Software Bill of Materials Related Efforts

NTIA Multistakeholder Process on Software Component Transparency
Awareness & Adoption Working Group
2021-10-29

The following collection enumerates initiatives, guidance, models, frameworks, and reports that explicitly or implicitly highlight the value of Software Bill of Materials (SBOM).[1] This list was compiled as part of the National Telecommunications and Information Administration (NTIA) Multistakeholder Process on Software Component Transparency.[2]

[1] For more information on Software Bill of Materials, see www.ntia.gov/SBOM.
[2] NTIA Software Component Transparency https://www.ntia.gov/SoftwareTransparency.

Table of Contents

Introduction 3
Projects Related to SBOM 3
Atlantic Council “Breaking Trust” Report 3
BSA Framework for Secure Software 3
Building Security in Maturity Model 4
CISQ Trustworthy System Manifesto 4
Cybersecurity Maturity Model Certification (CMMC) 4
Digital Bill of Materials 5
Edison Electric Institute – Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk 5
ENISA – European Cybersecurity Certification Scheme for Cloud Services 6
ENISA – Guidelines for Securing the Internet of Things 6
FDA Premarket Guidance 6
FS-ISAC Third-Party Governance 7
International Organization for Standardization (ISO) 7
ISO/IEC 27001 and 27002 – Information Security Management and Code of Practice for Information Security Controls 7
ISO/IEC 5230:2020 – OpenChain Specification 7
ISO/SAE 21434 – Road Vehicles - Cybersecurity Engineering 8
Joint Security Plan 8
Linux Foundation Open Source Security Foundation 8
Manufacturer Disclosure Statement for Medical Device Security 8
MITRE Deliver Uncompromised 9
Manufacturer Usage Description 9
NERC CIP-013 9
National Cyber Security Centre (NCSC) – Using the Software Bill of Materials for Enhancing Cybersecurity 9
National Highway Traffic Safety Administration – Cybersecurity Best Practices for the Safety of Modern Vehicles 10
NIST’s Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) 10
Open Command and Control 10
OWASP Component Analysis Project 10
OWASP Software Component Verification Standard 11
SAFECode Managing Security Risks Inherent in the Use of Third party Components 11
Software Heritage 11
UL 2900-1 – Standard for Software Cybersecurity for Network-Connectable Products 12
United Nations Economic Commission for Europe WP.29 / R155 12

Introduction

The work of this public, NTIA-convened initiative does not occur in a vacuum. A number of key works across the ecosystem have advanced or highlighted the importance of an SBOM at various points in the supply chain. The following is a list of related projects that are included to emphasize the growing use, support and importance of SBOMs. It is not an exhaustive list and the projects below are not endorsed by this group. An earlier version of this list was included in "Roles and Benefits of SBOM Across the Supply Chain" as "Appendix I - Related Efforts That Explicitly or Implicitly Highlight the Value of SBOM."[3]

Projects Related to SBOM

Atlantic Council "Breaking Trust" Report

The Breaking Trust[4] project evaluates a dataset of 138 software supply chain attacks and vulnerability disclosures collected from public reporting over the past 10 years to show that software supply chain attacks are popular, impactful, and used to great effect by states. The report argues that SBOM is one of many useful tools to establish trust and better secure our software supply chains and recommends that National Institute of Standards and Technology (NIST) and NTIA should integrate the draft SBOM standards developed by the NTIA multistakeholder process and continue to evangelize on the role and utility of software transparency through continued stakeholder engagement.

BSA Framework for Secure Software

This industry-drafted framework[5] from The Software Alliance (BSA) offers guidance on secure development of software, security capabilities of the software, and a secure lifecycle, citing standards and other authoritative guidance. It makes repeated references to the importance of tracking third-party code, advising it "to the maximum feasible through the use of manual and automated technologies, subcomponents integrated into third party components are documented, and their lineage and dependencies traced."

---

[3] Roles and Benefits for SBOM Across the Supply Chain https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf.
[4] Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/.
[5] The BSA Framework for Secure Software https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf.

