Enhanced Technology Development and Supply Chain Security Practices through O-TTPS / ISO 20243 Certification

Christine Bunke, Marie Cole, Wen Wei Low

IBM Systems Supply Chain Engineering

Keith Clisby, Warren Grunbok

*IBM Systems BISO**

Contact: bunkc@us.ibm.com

* Business unit Information Security Office

Purpose

- Highlight increased need for attention to systems cybersecurity practices
- Examples of cybersecurity standards spanning organizations and industries
- Review the contents and benefits of O-TTPS / ISO 20243 certification

Outline

- Introduction
- Cybersecurity risks drive new requirements
- Industry cybersecurity standards
- Client cybersecurity inquiries
- O-TTPS / ISO 20243
  - Requirements and recommendations
  - Item detail and evidence examples
  - Certification process
  - Benefits
- Conclusions

Introduction

"…cybersecurity is going to be the biggest issue of the next two decades" – Arvind Krishna, IBM CEO, (CRN Feb 2021)

- Increasing number of cyber incidents
- Increasing requests for security integrity evidence in development & supply chain
  - Business value in a standard approach
  - Demonstrate and certify business processes

Cybersecurity Standards

- Numerous security standards have been developed for use in the industry, examples include:
  - National Institute of Standards and Technology (NIST) Framework
  - ISO 27001 Information Security Management
  - Center for Internet Security (CIS) Controls®
  - Open Trusted Technology Provider™ Standard (O-TTPS) / ISO 20243
- Hardware suppliers must be concerned with IT & OT security: business continuity, data protection, asset physical protection, counterfeit parts, etc.

Cybersecurity Standards

Cybersecurity standards comparison (examples)

Identify		Protect		Detect		Respond		Recover	
Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #
Asset Management	1, 2, 12, 13, 14, 17, 19	Access Control	1, 3, 5, 9, 12, 14, 15, 16, 18	Anomalies and Events	1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 19	Response Planning	19	Recovery Planning	10
Business Environment		Awareness and Training	17, 18, 19						
Governance	19	Data Security	1, 2, 3, 13, 14, 18, 20	Security Continuous Monitoring	1, 2, 3, 4, 5, 7, 8, 9, 12, 13, 14, 15, 16, 20	Communications	19	Improvements	
Risk Assessment	4	Information Protection Processes & Procedures	3, 4, 5, 9, 10, 11, 16, 18, 19, 20			Analysis	4, 6, 8, 19		
Risk Management Strategy	4	Maintenance	3, 5	Detection Processes	19	Mitigation	4, 19	Communications	
Supply Chain Risk Management	4, 19, 20	Protective Technology	1, 3, 5, 6, 8, 12, 13, 11, 14, 15, 16			Improvements			

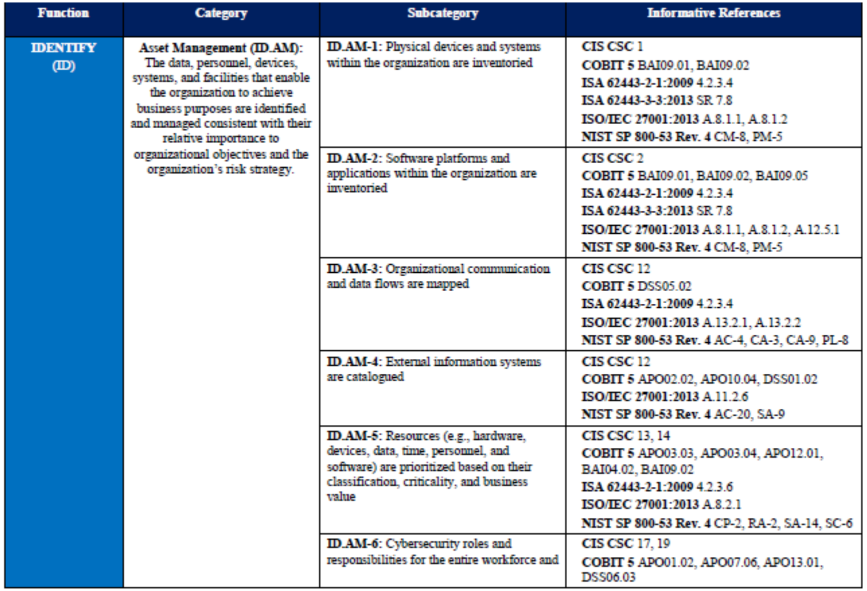
National Institute of Standards and Technology
U.S. Department of Commerce

