, or treat
- … A disease or other condition
- … That affects the structure or function of the body

FDA guidance

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Postmarket Management of Cybersecurity in Medical Devices
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

https://www.fda.gov/medical-devices/digital-health/cybersecurity

Example regulation: FTC



Regulation	Sanctions
Federal Trade Commission Act	• Fines up to $41,484 per violation, per day • Restitution for domestic and foreign victims • Audits (one-off or repeated) • Product recall or cease and desist orders • Imprisonment • Federal court and/or state civil action lawsuit • Requests for documentary evidence

Table 11 Sanctions: Federal Trade Commission Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 52: Dissemination of false advertisements (misrepresentation)	• Internationally recognised standards • Certification or conformity assessment • Adoption of security and best practice frameworks
Section 45: Unfair methods of competition unlawful; prevention by Commission (causes or is likely to cause substantial injury)	• Product lifecycle management and support • Encryption • Anonymisation and pseudonymisation
Section 50: Offenses and penalties (failure to produce documentary evidence)	• Certification or conformity assessment • Data Protection Policy • Privacy- and security-by-design policies • System or technical logs or backup files

Table 12 Treatment Examples: Federal Trade Commission Act

https://www.iotsecurityfoundation.org/best-practice-guidelines/

Example regulation: FTC

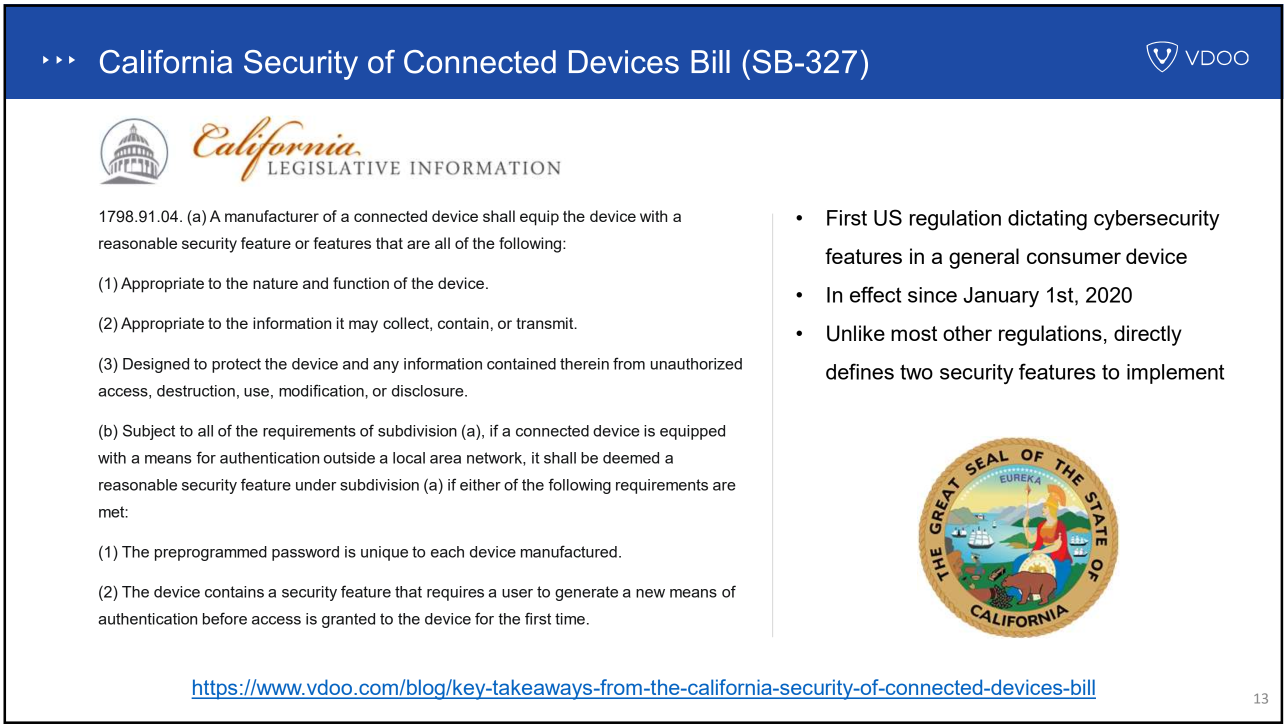
vs.

"TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure."
In fact, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address."

https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc

The charges were settled, with TRENDnet agreeing to:

- Stop misleading marketing
- Provide customers with free tech support over 2 years
- Establish a comprehensive information security program with third-party security audits every 2 years for 20 years.



California Security of Connected Devices Bill (SB-327)

VDOO

California LEGISLATIVE INFORMATION

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.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured.

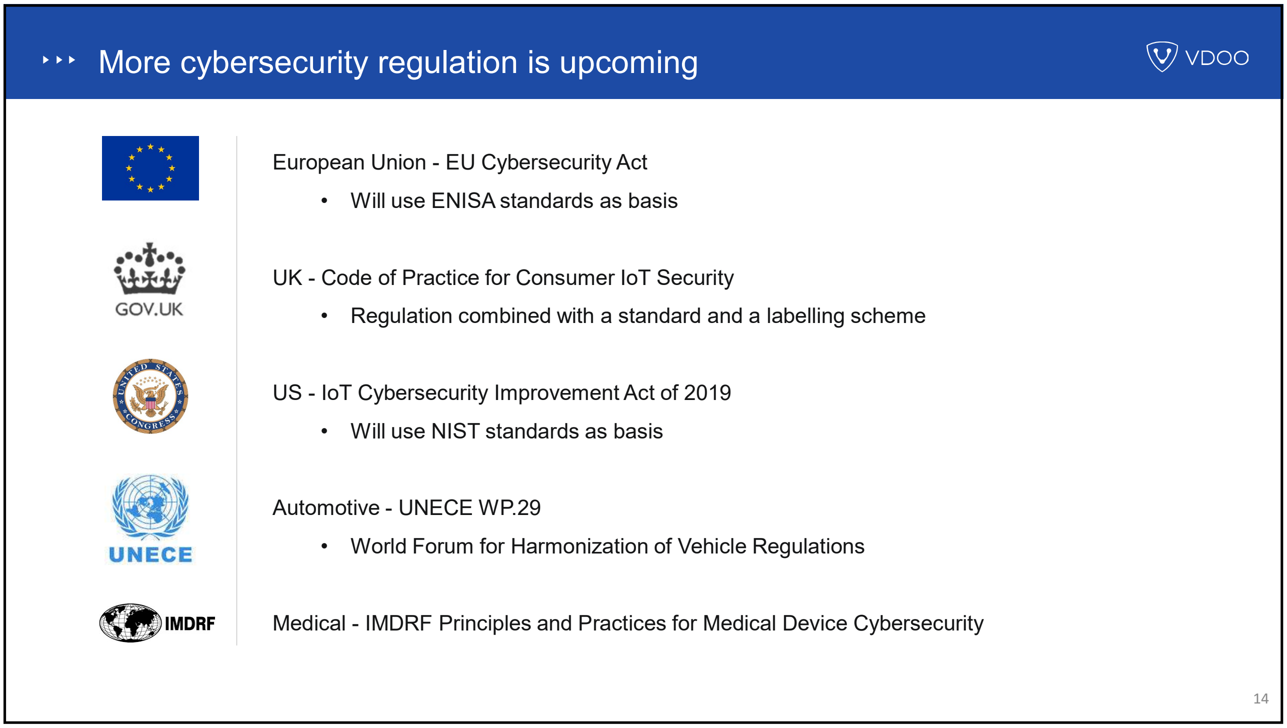
(2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

