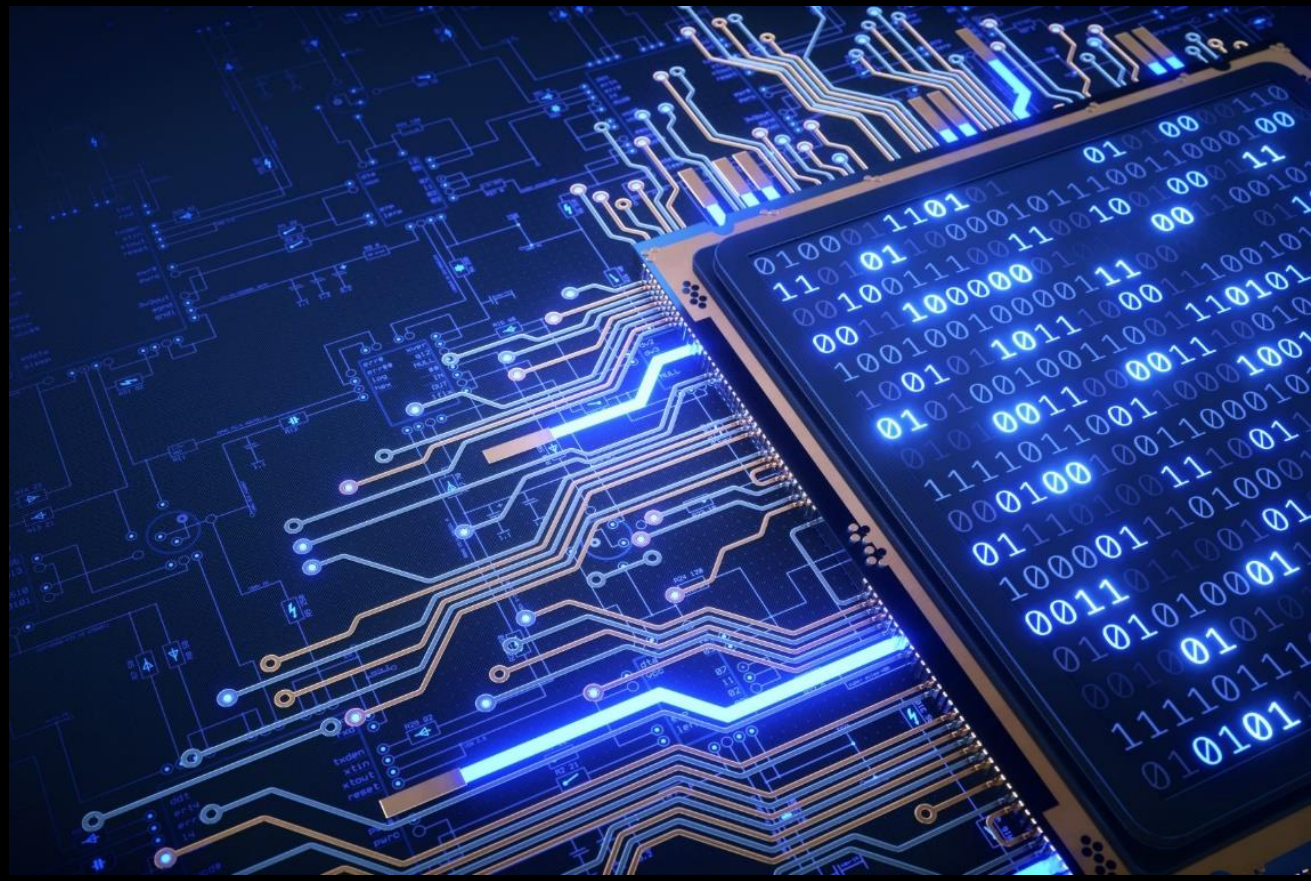
TATA CONSULTANCY SERVICES

Building on belief

IoT Security - Global Standards & Regulatory landscape



Ganesh Subramanya
Head, OT & IoT Security Practice
TCS Cyber Security

IoT Security Trends

Device interconnectivity introduces newer attack surfaces and increases risks

Convergence of IT and mainstream technologies into device software and platform thereby bringing traditional IT cyber risks