Center for Internet Security®
Confidence in the Connected World®

Cybersecurity Standards

Cybersecurity standards comparison (examples)

Identify		Protect		Detect		Respond		Recover	
Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #
Asset Management	1, 2, 12, 13, 14, 17, 19	Access Control	1, 3, 5, 9 12, 14, 1 16, 18						
Business Environment		Awareness and Training	17, 18, 1						
Governance	19	Data Security	1, 2, 3, 1 14, 18, 2						
Risk Assessment	4	Information Protection Processes & Procedures	3, 4, 5, 9 10, 11, 1 18, 19, 2						
Risk Management Strategy	4	Maintenance	3, 5						
Supply Chain Risk Management	4, 19, 20	Protective Technology	1, 3, 5, 6 12, 13, 1 14, 15, 1						



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

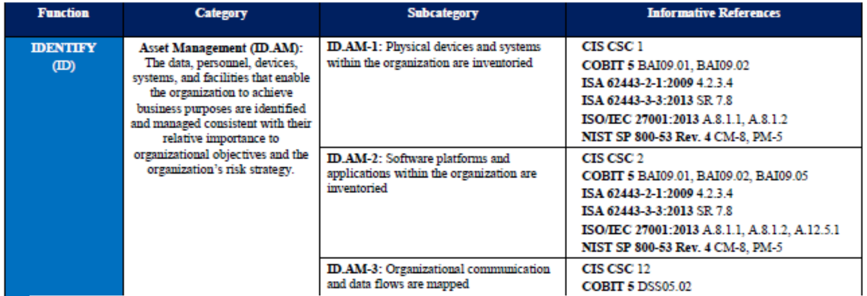
NIST National Institute of Standards and Technology U.S. Department of Commerce

CIS Center for Internet Security®
Confidence in the Connected World®

Cybersecurity Standards

Cybersecurity standards comparison (examples)

Identify		Protect		Detect		Respond		Recover	
Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #	Category	CIS Ref #
Asset Management	1, 2, 12, 13, 14, 17, 19	Access Control	1, 3, 5, 9 12, 14, 1 16, 18						
Business Environment		Awareness and Training	17, 18, 1						
Governance	19	Data Security	1, 2, 3, 1 14, 18, 2						
Risk Assessment	4	Information Protection Processes & Procedures	3, 4, 5, 9 10, 11, 1 18, 19, 2						
Risk Management Strategy	4	Maintenance	3, 5						
Supply Chain Risk Management	4, 19, 20	Protective Technology	1, 3, 5, 6 12, 13, 1 14, 15, 1						



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02

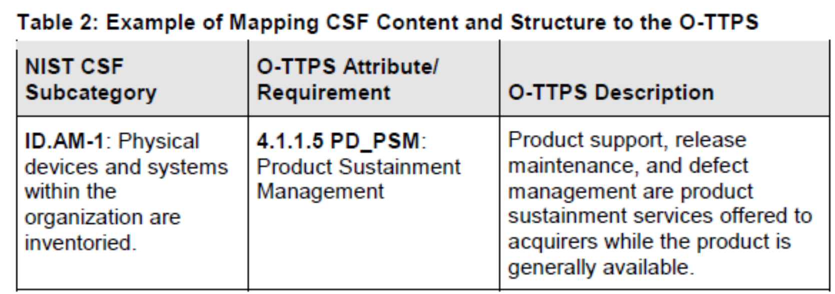


Table 2: Example of Mapping CSF Content and Structure to the O-TTPS

NIST CSF Subcategory	O-TTPS Attribute/ Requirement	O-TTPS Description
ID.AM-1: Physical devices and systems within the organization are inventoried.	**4.1.1.5 PD_PSM**: Product Sustainment Management	Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available.

