



**IPC-1791C**

# **Trusted Electronic Designer, Fabricator and Assembler Requirements**

Developed by the Trusted Supplier Task Group (2-19b) of the  
Electronic Product Data Description Committee (2-10) of IPC

***Supersedes:***

IPC-1791B -  
August 2021  
IPC-1791-AM1 -  
March 2019  
IPC-1791 -  
August 2018  
IPC-1071B -  
April 2016  
IPC-1071A -  
August 2014  
IPC-1071 -  
December 2010  
IPC-1072-AM1 -  
March 2017  
IPC-1072 -  
December 2015

Users of this publication are encouraged to participate in the  
development of future revisions.

**Contact:**

IPC  
3000 Lakeside Drive, Suite 105N  
Bannockburn, Illinois  
60015-1249  
Tel 847 615.7100  
Fax 847 615.7105

# Table of Contents

<b>1</b>	<b>SCOPE</b> .....	1	1.6.13	Federal Bureau of Investigation (FBI) Channeler .....	3
1.1	Purpose and Background .....	1	1.6.14	Foreign Person .....	3
1.1.1	Source Technology and Capability .....	1	1.6.15	Information Technology (IT) .....	4
1.1.2	Interpretation of Requirements for the Purposes of this Standard .....	1	1.6.16	International Traffic in Arms Regulations (ITAR) Registered .....	4
1.1.3	Benefits of Using Organizations Certified to this Standard .....	1	1.6.17	Organization .....	4
1.1.4	Additional Detail .....	2	1.6.18	Personnel .....	4
1.2	Classification .....	2	1.6.19	Policy .....	4
1.3	Definition of Requirements .....	2	1.6.20	Printed Board Assembler .....	4
1.4	Certification .....	2	1.6.21	Printed Board and Assembly Design .....	4
1.4.1	Type 1 – Printed Board Design Organizations ..	2	1.6.22	Printed Board and Assembly Design Organization .....	4
1.4.2	Type 2 – Printed Board Fabrication Organizations .....	2	1.6.23	Printed Board Trusted Assembler .....	4
1.4.3	Type 3 – Printed Board Assembly Organizations .....	2	1.6.24	Printed Board Trusted Design Organization .....	4
1.4.4	Type 4 – Cable and Wire Harness Assembly Organizations .....	2	1.6.25	Printed Board Trusted Fabricator .....	4
1.4.5	Length of Certification .....	2	1.6.26	Procedure .....	4
1.4.6	Ownership Changes .....	2	1.6.27	Product-Specific Special Case .....	4
1.4.7	Management Changes .....	2	1.6.28	Quality .....	4
1.5	Abbreviations and Acronyms .....	2	1.6.29	Security .....	4
1.6	Terms and Definitions .....	3	1.6.30	Supply Chain Risk Management (SCRM) .....	4
1.6.1	Chain of Custody (ChoC) .....	3	1.6.31	Trust .....	4
1.6.2	Commercial and Government Entity (CAGE) Code .....	3	1.6.32	Trusted Source or Trusted Supplier .....	5
1.6.3	Confidentiality .....	3	1.6.33	Trusted Cable and Wire Harness Assembler .....	5
1.6.4	Controlled Technical Information .....	3	<b>2</b>	<b>APPLICABLE DOCUMENTS</b> .....	5
1.6.5	Controlled Unclassified Information (CUI) .....	3	2.1	IPC .....	5
1.6.6	Covered Contractor Information System .....	3	2.2	Joint Standards .....	5
1.6.7	Covered Defense Information .....	3	2.3	Center for Development of Security Excellence .....	5
1.6.8	Cyber Incident .....	3	2.4	National Institute of Standards and Technology (NIST) .....	5
1.6.9	Deemed Export .....	3	2.5	SAE International .....	5
1.6.10	Department of Defense (DoD) Prime Contractor .....	3	2.6	U.S. Department of Defense (DoD) .....	6
1.6.11	Department of State Proforma for Permanent Export (DSP-5) .....	3	2.6.1	Directives and Instructions .....	6
1.6.12	Export Administration Regulations (EAR) .....	3	2.6.2	Specifications .....	6
			2.7	U.S. House of Representatives Office of the Law Revision Council .....	6
			2.8	U.S. Office of the Federal Register - Code of Federal Regulations (CFR) .....	6