Introduction of regulations especially in healthcare, CI (Critical Infrastructure)

Increasing cyber attacks on connected devices/IoT products

Increased awareness of consumer about data privacy and impact of cybersecurity on device/product safety

Top 3 drivers for regulations and standards

1	Increasing cyber risk and threat landscape	Impact not only on privacy and safety, but also national security and critical infrastructure.
2	Multiple stakeholders such as device manufacturers, service providers, network operators, regulators, and end-users.	Need to establish trust and confidence in the IoT ecosystem.
3	Fragmented and complex IoT regulatory environment across different geographies and sectors.	Need to harmonize and simplify

The global IoT standards and regulations landscape is expanding

Regulations & Directives

IoT Cybersecurity Improvement Act | EU CRA | EU RED | FDA QSR | TSA Directives | UN ECE R155 & R156

Consumer

ETSI EN 303 645

ETSI TS 103 701

ISO/IEC 27403.6

ETSI WI-00598

Automotive

ISO 21434

ISO PAS 5112

ISO/CD 24089

Industrial

ISA/IEC 62443 Series

UL 2900-2-2

UL2900-2-3

Medical & Healthcare

UL 2900-1, 2900-2-1

ISO 62304

ISO 60601-4-5

IEC 80001

Generic

ISO 27400

ISO 27402

ISO/IEC AWI 30149

ANSI/UL 2900-1

And several others..

US FDA Guidance for Medical Device Cybersecurity

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

The FDA has published[1] premarket and post market guidance that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous cybersecurity improvement throughout the product life-cycle to reduce risk.

Premarket Considerations

Applies to: Medical Device (IoMT / SaMD) Manufacturers

A

Use a Secure Product Development Framework (SPDF) to satisfy the Quality System Regulations (QSR)

- Security Risk Management (Threat modeling, Risk assessment, Third Party Software components – SBOMs)
- Security Architecture
- Cybersecurity testing

B

Cybersecurity Transparency

- Labeling Recommendations for Devices with Cybersecurity Risks
- Cybersecurity Management Plans
- Submission of Cybersecurity documentation for meeting QSR of FDA

Post market Considerations

Applies to: Medical Device (IoMT / SaMD) Manufacturers; Healthcare Device Operators (HDOs)

A

Medical Device Cybersecurity Risk Management

- A manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls.