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

CIS Center for Internet Security®
Confidence in the Connected World®

THE® Open GROUP

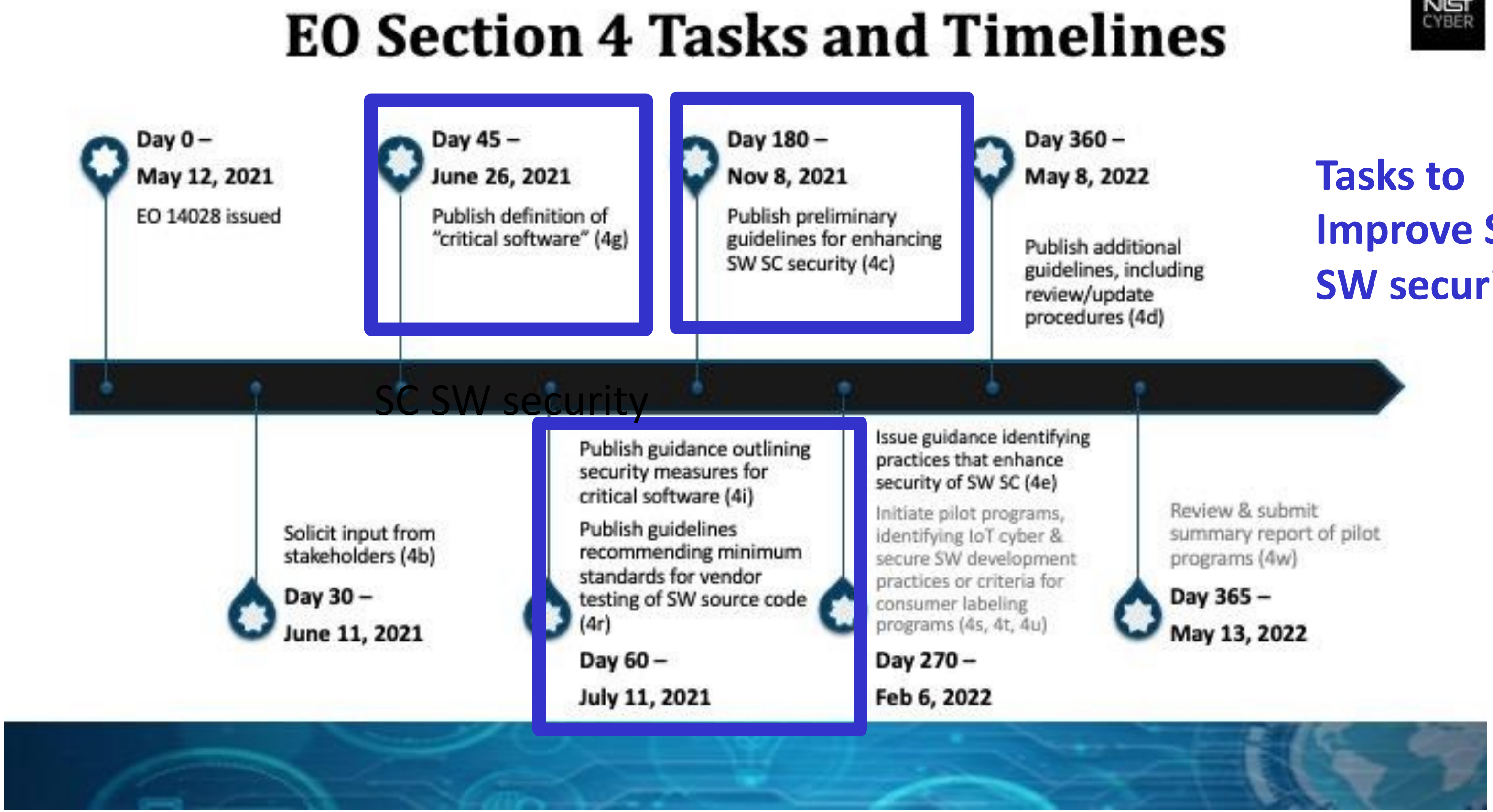
Client Inquiries

- Cybersecurity concerns drive significant client supply chain inquiries
  - Especially in government sectors but also utility & energy and finance & banking
  - 2021 U.S. Executive Order 14028 on “Improving the Nation’s Cybersecurity”
- Collateral and/or standards certification obtained in advance, streamlines responses
- Determine alignment of standards content to typical questionnaires