- First US regulation dictating cybersecurity features in a general consumer device
- In effect since January 1st, 2020
- Unlike most other regulations, directly defines two security features to implement

THE GREAT SEAL OF THE STATE OF CALIFORNIA
EUREKA

https://www.vdoo.com/blog/key-takeaways-from-the-california-security-of-connected-devices-bill

13



More cybersecurity regulation is upcoming

VDOO

European Union - EU Cybersecurity Act

- Will use ENISA standards as basis

GOV.UK

UK - Code of Practice for Consumer IoT Security

- Regulation combined with a standard and a labelling scheme

US - IoT Cybersecurity Improvement Act of 2019

- Will use NIST standards as basis

UNECE

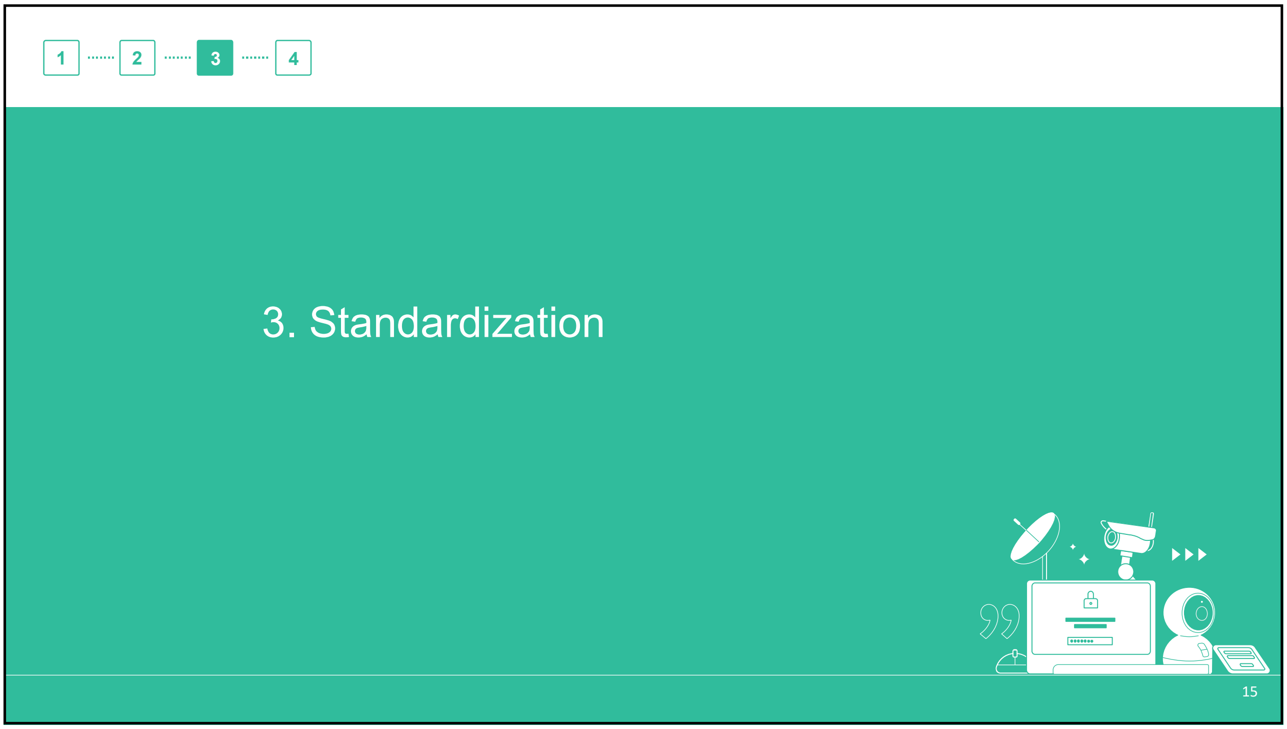
Automotive - UNECE WP.29

- World Forum for Harmonization of Vehicle Regulations

IMDRF

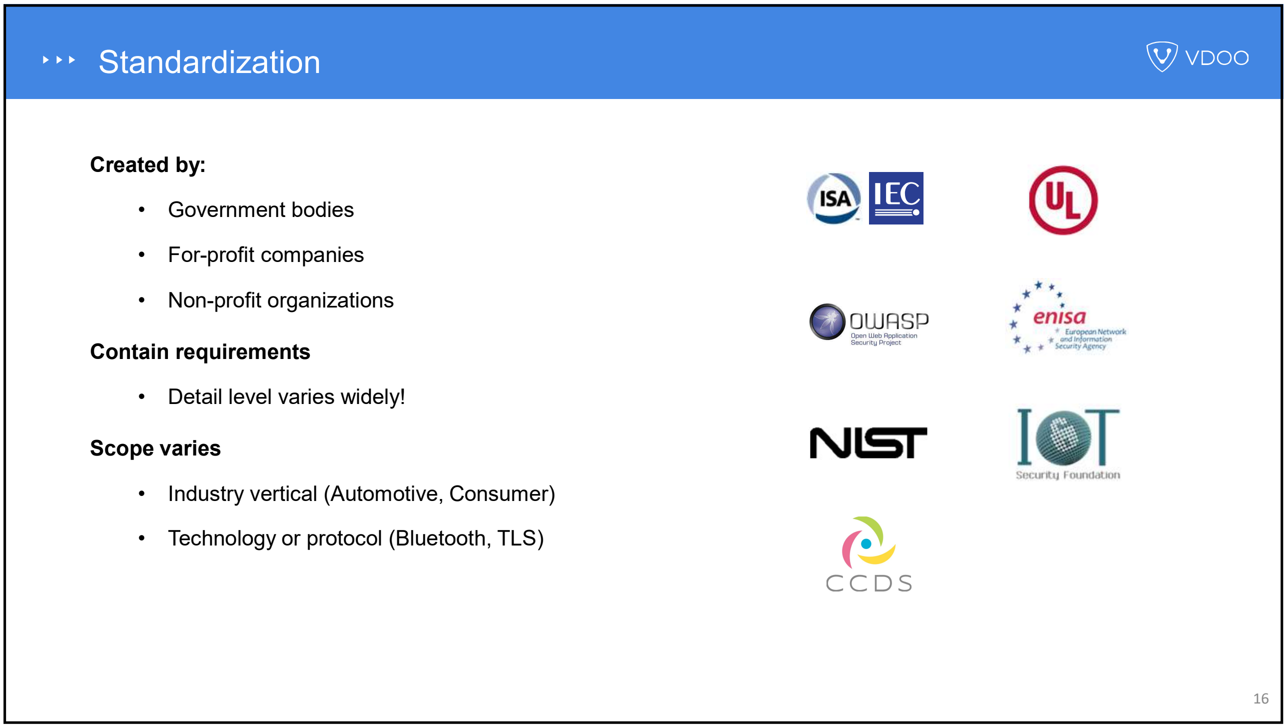
Medical - IMDRF Principles and Practices for Medical Device Cybersecurity

14



3. Standardization

15



Standardization

VDOO
ISA
IEC
UL
OWASP
Open Web Application Security Project
enisa
European Network and Information Security Agency
NIST
IoT
Security Foundation
CCDS

Created by:

- Government bodies
- For-profit companies
- Non-profit organizations

Contain requirements

- Detail level varies widely!

Scope varies

- Industry vertical (Automotive, Consumer)
- Technology or protocol (Bluetooth, TLS)

16

Example standard: FIPS 140-2

VDOO

Development pace
- Last published in 2002
- Incremental changes made to guidance documents
- Superseded by FIPS 140-3 in 2020

Region
- Originally – US
- In fact widely influential

Industry and product class
- Originally - cryptographic modules
- In fact widely used in the embedded industry

NIST

FIPS 140-2

Technical detail level
- High

Enforcement
- For US government purchases only

Certification type
- Explicit - Cryptographic Module Validation Program
- Uses certification laboratories
- Involves releasing materials to the public
- Explicit re-certification program
- Many companies claim compliance without certification
- FIPS 140-2 certification closes in Sept 2021

Example standard: FIPS 140-3

VDOO

Development pace
- Published in 2020
- Based on two ISO/IEC documents:
  - ISO/IEC 19790:2012
  - ISO/IEC 24759:2017

Region
- US, Canada
- Expected to be widely influential like its predecessor

Industry and product class
- Still meant for cryptographic modules

NIST

FIPS 140-3

Technical detail level
- High

Enforcement
- For US government purchases only

Certification type
- Explicit - Cryptographic Module Validation Program (same as for FIPS 140-2)

Differences from FIPS 140-2
- Multiple changes
- Requires buying the ISO/IEC standards

Example standard: NIST SP 800-171

Development pace

- Last published in Feb 2020
- Previous versions in 2015, 2016

Region

- Originally – US
- In fact widely influential

Industry and product class

- Enterprise organizations deploying general purpose PCs, connected devices, and mobile phones (including BYOD scenarios)
- In fact widely used in the embedded industry

Technical detail level

- Medium
- Refers to multiple NIST standards by relevant area

NIST
SP 800-171

Enforcement

- Required by Department of Defense via DFARS clause 252.204-7012 (Federal Acquisition Regulation)
- Applies to contractors and sub-contractors!
- Based on the Federal Information Security Management Act of 2002 (FISMA) Moderate level requirements

Certification type

- Uses third-party companies

Example standard: UL 2900

Development pace

- Only published in 2017

Region

- US-based, worldwide influence

Industry and product class

- General: 2900-1
- Industrial: 2900-2-2
- Medical: 2900-2-3
- Cryptographic modules: 2900-3-1