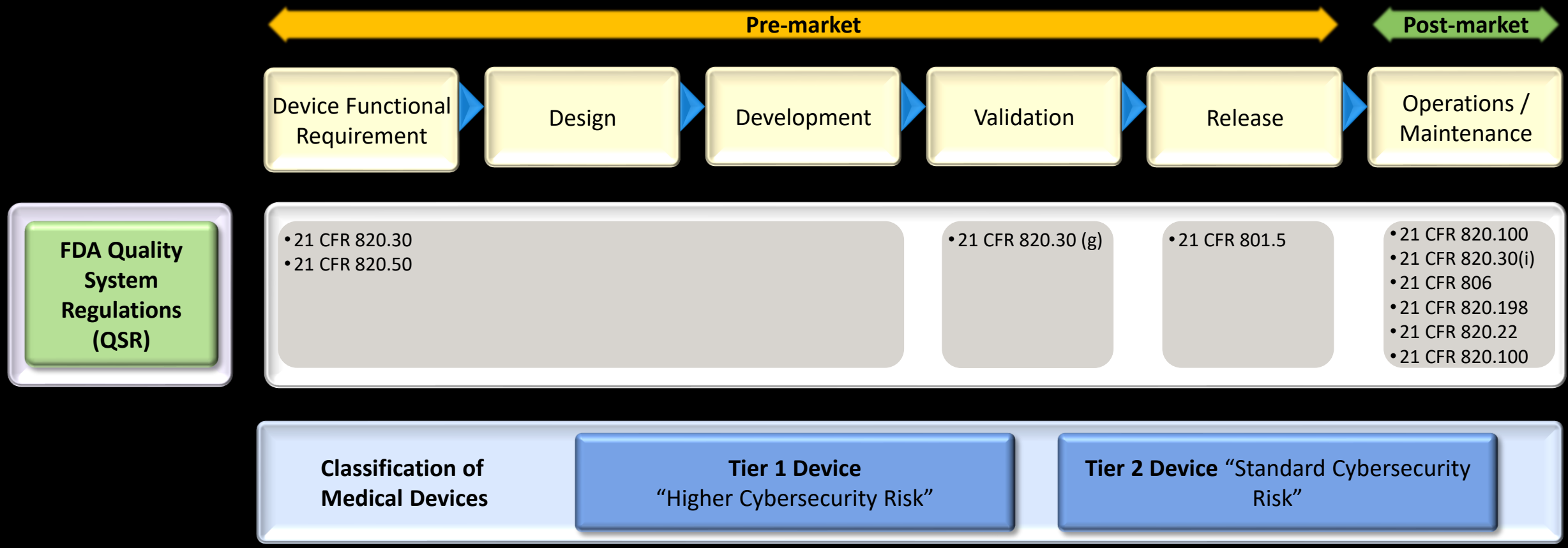
B

Remediating and Reporting Cybersecurity Vulnerabilities

- Adopt a coordinated vulnerability disclosure policy and practice
- Remediate cybersecurity vulnerabilities to reduce the risk of patient harm to an acceptable level

Ref: "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" document issued by FDA on September 27, 2023

US FDA Quality System Regulations and the Medical Devices Lifecycle



Other Prominent Standards For Medical Device Cybersecurity

TIR 57 - Technical Information Report 57

- Publisher : Association for the Advancement of Medical Instrumentation (AAMI)
- Cybersecurity risk management in the overall development of the device
- Based on ANSI/AAMI/ISO 14971
- Highly focuses on cyber risks as compared to ISO 14971 for overall risks
- **Recognized by FDA as Approved Standard**

UL 2900 Series

- Made up of three specifications
- Testing framework for manufacturers for FDA compliance
- Provides repeatable, reproducible, testing-oriented criteria to assess a device
- **Recognized by US FDA as approved standard**

ISO 14971

- Overall risk management for medical devices
- **De facto standard for medical device manufacturers**
- Recognized by major regulatory bodies as an approved standard

Other References

- NIST SP 800-53 v4
- DTMoST
- 21 CFR 820 - QS Regulations
- ISO 13485 - Quality Standards
- AAMI SW 68
- ISO 27001
- ISO/IEC 80001

UNECE WP.29 Regulations on Connected Vehicles

R155. Cyber Security Management System (CSMS)

Scope Passenger cars, vans, trucks and buses, light four-wheeler vehicles equipped with automated driving functionality

Applicability 54 Contracting parties of the 1958 Agreement

R156. Software Update Management System (SUMS)

Release Adopted in June 2020, **in force from January 2021**

Principles 4 Distinct Principles

- **Manage Vehicle Cyber Risks**
- **Security by Design** to mitigate risks along the value chain
- **Detect and Respond to security incidents** across vehicle fleet
- **Safe and Secure software updates**