U.S. Executive Order 14028 on Improving the Nation’s Cybersecurity

- Policy to address persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector
- U.S. Executive Order objectives include
  - Sec. 2. Remove Barriers to Threat Information Sharing Between Government and the Private Sector
  - Sec. 3. Modernize and Implement Stronger Cybersecurity Standards in the Federal Government - moves Fed Gov to secure cloud services and a zero-trust architecture, and mandates deployment of multifactor authentication and encryption
  - **Sec. 4. Improve Software Supply Chain Security -** Directs NIST (National Institute of Standards and Technology) to develop baseline security standards for software development
  - Sec. 5. Establish a Cybersecurity Safety Review Board
  - Sec. 6. Create a Standard Playbook for Responding to Cyber Incidents
  - Sec. 7. Improve Detection of Cybersecurity Incidents on Federal Government Networks
  - Sec. 8. Improve Investigative and Remediation Capabilities

U.S. Executive Order 14028 Software Supply Chain Security



EO Section 4 Tasks and Timelines

Day 0 – May 12, 2021

EO 14028 issued

Day 30 – June 11, 2021

Solicit input from stakeholders (4b)

Day 45 – June 26, 2021

Publish definition of "critical software" (4g)

Day 60 – July 11, 2021

Publish guidance outlining security measures for critical software (4i)

Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

Day 180 – Nov 8, 2021

Publish preliminary guidelines for enhancing SW SC security (4c)

Day 270 – Feb 6, 2022

Issue guidance identifying practices that enhance security of SW SC (4e)

Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

Day 360 – May 8, 2022

Publish additional guidelines, including review/update procedures (4d)

Day 365 – May 13, 2022

Review & submit summary report of pilot programs (4w)

SC SW security

Tasks to Improve SC SW security

Ref: https://www.nist.gov/system/files/documents/noindex/2022/04/27/EO-task_and-timeline.pdf