Technical detail level

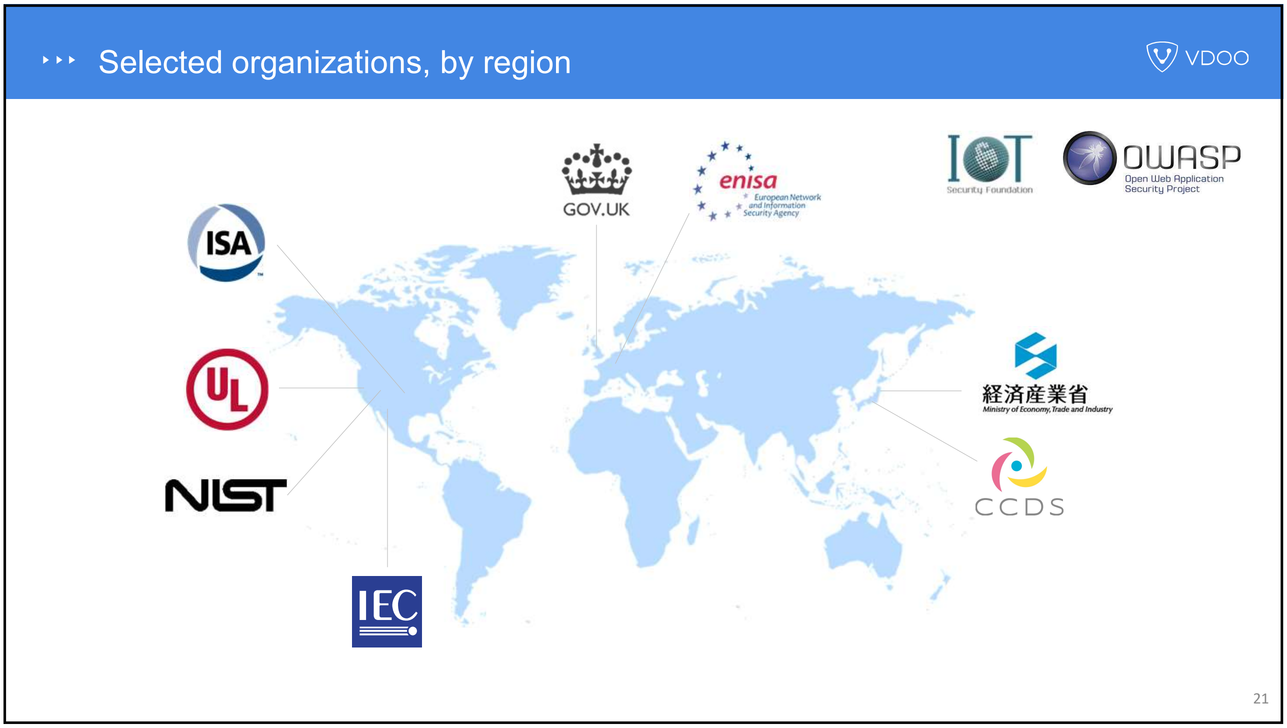
- Low to Medium

Enforcement

- None

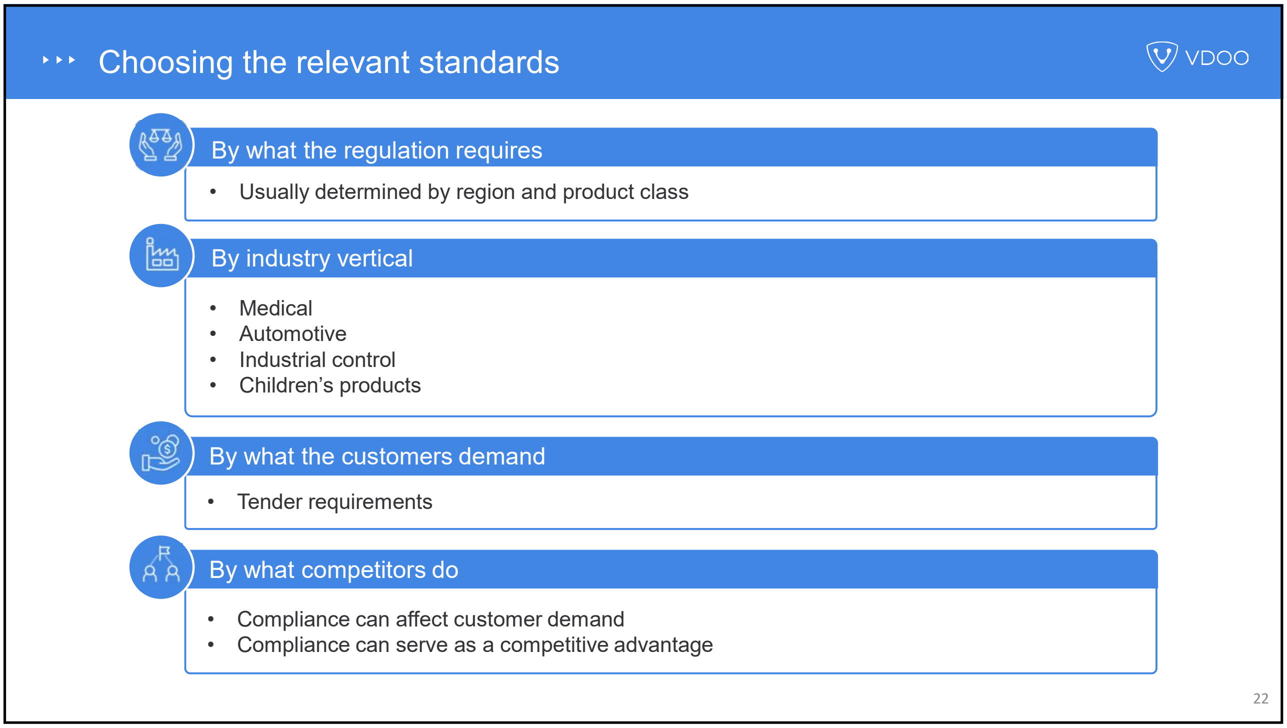
Certification type

- Explicit
- Uses UL certification laboratories
- Recognized by FDA



Selected organizations, by region

VDOO
GOV.UK
enisa
European Network and Information Security Agency
IoT
Security Foundation
OWASP
Open Web Application Security Project
ISA
UL
NIST
IEC
経済産業省
Ministry of Economy, Trade and Industry
CCDS
21



