Brochure

Approach to developing secure TETRA products

MOTOROLA SOLUTIONS

Cyber climate and security principles

Motorola Solutions uses a risk-based approach throughout our entire product development, implementation and operational support lifecycle. We strongly believe in the three foundational pillars of cybersecurity: Confidentiality, Integrity and Availability. We address these pillars with the application of protection, detection and response controls built with industry-leading people, processes and technology.

Organisations of all types are increasingly subject to data theft and loss, whether the asset is personal information, intellectual property, or sensitive data. It is therefore essential to ensure that the development practices that enforce strong security principles are in place. The US National Institute for Standards and Technology (NIST), housed within the US Department of Commerce, has developed standards and guidance for information protection. One of these is the Cybersecurity Framework (CSF), which helps provide structure and context to cybersecurity. NIST also provides the Secure Development Framework (SDF) which is a set of fundamental, sound and secure development practices based on established best practice documents from multiple organisations. We follow the principles defined by the NIST Cybersecurity Framework and the Secure Development Framework as part of our secure development methodology.

Secure development methodology

The following is a high level description of the practices we apply to the secure development of our TETRA radio infrastructure and devices:

Define

Prepare the organisation

Ensure that the organisation's people, processes and technology are prepared to perform secure software development at the organisation level and for individual development groups or projects.

Design

Protect the software

Define Cybersecurity solutions:

- Threat & Risk Driven
- Leverage Industry
- Attack Surface Reduction

Develop

Produce well-secured software

Produce well-secured software with secure testing and prioritisation of fixes.

Deploy

Respond to vulnerabilities

Release project to the field, taking into account:

- Residual Risk
- Incident Response Plan

How we cover the secure development activities

Define

Security requirements

- Product cybersecurity scope definition
- Open source review board
- Software configuration and management policies
- Key Performance Indicators (KPI)

Business environment

- Strong customer engagement to identify requirements
- Motorola Solutions Cybersecurity Risk Management Framework for vendors

Governance and compliance

- Product and services governance
- Risk Register and business risk owner
- Defined roles and responsibilities

Awareness and Training

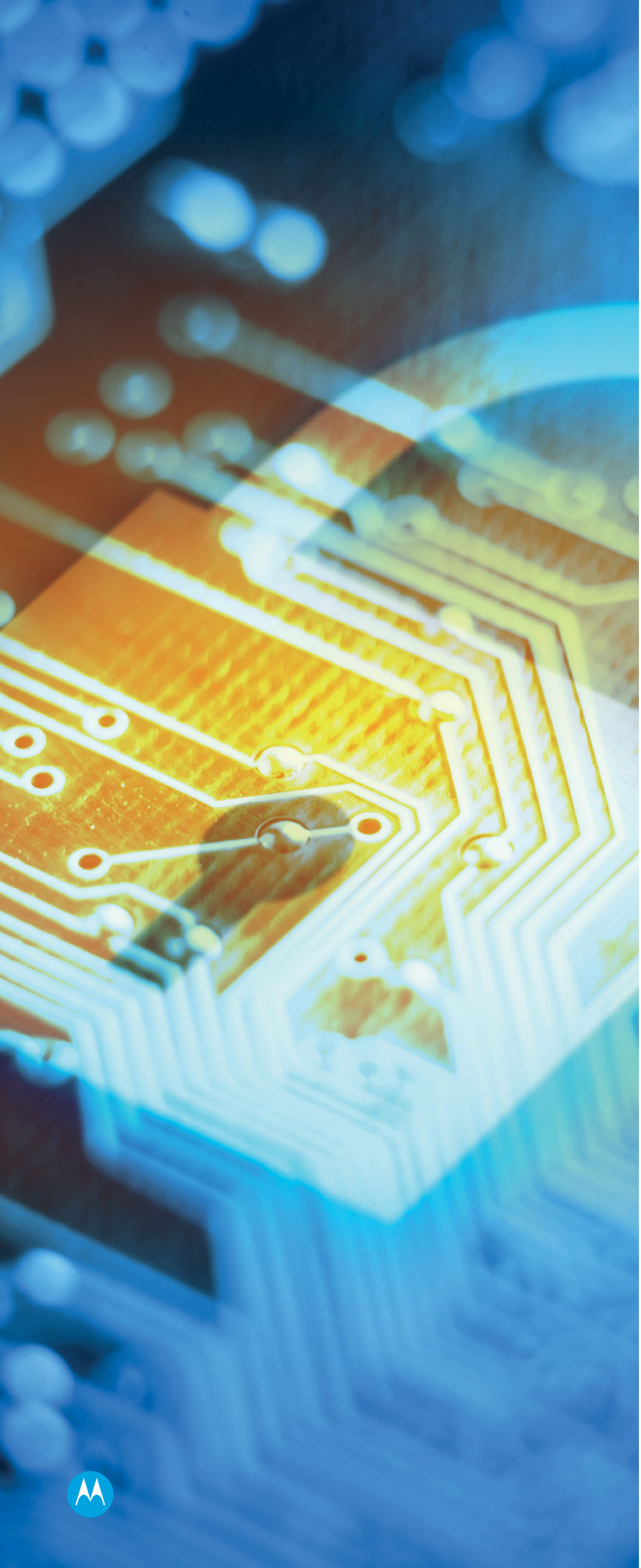
- Motorola Solutions personnel are required to receive regular and rigorous security training
- Security training is available for customers

Cybersecurity risk assessment

- System and product risk assessments based on NIST risk management frameworks
- Threat intelligence and communication
- Cybersecurity risk assessments of third party vendor products

Supply chain risk management

- Supplier qualification
- Supply chain controls



Design

Information protections and procedures

- Change control management
- Personally Identifiable Information (PII) assessment