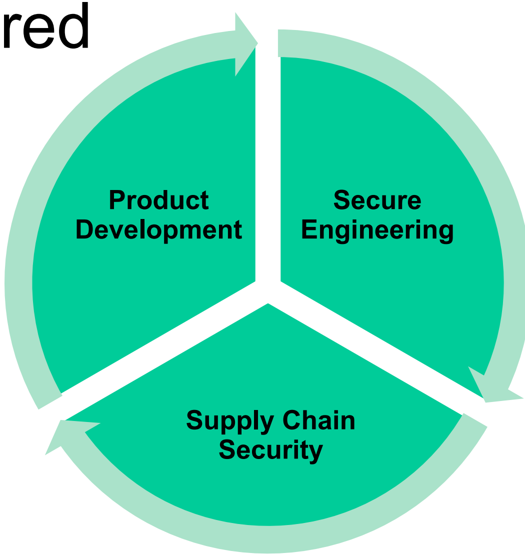
U.S. Executive Order 14028 – Section 4

Areas referenced by NIST SP 800-161r1 guidance in Supply Chain security

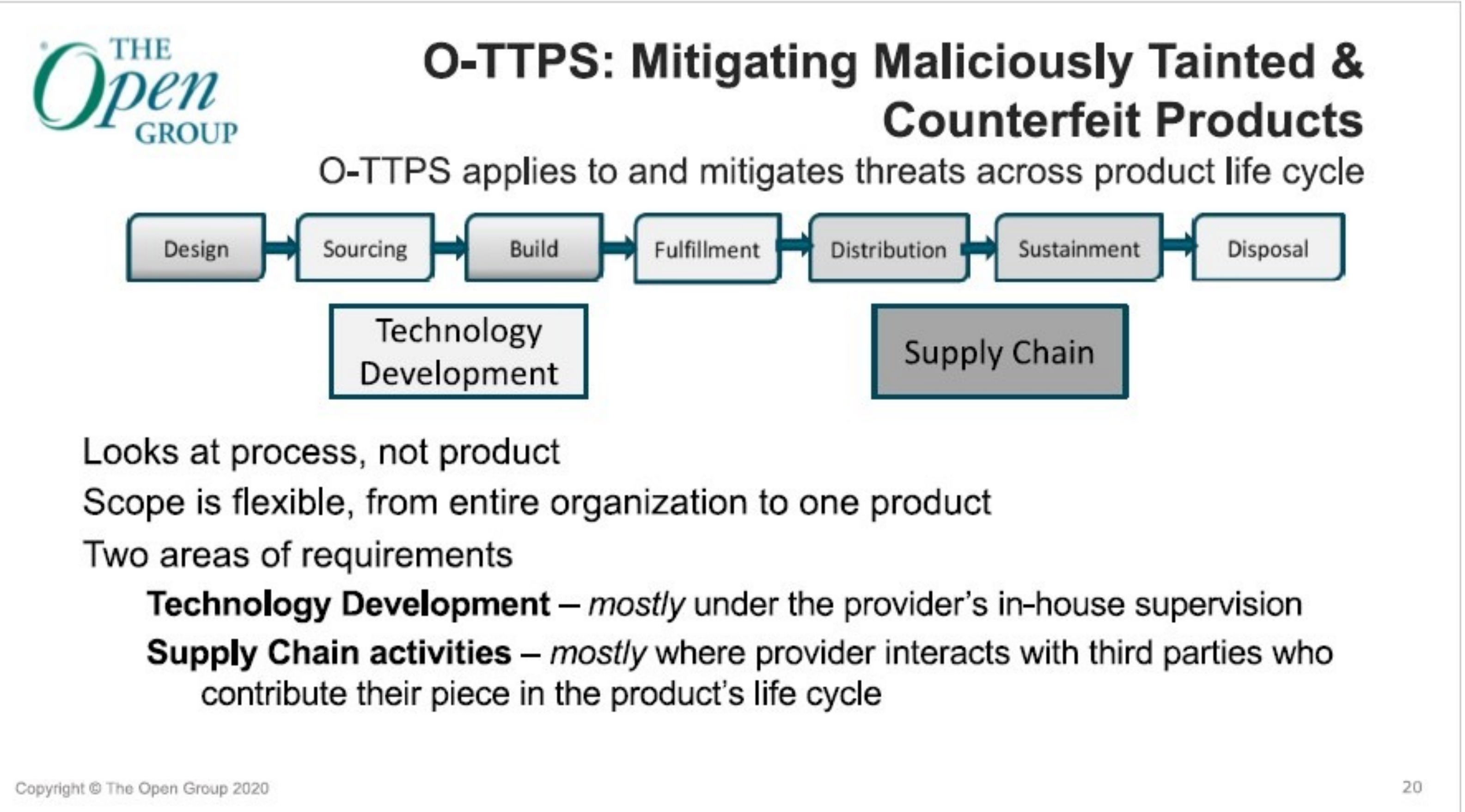
- Secure Software Development
  - Separate environments
  - Auditing trust relationships
  - Multi-factor, risk-based authentication
  - Data encryption
  - Monitoring/response
- Use of automated tools
- Documentation of artifacts
- Software Bill of Materials (SBOM)
- Vulnerability Disclosure program
- Conformity with secure software development practices
- Open-source software integrity

Cybersecurity Standard Selection

- Recommendations from input / requests from clients
- Open / available to clients, partners and suppliers
- Applicable to multiple market segments
- Flexible scope to apply as needed / desired
- Spans product life cycle, including
  - Product / technology development
  - Product security
  - Supply chain security



O-TTPS / ISO 20243 Overview



O-TTPS: Mitigating Maliciously Tainted & Counterfeit Products

O-TTPS applies to and mitigates threats across product life cycle

Design → Sourcing → Build → Fulfillment → Distribution → Sustainment → Disposal

Technology Development

Supply Chain

- Looks at process, not product
- Scope is flexible, from entire organization to one product
- Two areas of requirements
  - **Technology Development** – *mostly* under the provider's in-house supervision
  - **Supply Chain activities** – *mostly* where provider interacts with third parties who contribute their piece in the product's life cycle