Building Security in Maturity Model

Building Security in Maturity Model (BSIMM) is a large group of software developers in academia, government, and industry that benchmarks best practices in software development. The group creates practices that organizations can use as benchmarks and assess where they are relative to their peers in their industry or overall. Version 11 of the BSIMM[6] contains several SBOM-related requirements:

> SR2.4 “Identify open source”
> SR3.1 “Control open source risk”
> CMVM2.3 “Develop an operations inventory of applications”
> SFD3.2 “Require use of approved security features and frameworks”
> SE3.6 “Enhance application inventory with operations bill of materials”

CISQ Trustworthy System Manifesto

The Council on IT Software Quality (CISQ) has published the “CISQ Trustworthy System Manifesto”[7] on holding senior executives accountable for cybersecurity. Section III is “Traceable Properties of System Components,” which includes requirement #2, “Evidence of provenance and trustworthiness should be carried forward with components and shared across the supply chain.” The description includes:

> *“When developers incorporate open source components, external APIs, or microservices, they should document their source and related data for inclusion in a System Bill of Materials (SBOM)."*

Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) framework[8] was created “in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the U.S. Department of Defense (DoD) supply chain.” The CMMC Framework builds upon the NIST SP 800–171 DoD Assessment Methodology by adding “a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.” For each CMMC level, the associated sets of maturity processes and cybersecurity best practices, drawn from multiple references and standards, are cumulative and “demonstrate a progression of cybersecurity maturity.” CMMC will apply to all DoD solicitations and contracts, except those for commercially available off-the-shelf (“COTS”) items, starting on or after October 1, 2025.

CMMC touches on SBOM through references and guidance around Asset Management (AM.4.226) and Configuration Management (CM.2.061 and CM.5.074).

[6] BSIMM11 https://www.bsimm.com/content/dam/bsimm/reports/bsimm11.pdf.
[7] CISQ Trustworthy System Manifesto https://www.it-cisq.org/trustworthy-systems-manifesto/index.htm.
[8] CMMC Framework https://www.acq.osd.mil/cmmc/.

Digital Bill of Materials

The Digital Bill of Materials (DBoM)[9] Consortium and technology were created to develop an instrumented infrastructure for supply chain attestation sharing. This attestation structure consists of DBoM Nodes which act as gateways to attestation repositories. SBOMs are critical attestations regarding composition of software artifacts and therefore are implicitly necessary for supply chain security stakeholders. Machine readable content and provenance attestations regarding software components will greatly increase organizations' ability to plan for and respond to malicious or accidental vulnerabilities to and/or exploitations of cybernetic supply chains. SBOMs are expected to populate attestation channels – policy-based repositories between supply chain partners – alongside attestations regarding known relevant vulnerabilities, hardware BOMs, custody, handling, and/or other critical data determined by supply chain partners as necessary to provide appropriate, actionable transparency.

Edison Electric Institute – Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

To facilitate managing cybersecurity supply chain risks, a committee of representatives of Edison Electric Institute (EEI) member companies developed this model procurement contract language[10] to align cybersecurity requirements and to encourage adoption by the vendor community. Recognizing the importance of procurement in managing supply chain risk, the member companies who developed the model focused on the processes required by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) supply chain risk management reliability standard – CIP-013-1 Requirement 1, Part 1.2 – and also included language that goes beyond this requirement with the goal of improving cybersecurity. The model is a starting point for negotiations with vendors and service providers. It should not be considered a best practice or requirement, has not yet been tested by vendors and service providers, and can be adopted/adjusted as appropriate. Version 2.0 includes revisions to reflect evolving industry practices, including changes that broaden references to specific industry standards, adjust notification timeframes and other time-specified requirements, and modify language where appropriate to support use with value-added resellers. Additional updates were made to clarify existing concepts, such as SBOM from software vendors.

[9] DBOM Project https://github.com/DBOMproject.
[10] Edison Electric Institute – Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf.

ENISA – European Cybersecurity Certification Scheme for Cloud Services

Article 51(d) of the European Union Cybersecurity Act (EUSCA) has identified as a security objective the identification and documentation of known dependencies and vulnerabilities. To help support that, supply chain transparency is identified in several European Union Agency for Cybersecurity (ENISA) standards.

The ENISA European Cybersecurity Certification Scheme for Cloud Services (EUCS)[11] supports three assurance levels: Basic, Substantial, and High. The security requirements for cloud services increase with assurance levels in several dimensions: scope, rigor, and depth. Assurance level Basic should be suitable for cloud services that are designed to meet typical security requirements for non-critical data and systems. Assurance level Substantial should be suitable for cloud services that are designed to meet typical security requirements for business-critical data and systems. Assurance level High should be suitable for cloud services that are designed to meet specific (exceeding level Substantial) security requirements for mission-critical data and systems.

ENISA – Guidelines for Securing the Internet of Things

ENISA created security guidelines[12] for the whole Internet of Things (IoT) lifespan: from requirements and design, to end use delivery and maintenance, as well as disposal. IoT supply chain security is of paramount importance to a holistic approach to IoT security. IoT security needs to be considered at all stages of the supply chain, from the early conceptual design to the end user delivery and maintenance. One of the suggested good practices for IoT Supply Chain Security is SBOMs for IoT devices. SBOMs increase visibility into the product and enable both the manufacturer and external users to check for known vulnerabilities and validate the device from a security standpoint, helping to reduce the gaps that enable attackers to successfully leverage a vulnerability for malicious purposes. Increased product visibility may also lead to increased trust between actors of the supply chain.

