The following published standards and guidance materials were identified in the three breakout groups or otherwise during the workshop as useful for the ME sector. This listing is separate from and will be integrated into the next iteration of the [**Microelectronics Standards Landscape**](https://share.ansi.org/Shared%20Documents/Standards%20Activities/Microelectronics%20Supply%20Chain%20Security/July%2027-29%2C%202022%20Workshop/ANSI_Microelectronics_Standards_Landscape%20%28RFI%20Form%202022%29.xlsx) that resulted from the request for information (RFI).

1. [Accellera SA-EDI Standard 1.0. Security Annotation for Electronic Design Integration](https://accellera.org/images/downloads/standards/Accellera_SA-EDI_Standard_v10.pdf)
2. [CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems](https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf)
3. [DHS CISA ICT SCRM Task Force: CISA Vendor SCRM template](https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf)
4. [DHS CISA ICT SCRM Task Force: ICT SCRM TF Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists](https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf)
5. [DoD Cybersecurity Maturity Model Certification (CMMC)](https://www.acq.osd.mil/cmmc/)
6. [DoD Defense Acquisition University (DAU) COTS Assembly Checklist, developed by the Parts Management Working Group](https://www.dau.edu/cop/PMKSP/Lists/COTS_Checklist/AllItems.aspx)
7. [DoD MIL-PRF-38535K, Performance Specification: Integrated Circuits (Microcircuits) Manufacturing, General Specification For (20-Dec-2013)](http://everyspec.com/MIL-PRF/MIL-PRF-030000-79999/MIL-PRF-38535K_48842/)
8. [DoDI 5000.83 Technology and Program Protection to Maintain Technological Advantage](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf)
9. [DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf)
10. [EASA CM-SWCEH-001 Development Assurance of Airborne Electronic Hardware](https://www.easa.europa.eu/en/document-library/product-certification-consultations/easa-cm-swceh-001)
11. [EASA COTS-AEH – Use of complex COTS (Commercial-Off-The-Shelf) in airborne electronic hardware – failure mode and mitigation](https://www.easa.europa.eu/en/downloads/16938/en)
12. [IEEE 1735-2014 - Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)](https://standards.ieee.org/ieee/1735/4358/)
13. [IPC-1782A - Standard for Manufacturing and Supply Chain Traceability of Electronic Products](https://shop.ipc.org/general-electronics/standards/1782-0-a-english)
14. [IPC-1791 B](https://shop.ipc.org/automotive-general-electronics-medical-space-and-defense/standards/1791-0-b-english): [IPC-1791B: Trusted Electronic Designer, Fabricator and Assembler Requirements](https://shop.ipc.org/automotive-general-electronics-medical-space-and-defense/standards/1791-0-b-english)
15. [ISO 13485:2016: Medical devices — Quality management systems — Requirements for regulatory purposes](https://www.iso.org/standard/59752.html)
16. [ISO 26262-1:2018: Road vehicles — Functional safety — Part 1: Vocabulary](https://www.iso.org/standard/68383.html)
17. [ISO 28000:2022: Security and resilience — Security management systems — Requirements](https://www.iso.org/standard/79612.html)
18. [ISO 9001:2015: Quality management systems — Requirements](https://www.iso.org/standard/62085.html)
19. [ISO/IEC 15026-2:2011: Systems and software engineering — Systems and software assurance — Part 2: Assurance case](https://www.iso.org/standard/52926.html)
20. [ISO/IEC 17000 Conformity assessment- Vocabulary and general principles](https://www.iso.org/standard/73029.html)
21. [ISO/IEC 19790:2012: Information technology — Security techniques — Security requirements for cryptographic modules.](https://www.iso.org/standard/52906.html)*\*Note will be replaced by ISO/IEC WD 19790.3: Information technology — Security techniques — Security requirements for cryptographic modules*
22. [ISO/IEC 20243-1:2018: Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations](https://www.iso.org/standard/74399.html)
23. [ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes](https://www.iso.org/standard/63711.html)
24. [ISO/SAE 21434:2021: Road Vehicles – Cybersecurity Engineering](https://www.iso.org/standard/70918.html)
25. [JEDEC JEP30 Part Model Guidelines](https://www.jedec.org/category/technology-focus-area/jep30)
26. [NASA SEWP Standards Crosswalk: ISO 20243 & NIST 800-161](https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf)
27. [NASA Solution for Enterprise-Wide Procurement (SEWP) approved contractors list](https://www.sewp.nasa.gov/sewp5public/approvedcontractors)
28. [NIST FIPS 140-3: Security Requirements for Cryptographic Modules](https://csrc.nist.gov/publications/detail/fips/140/3/final)
29. [NIST FIPS 200: Minimum Security Requirements for Federal Information and Information Systems](https://csrc.nist.gov/publications/detail/fips/200/final)
30. [NISTIR 8419 Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives](https://csrc.nist.gov/publications/detail/nistir/8419/final)
31. NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
32. [NIST SP 800-160 Systems Security Engineering (SSE) Project](https://csrc.nist.gov/Projects/systems-security-engineering-project/publications)
33. [NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final)
34. [NIST SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final)
35. [NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities](https://csrc.nist.gov/publications/detail/sp/800-218/final)
36. [NSA U/OO/173659-22: DoD Microelectronics: Levels of Assurance Definitions and Applications](https://media.defense.gov/2022/Jul/14/2003034921/-1/-1/0/CTR_DOD_MICROELECTRONICS_LEVELS_OF_ASSURANCE_DEFINITIONS_AND_APPLICATIONS_20220714.PDF)
37. [RTCA DO-254 Design Assurance Guidance for Airborne Electronic Hardware](https://my.rtca.org/NC__Product?id=a1B36000001IcjUEAS)
38. [SAE AS5553D, Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition](https://www.sae.org/standards/content/as5553d/)
39. [SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors](https://www.sae.org/standards/content/as6081)
40. [SAE AS6171A, series of standards for Suspect/Counterfeit EEE Parts Detection](https://www.sae.org/standards/content/as6171a/)
41. [SAE AS6496, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution](https://www.sae.org/standards/content/as6496/)
42. [SAE AS9100D, Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations](https://www.sae.org/standards/content/as9100d/)
43. [SAE JA6678 Cyber Physical Systems Security Software Assurance](https://www.sae.org/standards/content/ja6678/)
44. [SAE JA6801 Cyber Physical Systems Security Hardware Assurance](https://www.sae.org/standards/content/ja6801/)
45. [SAE JA7496\_202206, Cyber-Physical Systems Security Engineering Plan (CPSSEP)](https://www.sae.org/works/documentHome.do?comtID=TEAG32&docID=JA7496_202206&inputPage=dOcDeTaIlS)
46. TIA QuEST Forum, [SCS 9001: Global Supply Chain Security Standard (Handbook)](https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/buy-handbook/)