O-TTPS / ISO 20243

Requirements and Recommendations

Area	Category / Attribute	Requirement (green) , Recommendation (gray)						
Technology Development	**Product Development**							
	Product Design Process	PD_DES.01	PD_DES.02	PD_DES.03				
	Configuration Management	PD_CFM.01	PD_CFM.02	PD_CFM.03	PD_CFM.04	PD_CFM.05	PD_CFM.06	
	Development Process and Practices	PD_MPP.01	PD_MPP.02					
	Quality and Test Management	PD_QAT.01	PD_QAT.02	PD_QAT.03				
	Product Sustainment Management	PD_PSM.01	PD_PSM.02	PD_PSM.03	PD_PSM.04	PD_PSM.05		
	Secure Engineering							
	Threat Analysis and Mitigation	SE_TAM.01	SE_TAM.02	SE_TAM.03				
	Run-time Protection Techniques	SE_RTP.01	SE_RTP.02	SE_RTP.03				
	Vulnerability Analysis and Response	SE_VAR.01	SE_VAR.02	SE_VAR.03	SE_VAR.04			
	Product Patching and Remediation	SE_PPR.01	SE_PPR.02	SE_PPR.03	SE_PPR.04			
	Secure Engineering Practices	SE_SEP.01	SE_SEP.02	SE_SEP.03				
	Monitor and Assess the Impact of Changes in the Threat Landscape	SE_MTL.01	SE_MTL.02	SE_MTL.03				
Supply Chain	**Supply Chain Security**							
	Risk Management	SC_RSM.01	SC_RSM.02	SC_RSM.03	SC_RSM.04	SC_RSM.05	SC_RSM.06	
	Physical Security	SC_PHS.01	SC_PHS.02	SC_PHS.03				
	Access Controls	SC_ACC.01	SC_ACC.02	SC_ACC.03	SC_ACC.04	SC_ACC.05		
	Employee and Supplier Security and Integrity	SC_ESS.01	SC_ESS.02	SC_ESS.03	SC_ESS.04	SC_ESS.05		
	Business Partner Security	SC_BPS.01	SC_BPS.02	SC_BPS.03				
	Supply Chain Security Training	SC_STR.01						
	Information Systems Security	SC_ISS.01						
	Trusted Technology Components	SC_TTC.01	SC_TTC.02	SC_TTC.03	SC_TTC.04			
	Secure Transmission and Handling	SC_STH.01	SC_STH.02	SC_STH.03	SC_STH.04	SC_STH.05	SC_STH.06	SC_STH.07
	Open Source Handling	SC_OSH.01	SC_OSH.02	SC_OSH.03	SC_OSH.04			
	Counterfeit Mitigation	SC_CTM.01	SC_CTM.02	SC_CTM.03	SC_CTM.04			
	Malware Detection	SC_MAL.01	SC_MAL.02					

Example Category Comparison

U.S. Executive Order 14028 Supply Chain Security Risk Areas	O-TTPS / ISO 20243 Standard		
	Product Dev	Secure Eng	Supply Chain Security
Secure Software Development	X	X	
Automated tools/processes		X	
Data Encryption		X	X
Internal and third-party controls on SW			X
SBOM	X		
Vulnerability Management and Disclosure	X	X	X
Document Artifacts	X		
Open-Source SW Integrity			X

O-TTPS / ISO 20243 Requirements

Example of category detail

Area	Category / Attribute
Technology Development	**Product Development**
	Product Design Process
	Configuration Management
	Development Process and Practices
	Quality and Test Management
	Product Sustainment Management
	Secure Engineering
	Threat Analysis and Mitigation
	Run-time Protection Techniques
	Vulnerability Analysis and Response
	Product Patching and Remediation
	Secure Engineering Practices
	Monitor and Assess the Impact of Changes in the Threat Landscape

Category Definition:

Secure Engineering Practices

- Secure engineering practices are established to avoid common engineering errors that lead to exploitable product vulnerabilities.