FDA Premarket Guidance

The U.S. Food and Drug Administration (FDA) has published draft Pre-Market Guidance[13] for medical device manufacturers seeking FDA certification. This guidance maintains that: “The device design should provide a CBOM in a machine readable, electronic format to be consumed automatically” where Cybersecurity Bill of Materials (CBOM) is defined as “a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities.”

[11] ENISA EUCS - Cloud Services Scheme https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/.
[12] ENISA Guidelines for Securing the Internet of Things https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain.
[13] FDA Cybersecurity Guidance and Safety Communications https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#guidance.

FS-ISAC Third-Party Governance

The Financial Services Information Sharing and Analysis Center (FS-ISAC) published "Appropriate Software Security Control Types for Third Party Service and Product Providers" in 2015. It includes Control Type 3B, "A Bill of Materials (BOM) for Commercial Software to Identify Open Source Libraries Used."[14]

International Organization for Standardization (ISO)

ISO/IEC 27001 and 27002 – Information Security Management and Code of Practice for Information Security Controls

ISO/IEC 27001:2013[15] specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. Specifically Sections 5 and 6 highlight the requirements of software resources transparency to adequately assess the environment under considerations. The supporting guidelines in ISO/IEC 27002:2013[16] provides recommendations in Sections 5, 9, 10, and 14 on areas of concern where an organization will utilize SBOM to meet many of these recommendations. There are also a number of industry specific ISO standards, such as 13485 (Healthcare) and 16949 (Automotive), that adapt these standards to industry specific guidelines with a view into software quality and provide safe software systems for these specific industrial sectors.

ISO/IEC 5230:2020 – OpenChain Specification

The Linux Foundation OpenChain[17] project is an ISO Standard[18] on the use of open source and contains: "A process exists for creating and managing a FOSS component bill of materials which includes each component (and its Identified Licenses) from which the Supplied Software is comprised."

[14] Financial Services ISAC Third Party Software Security Working Group. "Appropriate Software Security Control Types for Third Party Service and Product Providers" Version 2.3 was published in October, 2015. https://www.fsisac.com/.
[15] ISO/IEC 27001:2013 – Information Security Management - Requirements https://www.iso.org/standard/54534.html.
[16] ISO/IEC 27002:2013 – Code of Practice for Information Security Controls https://www.iso.org/standard/54533.html.
[17] OpenChain Specification Version 2 https://wiki.linuxfoundation.org/_media/openchain/openchainspec-current.pdf.
[18] ISO/IEC 5230:2020 – OpenChain Specification https://www.iso.org/standard/81039.html.

ISO/SAE 21434 – Road Vehicles - Cybersecurity Engineering

Among the many ISO standards is 21434,[19] "Road Vehicles - Cybersecurity Engineering," created jointly with the Society of Automotive Engineers (SAE) in the U.S. Expected publication is in early 2021. The standard provides guidance for the auto industry in complying with a number of emerging requirements in cybersecurity, including UNECE WP.29 R155, and has a particular focus on risk assessment and management. The standard does not explicitly mention SBOM, but it does cover the related topic of vulnerability management. ISO/SAE 21434 is compatible with SBOM as envisioned by the NTIA but does not require it.

Joint Security Plan

The Joint Security Plan (JSP)[20] was drafted by healthcare stakeholders to address cybersecurity challenges in healthcare. One objective was to create a framework and voluntary guidance for medical devices and healthcare IT, including ways for smaller medical device manufacturers and healthcare delivery organizations to implement cybersecurity in their environments. The JSP addresses risk for end-of-life products, promotes transparency, and provides consistent and secure product development practices. The JSP includes SBOMs as part of third-party security assessments and customer security documentation for improving supply chain security and vigilance.

Linux Foundation Open Source Security Foundation

Open source software that ultimately reaches end users has a chain of contributors and dependencies and it is important that those responsible for their user or organization's security are able to understand and verify the security of this dependency chain. The Open Source Security Foundation (OpenSSF)[21] initiative will focus on: Vulnerability Disclosures, Security Tooling, Security Best Practice, Identifying Security Threats to Open Source Projects, Securing Critical Projects, and Digital Identity Attestation.