Choosing the relevant standards

By what the regulation requires

- Usually determined by region and product class

By industry vertical

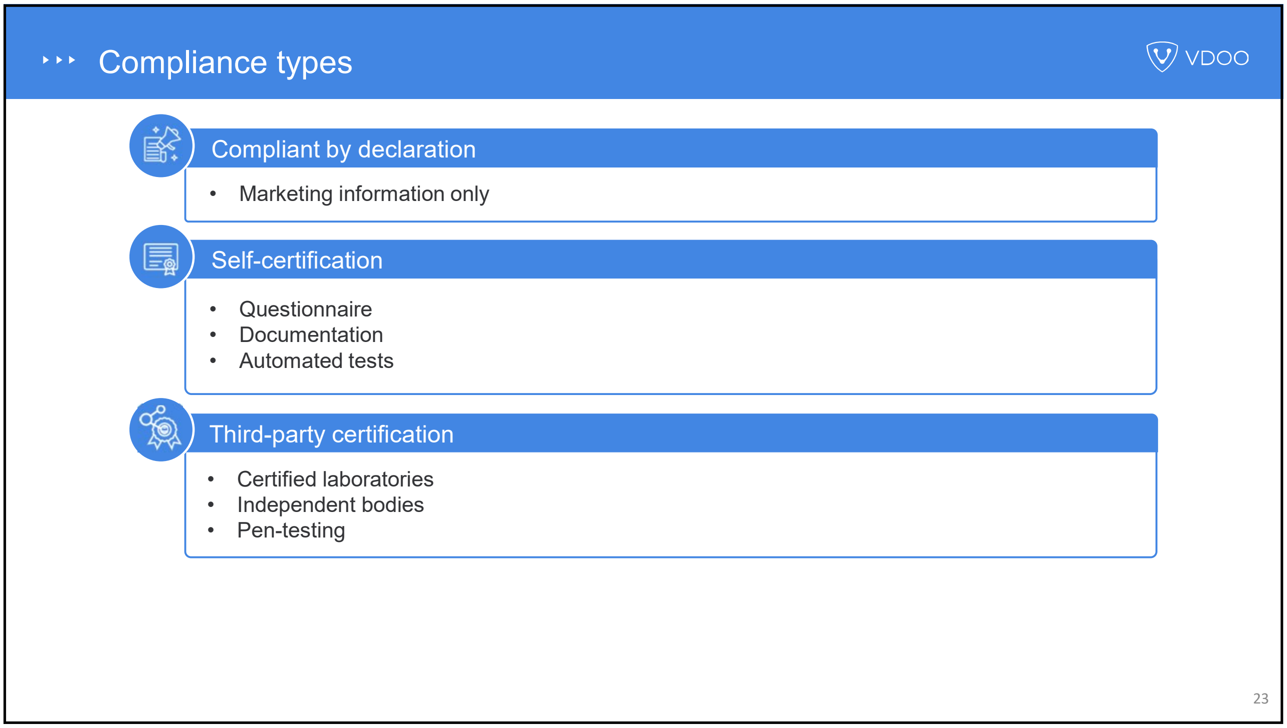
- Medical
- Automotive
- Industrial control
- Children’s products

By what the customers demand

- Tender requirements

By what competitors do

- Compliance can affect customer demand
- Compliance can serve as a competitive advantage