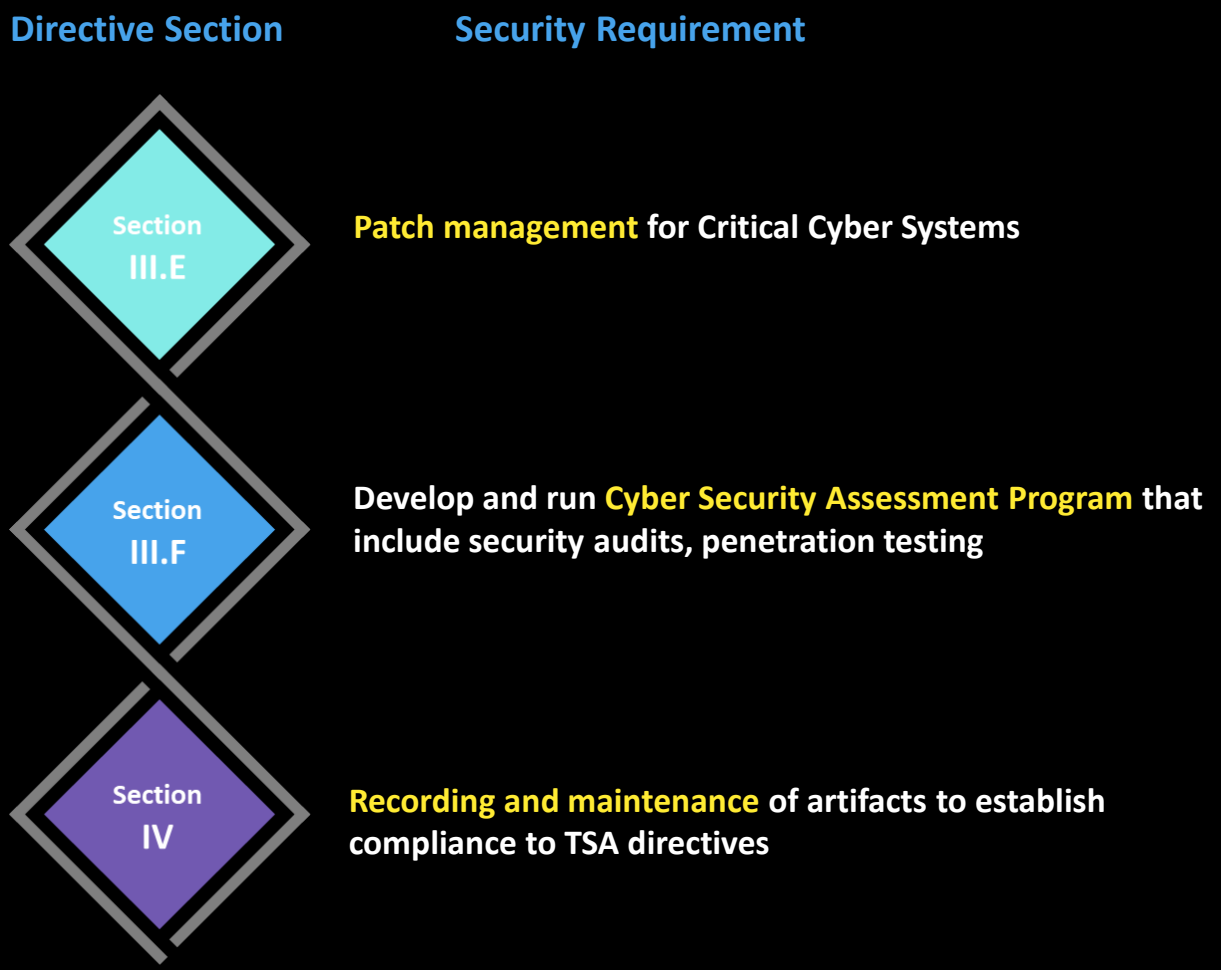
CSMS certification is mandatory for all new Vehicle Type Approvals

TSA Railroad Cyber Security Directive

Directive Section	Security Requirement
Section III.A	**Identification of critical cyber systems** deployed in owner/operator's railroad infrastructure
Section III.B.1	Define **network segmentation** policies and identify assets, network zoning requirement, communication and remote access requirements for Information Technology (IT) and Operational Technology (OT) cyber systems
Section III.B.2	Identification of cyber security controls for **securing various network zones** hosting IT/OT cyber systems
Section III.C	Implementation of **access control measures** to secure and prevent unauthorized access to critical cyber systems