Manufacturer Disclosure Statement for Medical Device Security

The Manufacturer Disclosure Statement for Medical Device Security (MDS2)[22] was originally developed by the Healthcare Information and Management Systems Society (HIMSS) and the American College of Clinical Engineering (ACCE), and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association (NEMA). The MDS^2 form provides medical device manufacturers with a means for disclosing to healthcare providers the security related features of the medical devices they manufacture.

---

[19] ISO/SAE 21434– Road Vehicles - Cybersecurity Engineering https://www.sae.org/standards/content/iso/sae21434.d1/.
[20] The Joint Security Plan (JSP) https://healthsectorcouncil.org/the-joint-security-plan/.
[21] Open Source Security Foundation https://openssf.org/.
[22] Manufacturer Disclosure Statement for Medical Device Security https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx.

MITRE Deliver Uncompromised

MITRE, in its report on the national security supply chain, "Deliver Uncompromised"[23] recommends SBOMs as part of supply chain integrity. It notes, "If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements." A 2021 followup report on "Securing Critical Software Supply Chains" explicitly focused on software, and gave more attention to the benefits of SBOM in particular.[24]

Manufacturer Usage Description

One of the challenges that deployments are likely to face is how to locate an SBOM. Manufacturer Usage Description (MUD)[25] is a standardized discovery mechanism that provides manufacturers an opportunity to provide computer-readable declarations about their products, such as the manufacturer and model of a device, as well as what access that device needs to function correctly. An extension to MUD is now being developed that would provide manufacturers the opportunity to make such statements as, "The SBOM can be found at the following URL on the Internet" or "The SBOM can be found on the device in the following way." This permits security management systems to automatically discover the SBOM.

NERC CIP-013

North American Electric Reliability Corporation Critical Infrastructure Protection Standard 013 (NERC CIP-013)[26] is a standard for supply chain cybersecurity of systems that is used to control the Bulk Power System in the US and Canada. It requires the electric utility to "identify and assess" supply chain cybersecurity risks and mitigate the most important of those. It does not require that any specific risks be identified or mitigated, just those that the utility decides are most significant. One of the most important supply chain cyber risks is the risk posed by unpatched vulnerabilities in software components. An SBOM would enable an organization to identify the components installed in their environment, and then the vulnerabilities that apply to them.

National Cyber Security Centre (NCSC) – Using the Software Bill of Materials for Enhancing Cybersecurity

The Dutch government's National Cyber Security Centre (NCSC) recognizes the importance that SBOMs play in the software supply chain. In a white paper published in January 2021 titled "Using the Software Bill of Materials for Enhancing Cybersecurity,"[27] NCSC provides an overview of the state of SBOMs, their importance and potential impact in the software supply chain, and guidance and recommendations for SBOM security use cases.

---

[23] Deliver Uncompromised https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.
[24] Deliver Uncompromised - Securing Critical Software Supply Chains https://www.mitre.org/publications/technical-papers/deliver-uncompromised-securing-critical-software-supply-chains.
[25] Manufacturer Usage Description Specification https://www.rfc-editor.org/rfc/rfc8520.html.
[26] NERC CIP-013 https://www.nerc.com/pa/Stand/Pages/CIP0131RI.aspx.
[27] NL NCSC Using the Software Bill of Materials for Enhancing Cybersecurity https://english.ncsc.nl/research/publications/publications/2021/february/4/using-the-software-bill-of-materials-for-enhancing-cybersecurity.

National Highway Traffic Safety Administration – Cybersecurity Best Practices for the Safety of Modern Vehicles

The National Highway and Traffic Safety Administration (NHTSA), a part of the U.S. Department of Transportation, is the primary agency in the U.S. government charged with ensuring motor vehicle safety. NHTSA is one of several regulators for the automotive industry, and also offers safety guidance and assistance to all levels of government, industry, academia, and individual citizens.

NHTSA recognizes the importance of cybersecurity to safety in modern vehicles, and publishes voluntary guidance in the paper "Cybersecurity Best Practices for the Safety of Modern Vehicles."[28]. The 2020 draft version of this document includes section 4.2.6, "Inventory and Management of Software Assets on Vehicle," which describes the use of SBOM and mentions the term "SBOM" explicitly in a footnote. It is fully compatible with NTIA recommendations.

NIST's Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

A NIST 2020 white paper[29] recommends a core set of high level secure software development practices. Among these, it recommends that organizations seeking to protect their software "Create and maintain a software bill of materials (SBOM) for each software package created."

Open Command and Control

Open Command and Control (OpenC2)[30] is a standardized language for the command and control of technologies that provide or support cyber defenses. By providing a common language for machine-to-machine communication, OpenC2 is vendor and application agnostic, enabling interoperability across a range of cyber security tools and applications. The use of standardized interfaces and protocols enables interoperability of different tools, regardless of the vendor that developed them, the language they are written in, or the function they are designed to fulfill. OpenC2 has commands to obtain SBOMs from devices, as well as commands to act on the results from analyzing the SBOM.