Compliance types

VDOO

Compliant by declaration

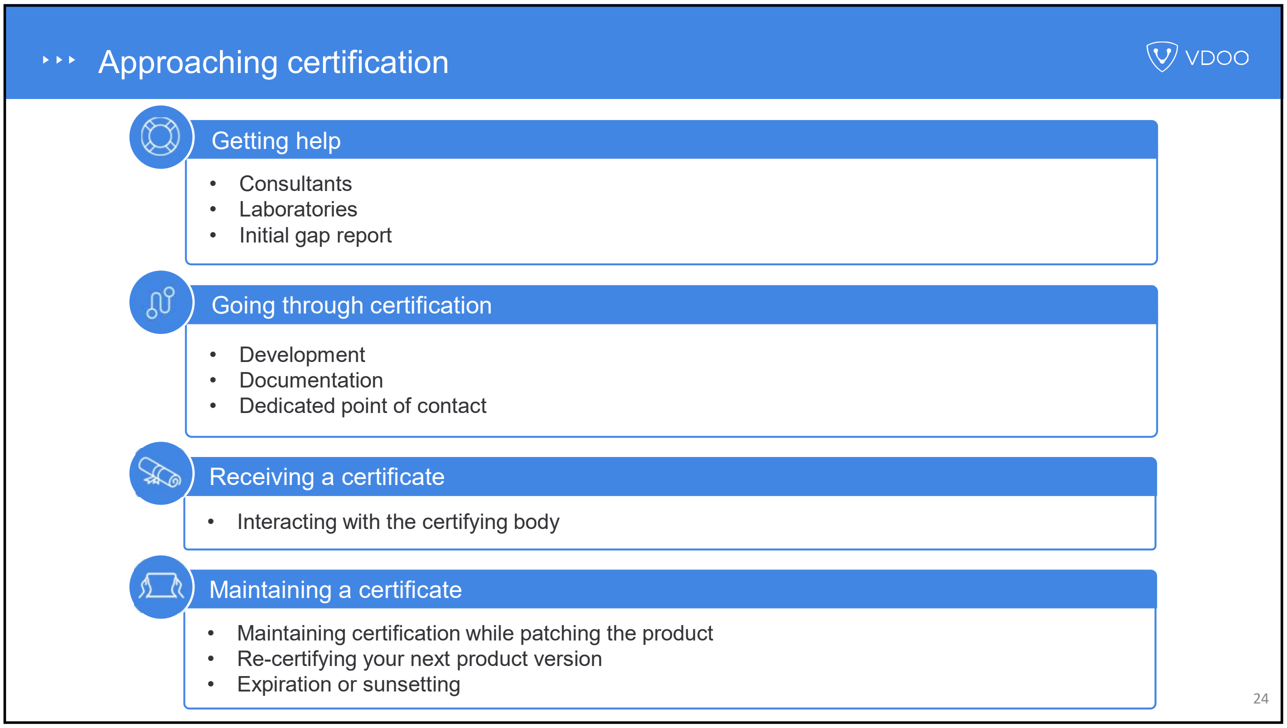
- Marketing information only

Self-certification

- Questionnaire
- Documentation
- Automated tests

Third-party certification

- Certified laboratories
- Independent bodies
- Pen-testing



Approaching certification

VDOO

Getting help

- Consultants
- Laboratories
- Initial gap report