Secure architecture principles

- Threat modelling
- Attack surface mapping
- Risk assessment
- Secure design reviews and audits
- Common secure design blocks

Data security

- Data at rest and in-transit security analysis
- Sensitive data identification

Design verification

- Review the design to confirm that it addresses applicable security requirements
- Review the design to confirm that it satisfactorily addresses the identified risks

Develop

Secure coding

- Compiler, interpreter and build tool configuration
- Secure code development training for all software engineers

Detect vulnerabilities

- Vulnerability scanning
- Static Application Security Testing (SAST)
- Abuse / misuse case testing
- Secure code reviews

Code verification

- Key Performance Indicators (KPI) review
- Default configuration states are secure
- Defect management, review and prioritisation

Improvements

- Feed findings and remediations back into the development cycle

Deploy

Release management

- Business risk owner review and sign off
- Validation of security requirements
- Security artifact collection and review

Maintenance

- Regular maintenance release
- Product specific releases
- Emergency releases when needed with minimal disruption to services

Communications

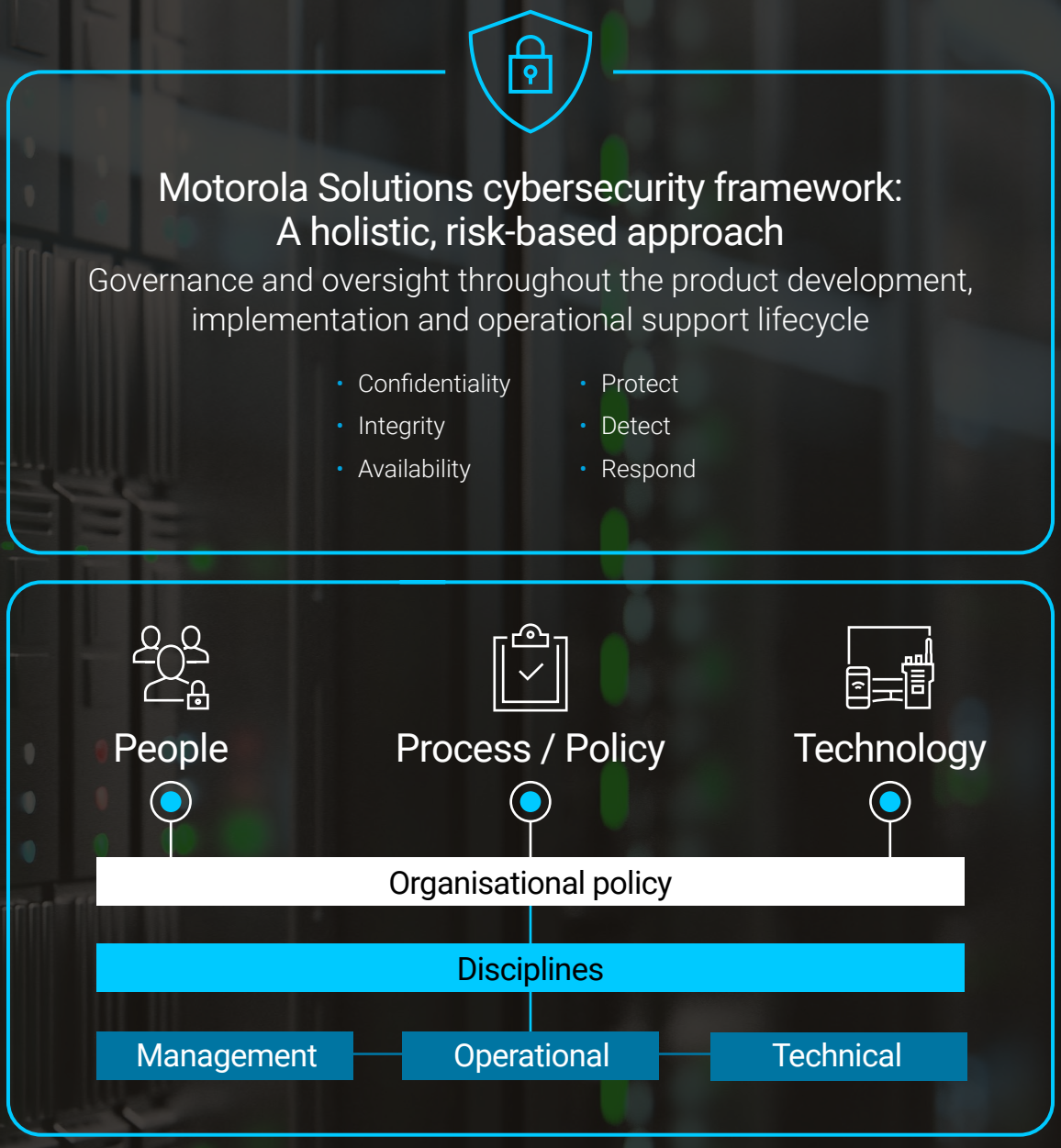
- Customer engagement
- Coordinated communications

Mitigation

- Customer issue resolution policy
- Incident management process
- Technical notification and updates

Motorola Solutions follows a robust secure development methodology based on industry trusted NIST cybersecurity frameworks to protect its products.

Utilising industry standard frameworks leverages proven guidelines for securing systems. This helps with risk-based approaches throughout our entire product development, implementation and operational support lifecycle. It also better prepares the organisation in identifying, detecting, preventing, responding and recovering in the event of a cybersecurity event.



Holistic risk management-based approach instead of 'Check-the-box' mindset

To learn more about TETRA, visit:
www.motorolasolutions.com/tetra

MOTOROLA SOLUTIONS

Motorola Solutions Ltd., Nova South, 160 Victoria Street, London, SW1E 5LB, United Kingdom