OWASP Component Analysis Project

The Open Web Application Security Project (OWASP) industry expert group's guidance on component analysis[31] includes the recommendation: "Contractually require SBOMs from vendors and embed their acquisition in the procurement process" as well as a list of best practices using the SBOM to improve security.

---

[28] NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles https://www.federalregister.gov/documents/2021/01/12/2021-00390/cybersecurity-best-practices-for-the-safety-of-modern-vehicles.

[29] NIST White Paper: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final.

[30] OpenC2 https://openc2.org/.

[31] OWASP Component Analysis https://owasp.org/www-community/Component_Analysis#software-bill-of-materials-sbom.

OWASP Software Component Verification Standard

The Software Component Verification Standard (SCVS)[32] is a community-driven effort to establish a framework for identifying activities, controls, and best practices, which can help in identifying and reducing risk in a software supply chain. SCVS is designed to be implemented incrementally, and to allow organizations to phase in controls at different levels over time.

SAFECode Managing Security Risks Inherent in the Use of Third party Components

Industry group SAFECode drafted a white paper[33] capturing the collective knowledge on the benefits and challenges of managing third-party code risk in product development, with an explicit emphasis on the importance of tracking third-party code via a bill of materials.

Software Heritage

Software Heritage[34] is a non-profit initiative actively supported by a large number of organizations[35] – software, systems and tool vendors, IT users, academic and governmental institutions. It is building a universal archive of software source code, as a common infrastructure catering to a variety of use cases from industry to science and culture. One of the use cases specifically listed on their mission statement is source code tracking for industry:[36]

> "*Because industry cannot afford to lose track of any part of its source code, we track software origin, history, and evolution. Software Heritage will provide unique software identifiers, intrinsically bound to software components, ensuring persistent traceability across future development and organizational changes.*"

These intrinsic identifiers are based on cryptographic signatures, have a precise formal definition,[37] and are already available for the more than 10 billions of artifacts stored in the Software Heritage archive.[38] They are an essential building block for ensuring the integrity of a source code base, are recognized by the Wikidata community,[39] and are currently being used by some major industry players to implement a part of their SBOM workflow related to source code distribution obligations.[40]

---

[32] OWASP Software Component Verification Standard https://owasp.org/scvs.
[33]SAFECode White Paper: Managing Security Risks Inherent in the Use of Third-Party Components https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.
[34] Building the Universal Archive of Source Code https://cacm.acm.org/magazines/2018/10/231366-building-the-universal-archive-of-source-code/abstract.
[35] Software Heritage Testimonials https://www.softwareheritage.org/support/testimonials/.
[36] Software Heritage Mission Statement: An Essential Infrastructure for Industry https://www.softwareheritage.org/mission/industry/.
[37] Software Heritage: Persisten Identifiers https://docs.softwareheritage.org/devel/swh-model/persistent-identifiers.html
[38] Software Heritage: Archive https://archive.softwareheritage.org.
[39] SWH Release ID https://www.wikidata.org/wiki/Property:P6138.
[40] Outsourcing Source Code Distribution Requirements https://archive.fosdem.org/2018/schedule/event/outsourcing_distribution_requirements/.

UL 2900-1 – Standard for Software Cybersecurity for Network-Connectable Products

UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products[41] section 4.1.1 c states that vendors shall provide a list of all executables and libraries in the product – including third-party – and list by name and version along with guidance regarding operating system features and libraries. Section C states, "An equivalent software bill of materials – i.e., a list of the contents of the software – can be substituted."

United Nations Economic Commission for Europe WP.29 / R155

The United Nations Economic Commission for Europe (UNECE) sponsors Working Party 29 (WP.29)[42] with a mission to ensure multinational harmonization of technical standards for vehicles. Though the WP.29 automotive work does not apply to all countries, due to the nature of global markets, the standards are observed by nearly all of the auto industry in nearly all markets.

UN Regulation No. 155 (R155)[43,44] is one of many regulations issued under WP.29, and provides broad guidance for minimal acceptable practices for cybersecurity in vehicle technology, and also requires a "cyber security management system." R155 does not explicitly describe or require SBOM or similar functions but is compatible with NTIA recommendations.

[41] UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-1.
[42] UNECE WP.29 https://unece.org/wp29-introduction.
[43] UN Regulation No.155, Cyber Security and Cyber Security Management System https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.
[44] Proposal for the Interpretation Document for UN Regulation No. [155] https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-182-05e.pdf.