Going through certification

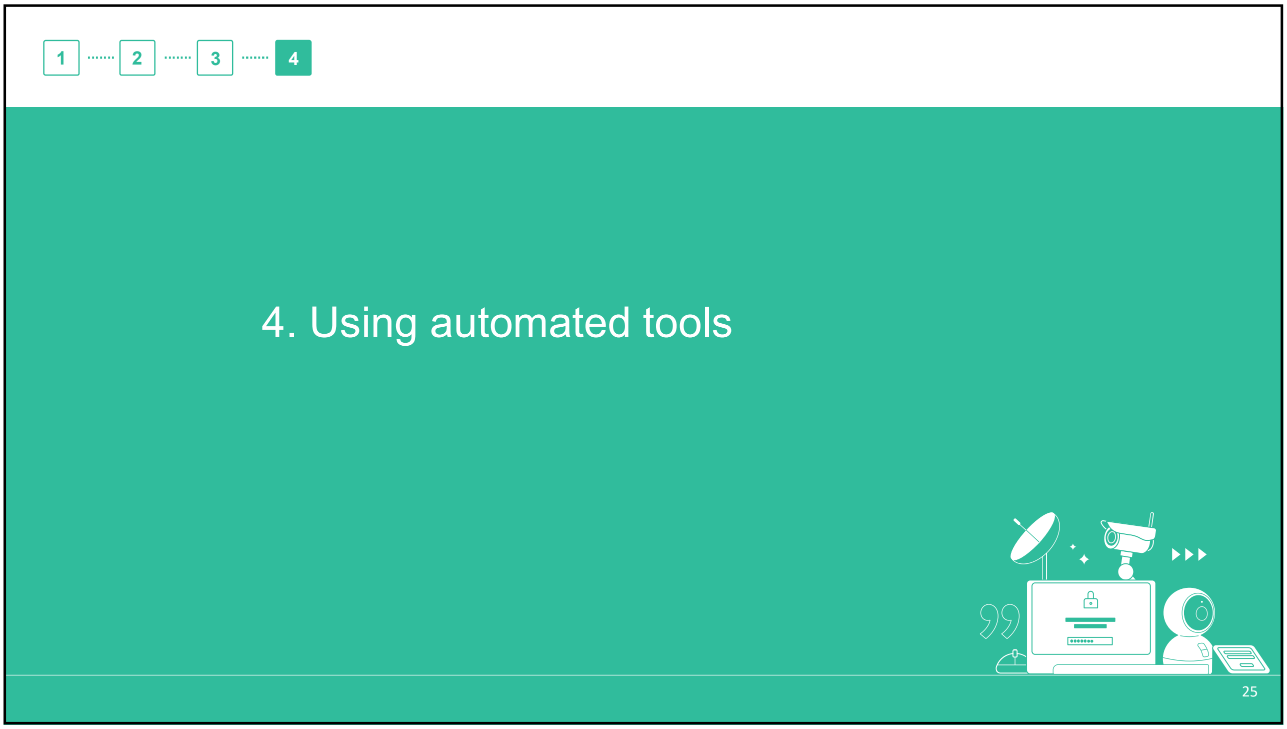
- Development
- Documentation
- Dedicated point of contact

Receiving a certificate

- Interacting with the certifying body

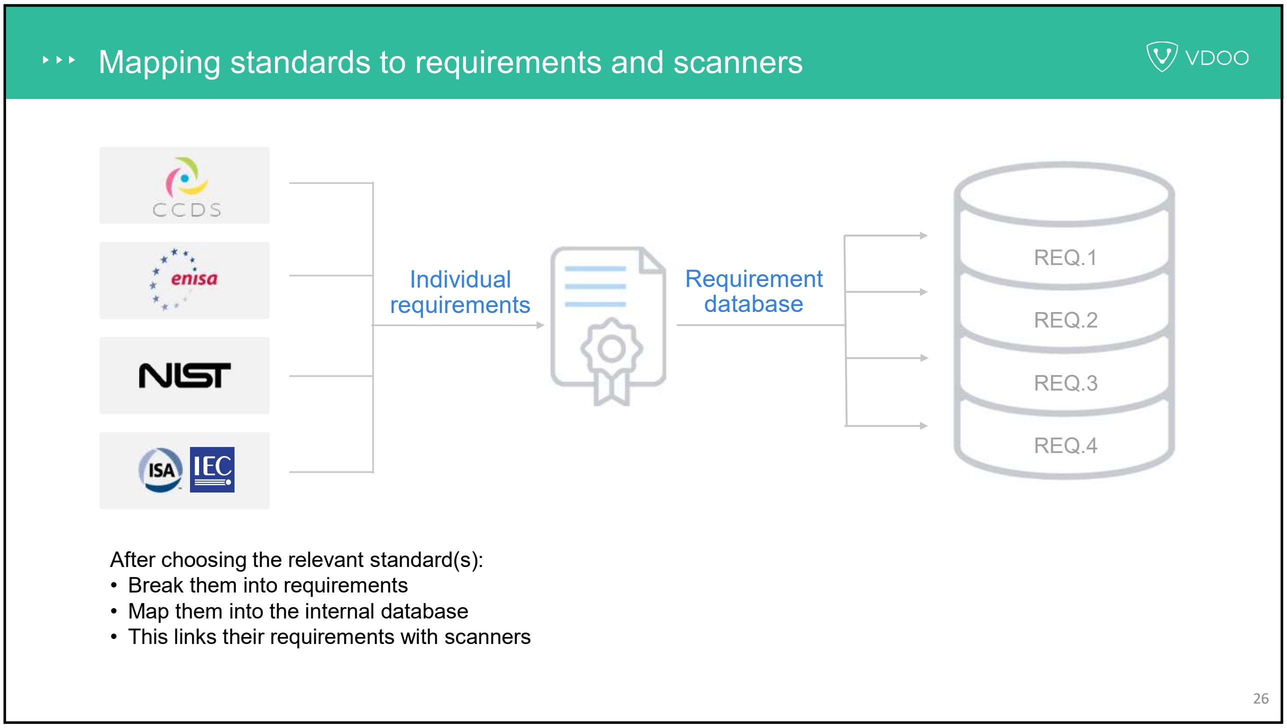
Maintaining a certificate

- Maintaining certification while patching the product
- Re-certifying your next product version
- Expiration or sunsetting