Each element has a similar description and further item detail per the O-TTPS requirements file

Category: O-TTPS Secure Engineering Practices

Example of item detail and evidence description

SE_SEP.01 Required: Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabilities. For example, user input validation, use of appropriate compiler flags, etc.

SE_SEP.02 Required: Secure hardware design practices (where applicable) shall be employed. For example, zeroing out memory and effective opacity.

SE_SEP.03 Required: Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.

Category: O-TTPS Secure Engineering Practices

Example of item detail and evidence description

SE_SEP.01 Required: Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabilities. For example, user input validation, use of appropriate compiler flags, etc.

Process Evidence: Product development process
Implementation Evidence: Acceptable coding patterns, results from tooling that enforces coding patterns, results from manual code reviews, minimize footprint

SE_SEP.02 Required: Secure hardware design practices (where applicable) shall be employed. For example, zeroing out memory and effective opacity.

Process Evidence: Product design process
Implementation Evidence: Evidence that design practices are implemented such as: results from tooling that enforce secure design practices, results from manual review of the application of secure design practices, design accounts for things like: tagging, tamper detection, deployment of anti-counterfeit technology

SE_SEP.03 Required: Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.

Process Evidence: Training process
Implementation Evidence: Evidence that training has been provided such as training artifacts; for example, training certificates, Computer-Based Training (CBT), training attendance statistics

IBM Secure Engineering Practices

- IBM Global Offering Management Discipline and Secure Release process must be followed to ensure all required product deliverables are met
  - Security and Privacy by Design (SPbD) reviews are performed by product Subject Matter Experts and Business unit Information Security Office leaders
- IBM Secure Lifecycle process consists of
  - Secure Design, Secure Release, Secure Checkup, and Secure Transition
- Annual education is required for all appropriate personnel
  - Security and Privacy by Design for Developers and Offering managers
  - Specialized Certified Ethical Hacker training
  - Digital Badges can also be achieved

O-TTPS Certification Program

The Open Group Open Certified

Self-Assessed
Open Trusted Technology Provider™ V1
O-TTPS 1.1.1 (ISO/IEC 20243:2018)

- O-TTPS Self-Assessed or Third-Party Assessed
  - Organization prepares for / conducts either Self-Assessment or selects an O-TTPS Recognized Assessor
  - Complete the Conformance Statement (Scope of Certification)
  - Register for Certification and pay Certification Fee
  - Submit the Conformance Statement to *The Open Group*
  - Sign / submit Certification and Trademark License Agreements
- Certification Authority reviews applicant submission
- Certification Awarded or clarification questions may be asked

Reference: https://ottps-cert.opengroup.org/

O-TTPS Certification Benefits

The Open Group Open Certified

Self-Assessed
Open Trusted Technology Provider™ V1
O-TTPS 1.1.1 (ISO/IEC 20243:2018)

- O-TTPS / ISO 20243 provides value
  - International standard demonstrates conformance
  - Assurance of best practices through the product lifecycle, including supply chain
  - Clients (Federal, Banking, Utilities) requesting product supply chain integrity assurance
  - O-TTPS certification provides collateral to satisfy these integrity assurance questions
- Certification reduces cyber security risks

Conclusions

- Cybersecurity concerns increasing
- Federal security requirements increasing
- Risk management programs critical
- Clients demanding supplier risk assessments
- Industry standards drive best practices
- Certification to industry standards can provide collateral to address client inquiries

Closing

- Acknowledgements
  - Many additional members of Supply Chain Engineering, Systems BISO and IBM CISO contributed to this content
  - Thanks also to all the IBM suppliers partnering to improve security

Christine Bunke is a senior engineer in the IBM Systems Supply Chain Engineering (SCE) group. Currently she is in IBM's Supply Chain Engineering ECAT team in the role of a Technology Qualification Engineer. She leads teams globally to apply the IBM PCBA qualification specifications to new contract manufacturing suppliers. She represents IBM supply chain as a member of the SC Cybersecurity team.

Warren Grunbok is an IBM Systems STSM reporting to the Systems Business Security Information Officer (BISO). In his role as a security architect, he is responsible for the secure development lifecycle program within Systems which applies to over 400 products and covers various standards initiatives including O-TTPS, Common Criteria, and a number of NIST standards.