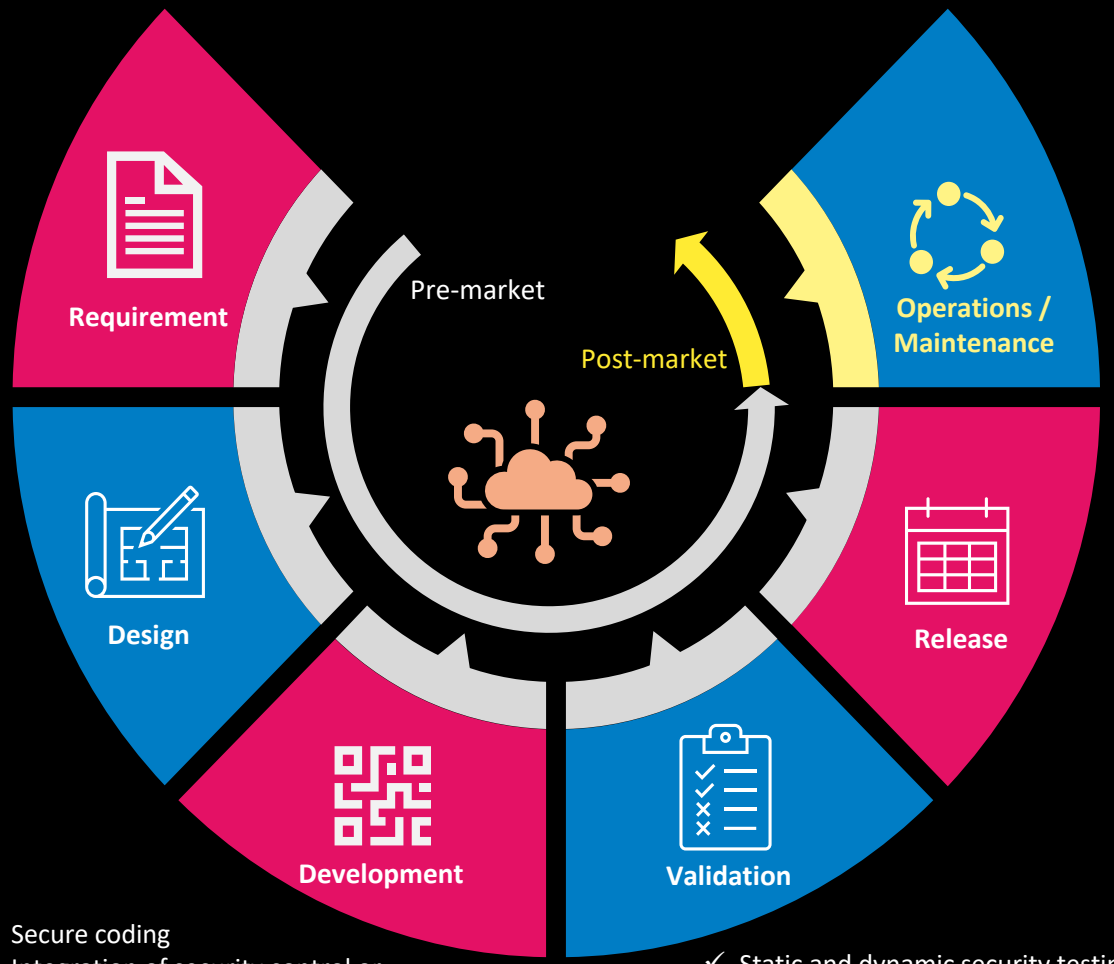
Directive Section	Security Requirement
Section III.D.1	Implementation of solution for **continuous threat monitoring** of critical cyber systems
Section III.D.2	Documentation of cyber incidents and implementation of **cyber incident response mechanism**
Section III.D.3	Ensure security logs are generated, collected, analyzed and retained for critical cyber physical systems
Section III.D.4	Implementation of control to ensure **quick isolation of OT network/systems** from IT network in case of cyber incident

TSA Railroad Cyber Security Directive



Ensure Security through the IoT Device Lifecycle

- ✓ Legal / Regulatory requirements
- ✓ Product security requirement specification
- ✓ Product's cyber risk profile



- ✓ **Zero-day vulnerability response plan**
- ✓ **Patch release program**
- ✓ **Remote / OTA updates**
- ✓ **SBOM Management**

- ✓ Secure design principle for software and device
- ✓ Threat modelling
- ✓ Risk assessment
- ✓ Security control design/selection
- ✓ Security of 3rd party/OEM component

- ✓ Labelling of cybersecurity risks and relevant security information
- ✓ Software Bill of Material (SBOM)

- ✓ Secure coding
- ✓ Integration of security control or solution
- ✓ Vulnerability remediation

- ✓ Static and dynamic security testing
- ✓ Device firmware security testing
- ✓ Interface / Integration security testing
- ✓ Vulnerability assessment and penetration testing of device

Stay ahead of regulations and standards

Establish and Implement an IoT Security Program

TATA CONSULTANCY SERVICES

Building on belief

Thank you


Ganesh.Subramanya@tcs.com


www.linkedin.com/in/ganeshsubramanya