SBOM Regulations

August 7, 2023

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Preface

- This slide deck was modified during the meeting and reflects both the original content as well as additions and feedback given.

Current SBOM Regulation

- EO 14028 Improving the Nation’s Cybersecurity

- NIST Secure Software Development Framework (SSDF) Version 1.1
- National Cybersecurity Strategy 2023
- “U.S. Cyber Trust Mark”

STANDARD / GUIDE NAME	NUMBER
IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities	IEEE 1686-2013
IEEE Standard for System, Software, and Hardware Verification and Validation	IEEE 1012-2016
Quality Management Systems Family of Standards	ISO 9000
Quality Management Systems- Requirements	ISO 9001:2015
Software Engineering – Guidelines for the application of ISO 9001:2015 to computer software	ISO/IEC/IEEE 90003
Information Technology- Programming Languages- Guidance to avoiding vulnerabilities in programming languages through language selection and use	ISO/IEC TR 24772
Guide to Computer Security Log Management	NIST SP 800-92
Guide to Industrial Control Systems (ICS) Security	NIST SP 800-82
Supply Chain Risk Management Practices for Federal Information	NIST SP 800-161
Verification and Test Methods for Access Control Policies/Models	NIST SP 800-192
Cyber Security- Supply Chain Risk Management	CIP-013-1
Cyber Security- Configuration Change Management and Vulnerability Assessments	CIP-010
Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components	ISA 62443
Technical Guide to Information Security Testing and Assessment	NIST SP 800-115
Security and Privacy Controls for Industrial Systems and Organizations	NIST 800-53
Pipeline SCADA Security	API 1164
NERC Cyber Security Standards	CIP 5, 7, 9, 10, 11, 13
Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC 27001:2013
IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques	ISO/IEC 20085-1:2019
Cyber Security Procurement Language for Control Systems	DHS/DOE
Contractors' Counterfeit Electronic Part Detection and Avoidance Systems	DFARS 246.870
Investigation for Software Cybersecurity for Network-Connectable Products ... for Industrial Control Systems	UL 2900-2-2
NIST Cyber Security Framework	NIST Cybersecurity Framework (CSF)
Contingency Planning Guide for Federal Information Systems	NIST SP 800-34 Rev. 1
Guide for Conducting Risk Assessments	NIST SP 800-30 Rev. 1
Managing Information Security Risk: Organization, Mission, and Information System View	NIST SP 800-39
IEEE Standard for SCADA and Automation Systems	IEEE Std C37.1™
IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications	IEEE Std C37.238™
Guidelines on Firewalls and Firewall Policy	SP 800-41 Rev. 1
"Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry"	INGAA Control Systems Cyber Security Guidelines
"Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan"	AGA Report No. 12
"ISMS Family of Standards"	ISO/IEC 27000
TSA “Pipeline Security Guidelines”	TSA PSG
TSA "Enhancing Pipeline Cybersecurity"	Security Directive Pipeline-2021-01
Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	ONG-C2M2
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)	ES-C2M2, SD2M2

Questions for the Group

1. More regulations/guidance/policy! (please send to Jess@pnnl.gov)

Green/Blue UAS Drone Regs https://www.auvsi.org/green-uas

IEC 62443 4-1

NIST IR 8406 - add to watch this space list

Feedback:

Standards vs Regulations vs Policy – much prefer industry-defined standards, rather than regulations. Use Case focused

Questions for the Group

2. Where *should* SBOM go?
    - Software Design Processes
    - QC/QA
    - Supply Chain
    - Vulnerability Assessments
    - Other?

Questions for the Group

3. Next Steps
    - Tools and how they tie in to the standards
        - Black Duck, Jfrog Xray, Synk, Gitlab Ultimate, and many more
    - Use Case Definitions