1 ······· 2 ······· 3 ······· 4

4. Using automated tools



Mapping standards to requirements and scanners

VDOO

CCDS

enisa

NIST

ISA IEC

Individual requirements

Requirement database

REQ.1

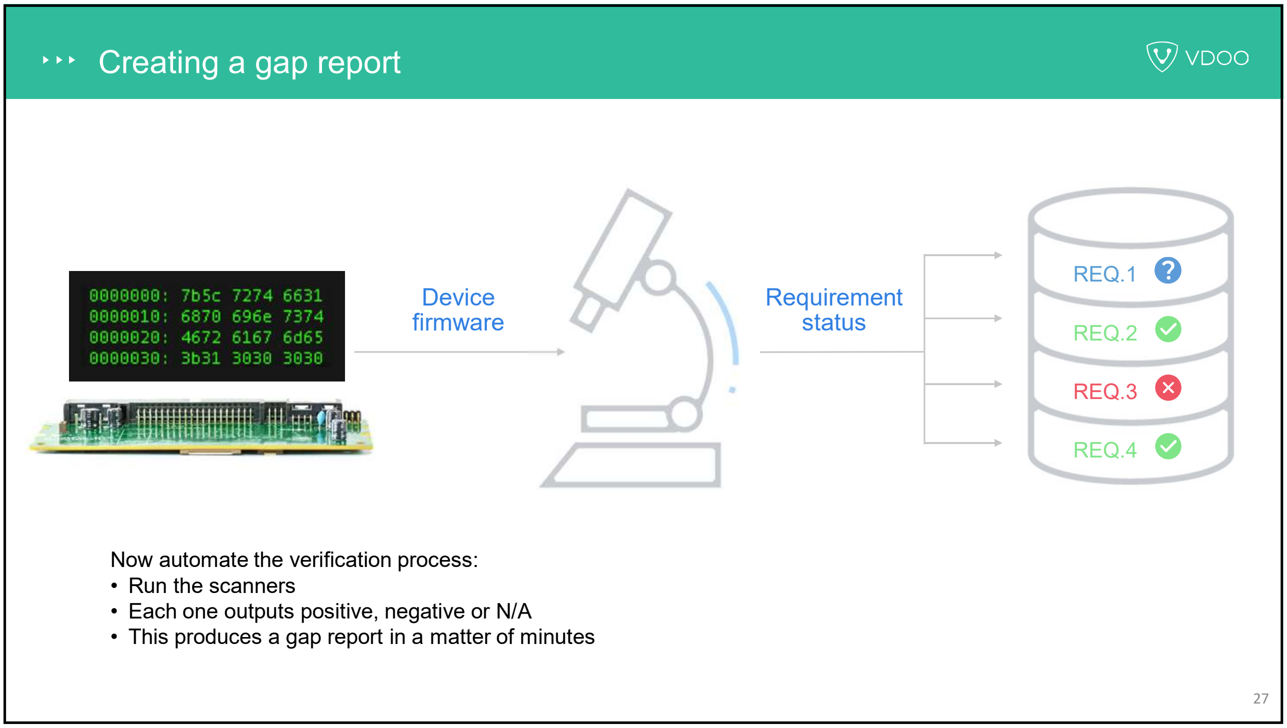
REQ.2

REQ.3

REQ.4

After choosing the relevant standard(s):

- Break them into requirements
- Map them into the internal database
- This links their requirements with scanners

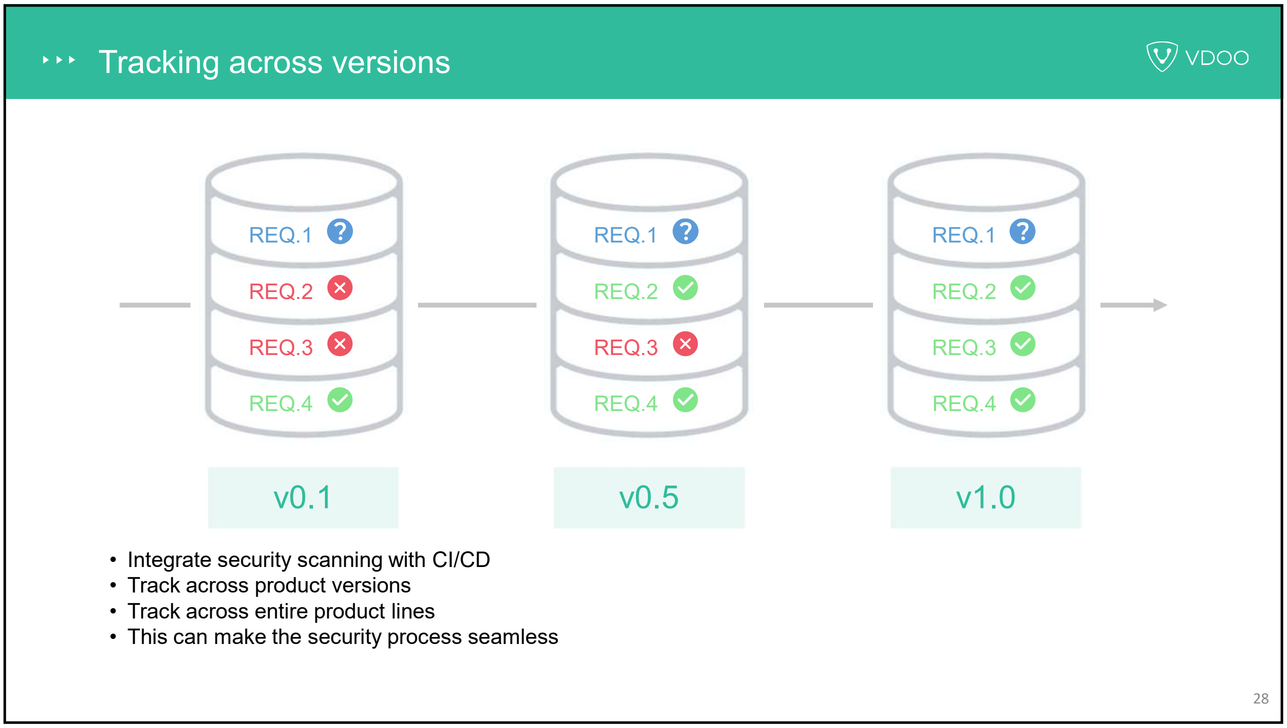


Creating a gap report

```
0000000: 7b5c 7274 6631
0000010: 6870 696e 7374
0000020: 4672 6167 6d65
0000030: 3b31 3030 3030
```