2.9	U.S. Office of the Federal Registrar – Defense Acquisition Regulation Supplement (DFARS) ..	6	3.4.4	Destruction of Scrap (In-Process or Finished Design Data, Layers and Panels, Subassemblies and Assemblies) .....	11
<b>3</b>	<b>REQUIREMENTS</b> .....	<b>6</b>	3.4.5	Repeat Orders .....	11
3.1	Quality Requirements .....	6	3.4.6	Shipping.....	11
3.1.1	Type 1 – Printed Board Design Organization ...	6	3.4.7	Training .....	11
3.1.2	Type 2 – Printed Board Fabrication Organization .....	7	3.5	Additional Chain of Custody (ChoC) Requirements for Type 1 Organizations .....	12
3.1.3	Type 3 – Printed Board Assembly Organization.	7	<b>4</b>	<b>EXPORT CONTROL COMPLIANCE</b> .....	<b>12</b>
3.1.4	Type 4 .....	7	4.1	Compliance with Export Control Laws .....	12
3.2	Supply Chain Risk Management (SCRM) Policy. ....	7	4.2	Export .....	12
3.2.1	Supplier Assessment. ....	7	4.3	Empowered Official .....	13
3.2.2	Outsource Process Suppliers .....	7	4.4	Export-Controlled Data on Portable Electronic Devices .....	13
3.2.3	Commercial and Government Entity (CAGE) Code/NATO Commercial and Government Entity (NCAGE) .....	7	<b>5</b>	<b>NIST SP 800-171 and CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) EXPLANATION</b> .....	<b>13</b>
3.3	Security .....	7	5.1	Compliance with NIST SP 800-171 Cybersecurity Regulations .....	13
3.3.1	Responsible Security Officer and Team .....	7	5.1.1	NIST SP 800-171 Scope.....	13
3.3.2	Personnel Security Requirements .....	8	5.1.2	Application of NIST SP 800-171 Requirements. ....	13
3.3.2.1	Nondisclosure Agreements (NDAs) .....	8	5.1.3	Families of Security Requirements .....	13
3.3.2.2	Background Checks .....	9	5.1.4	Cyber Incident Reporting.....	13
3.3.2.3	Citizenship. ....	9	5.2	Cybersecurity Maturity Model Certification (CMMC) Framework .....	13
3.3.2.4	Training .....	9	5.2.1	CUI Definition .....	13
3.3.3	Publication Approval .....	9	5.2.2	CMMC Requirements/Practices .....	13
3.3.4	Physical Protection .....	9	5.2.3	CMMC Certification .....	13
3.3.4.1	Reception Area .....	9	5.2.4	CMMC Implementation. ....	14
3.3.4.2	Information Processing .....	9	<b>6</b>	<b>REQUIREMENTS FOR TRUST CERTIFICATION OF NON-U.S. ELECTRONIC DESIGN, FABRICATION AND ASSEMBLY ORGANIZATIONS</b> .....	<b>14</b>
3.3.4.3	Data Center and Storage Areas .....	9	6.1	Certification .....	14
3.3.4.4	Perimeter Security, Entrances and Exits .....	9	6.1.1	Non-U.S. Organizations .....	14
3.3.4.5	Excluded Electronics .....	10	6.1.2	Length of Certification .....	14
3.3.4.6	Security Guards.....	10	6.1.3	Ownership or Management Change Notification .....	14
3.3.4.7	Foreign Person Access .....	10	6.1.4	Certification Duration .....	14
3.3.4.8	Removing Data from the U.S. ....	10	6.2	Security Requirements.....	14
3.3.4.9	Restricting Export-Controlled Data .....	10			
3.3.4.10	Visitors .....	10			
3.4	Chain of Custody (ChoC) for Type 1, 2, 3 and 4 Organizations .....	10			
3.4.1	Traceability Records.....	10			
3.4.2	Serialization and Identification .....	11			
3.4.3	Managing Sample Materials .....	11			



# IPC-1791C

## Trusted Electronic Designer, Fabricator and Assembler Requirements

---

### 1 SCOPE

This standard provides minimum requirements, policies and procedures for printed board design, fabrication, assembly, and cable and wire harness assembly organizations and/or companies to become trusted sources for markets requiring high levels of confidence in the integrity of delivered products. These trusted sources **shall** ensure quality, supply chain risk management (SCRM), security and chain of custody (ChoC).

Trusted source certification of non-U.S. printed board design, fabrication, assembly, and cable and wire harness assembly organizations requires a sponsor and to meet the requirements in Section 6, in lieu of section 3.3 and Section 4.

Cybersecurity Maturity Model Certification (CMMC) is scheduled to be fully implemented by the end of Fiscal Year 2025. The rollout starts gradually, accelerating in Fiscal Year 2023. During this period there will be instances in which a U.S. Department of Defense (DoD) supplier may not be required to meet CMMC but may be required to meet NIST SP 800-171 compliance. Therefore, this revision of IPC-1791 contains reference to CMMC, and Section 5 provides clarification on the relationship between CMMC and NIST SP 800-171.

Demonstration of the ability to meet and maintain the requirements of this standard as trusted design, fabrication, assembly, or cable and wire harness assembly organizations benefits customers that provide end-products for markets desiring a high level of integrity assurance (e.g., commercial, industrial, military, aerospace, automotive and medical).

In the context of this standard, the terms trust and trusted are used to reflect a commitment to product and process integrity assurance by printed board designers, fabricators, assemblers, and cable and wire harness assemblers. The user should not confuse this certification with defense-microelectronics-specific “Trusted Supplier” accreditation administered by the Defense Microelectronics Activity (DMEA) Trusted Access Program Office. IPC-1791 certification does not include DoD facility clearance unless compelled by customer-specific requirements and pursued independent of this standard.

**1.1.1 Source Technology and Capability** Design, fabrication, assembly, and cable and wire harness assembly organizations have different levels of capability in terms of technology, materials, product complexity, capacity and lead times. This standard assumes the customer has certified the capability of their chosen supplier.

**1.1.2 Interpretation of Requirements for the Purposes of this Standard** This standard covers requirements for quality, SCRM, security and ChoC:

- Quality and performance requirements (e.g., IPC-2200 series, IPC-6010 series, IPC-A-600, IPC-A-610, MIL-PRF-31032, AS9100, National Aerospace and Defense Contractors Accreditation Program Nadcap) **shall** be as defined in this standard for the type of organization.
- Requirements for SCRM **shall** be as defined in this standard for the type of organization.
- Security requirements **shall** be the same for all types of organizations.
- The requirements for ChoC **shall** be the same for all types of organizations.

**1.1.3 Benefits of Using Organizations Certified to this Standard** By using designers, printed board fabricators, printed board assemblers, and cable and wire harness assemblers that are certified to this standard, customers will be assured that their supplier(s):

- Maintains a quality system
- Maintains a SCRM system to ensure any threats related to disruption in supply are understood and managed
- Manages a security system to protect products and services from unauthorized access, particularly in support of export control
- Provides an ensured ChoC system for electronic and physical materials

**1.1.4 Additional Detail** See Appendix A for additional explanatory material.