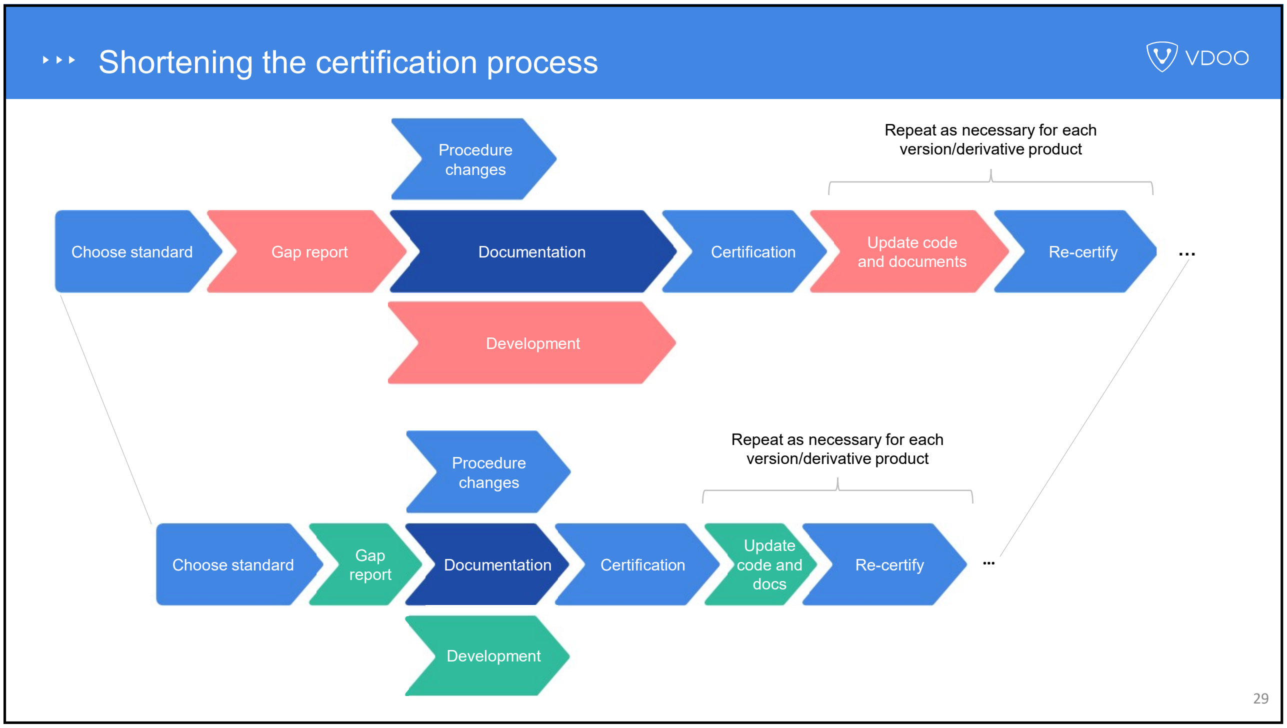
Now automate the verification process:

- Run the scanners
- Each one outputs positive, negative or N/A
- This produces a gap report in a matter of minutes



Tracking across versions

- Integrate security scanning with CI/CD
- Track across product versions
- Track across entire product lines
- This can make the security process seamless



Shortening the certification process

VDOO

Procedure changes

Repeat as necessary for each version/derivative product

Choose standard → Gap report → Documentation → Certification → Update code and documents → Re-certify …

Development

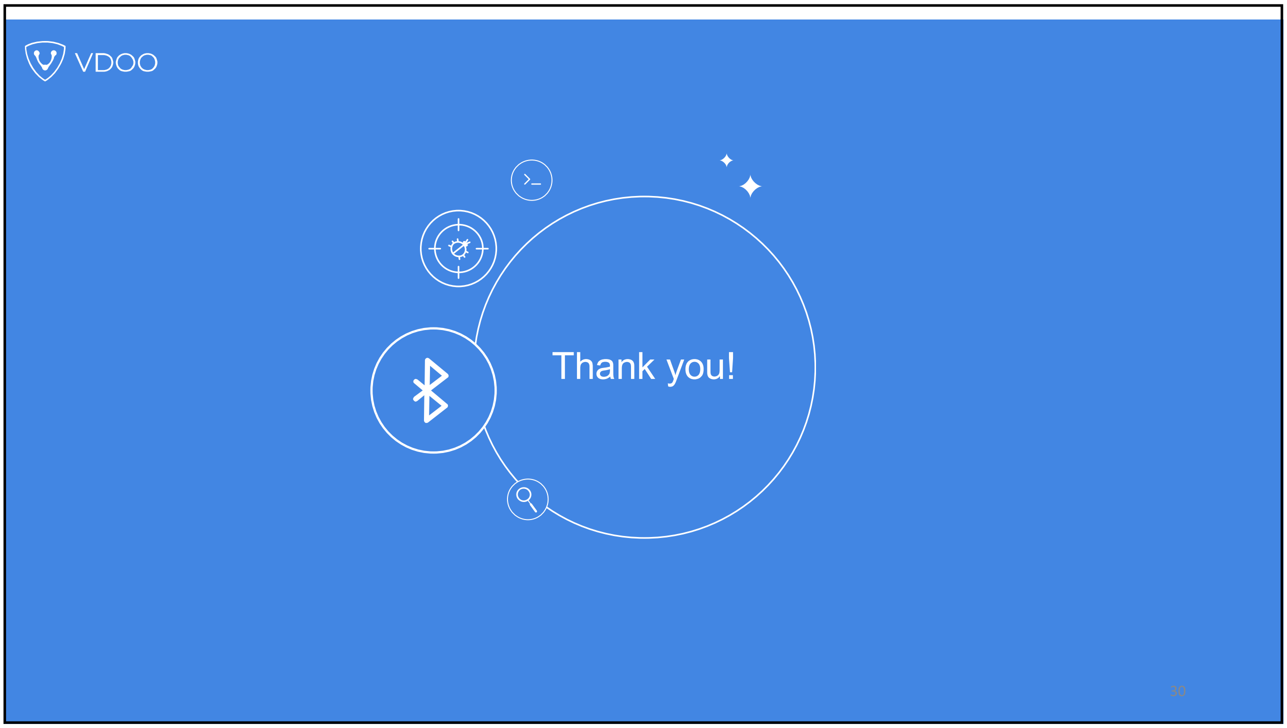
Procedure changes

Repeat as necessary for each version/derivative product

Choose standard → Gap report → Documentation → Certification → Update code and docs → Re-certify …

Development

29



VDOO

Thank you!

30