

---

**GEA Mission**

The Global Electronics Association promotes industry growth and strengthens supply chain resilience.

**About IPC Standards by Global Electronics Association**

IPC standards and publications by Global Electronics Association are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. Existence of such standards and publications shall not in any respect preclude any entity from manufacturing or selling products not conforming to such standards and publications, nor shall the existence of such standards and publications preclude their voluntary use.

IPC standards and publications by Global Electronics Association are approved by committees without regard to whether the standards or publications may involve patents on articles, materials or processes. By such action, Global Electronics Association does not assume any liability to any patent owner, nor does Global Electronics Association assume any obligation whatsoever to parties adopting a standard or publication. Users are wholly responsible for protecting themselves against all claims of liabilities for patent infringement.

**Global Electronics Association Position Statement on Specification Revision Change**

The use and implementation of IPC standards and publications by Global Electronics Association are voluntary and part of a relationship entered into by customer and supplier. When a standard or publication is revised or amended, the use of the latest revision or amendment as part of an existing relationship is not automatic unless required by the contract. Global Electronics Association recommends the use of the latest revision or amendment.

**Standards Improvement Recommendations**

Global Electronics Association welcomes comments for improvements to any standard in its library. All comments will be provided to the appropriate committee.

If a change to technical content is requested, data to support the request is recommended. Technical comments to include new technologies or make changes to published requirements should be accompanied by technical data to support the request. This information will be used by the committee to resolve the comment.

To submit your comments, visit the Status of Standardization page at [www.electronics.org/status](http://www.electronics.org/status).



**IPC-1791E**

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

If a conflict occurs between the English language and translated versions of this document, the English version will take precedence.

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

## **Global Electronics Association Standards and Artificial Intelligence (AI) Statement**

Global Electronics Association is the trading name of IPC International, Inc., which owns the copyright to all IPC Standards and other IPC materials.

The Global Electronics Association explicitly prohibits:

- The integration or transfer of any data whether in the form of IPC books, standards, metadata, or other formats — into AI engines or algorithms by any person or entity, including authorized distributors and their end users.
- Activities involving data harvesting, text and data mining, enrichment, or the creation of derivative works based on this data, including the use of automated data collection methods or artificial intelligence.

Any breach of these provisions is considered a copyright infringement unless expressly authorized in advance in writing by the Global Electronics Association.

### ***Supersedes:***

IPC-1791D - October 2023  
IPC-1791C - March 2023  
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:

Global Electronics Association  
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	1.6.16	Organization.....	4
<b>1.1</b>	<b>Purpose and Background</b> .....	1	1.6.17	Personnel.....	4
1.1.1	Source Technology and Capability .....	1	1.6.18	Policy .....	4
1.1.2	Interpretation of Requirements for the Purposes of this Standard .....	1	1.6.19	Printed Board Assembler .....	4
1.1.3	Benefits of Using Organizations Certified to this Standard .....	1	1.6.20	Printed Board and Assembly Design.....	4
1.1.4	Additional Detail .....	1	1.6.21	Printed Board and Assembly Design Organization.....	4
<b>1.2</b>	<b>Classification</b> .....	2	1.6.22	Printed Board Trusted Assembler.....	4
<b>1.3</b>	<b>Definition of Requirements</b> .....	2	1.6.23	Printed Board Trusted Design Organization.....	4
<b>1.4</b>	<b>Certification</b> .....	2	1.6.24	Printed Board Trusted Fabricator.....	4
1.4.1	Type 1 – Printed Board Design Organizations .....	2	1.6.25	Procedure .....	4
1.4.2	Type 2 – Printed Board Fabrication Organizations .....	2	1.6.26	Product-Specific Special Case.....	4
1.4.3	Type 3 – Printed Board Assembly Organizations .....	2	1.6.27	Quality .....	4
1.4.4	Type 4 – Cable and Wire Harness Assembly Organizations.....	2	1.6.28	Security .....	4
1.4.5	Length of Certification.....	2	1.6.29	Supply Chain Risk Management (SCRM) .....	4
1.4.6	Ownership Changes .....	2	1.6.30	Trust .....	4
1.4.7	Management Changes .....	2	1.6.31	Trusted Cable and Wire Harness Assembler.....	4
<b>1.5</b>	<b>Abbreviations and Acronyms</b> .....	2	1.6.32	Trusted Source or Trusted Supplier.....	5
<b>1.6</b>	<b>Terms and Definitions</b> .....	2	1.6.33	Visitors.....	5
1.6.1	Chain of Custody (ChoC).....	3	<b>2</b>	<b>APPLICABLE DOCUMENTS</b> .....	5
1.6.2	Commercial and Government Entity (CAGE) Code .....	3	<b>2.1</b>	<b>IPC</b> .....	5
1.6.3	Confidentiality .....	3	<b>2.2</b>	<b>Joint Standards</b> .....	5
1.6.4	Controlled Technical Information .....	3	<b>2.3</b>	<b>Center for Development of Security Excellence</b> ...	5
1.6.5	Controlled Unclassified Information (CUI) .....	3	<b>2.4</b>	<b>National Institute of Standards and Technology (NIST)</b> .....	5
1.6.6	Covered Defense Information .....	3	<b>2.5</b>	<b>SAE International</b> .....	5
1.6.7	Cyber Incident .....	3	<b>2.6</b>	<b>U.S. Department of Defense (DoD)</b> .....	6
1.6.8	Deemed Export.....	3	2.6.1	Directives and Instructions.....	6
1.6.9	Department of Defense (DoD) Prime Contractor .....	3	2.6.2	Specifications.....	6
1.6.10	Department of State Proforma for Permanent Export (DSP-5) .....	3	2.6.3	Office of Inspector General.....	6
1.6.11	Export Administration Regulations (EAR) .....	3	<b>2.7</b>	<b>U.S. House of Representatives Office of the Law Revision Council</b> .....	6
1.6.12	Federal Bureau of Investigation (FBI) Channeler .....	3	<b>2.8</b>	<b>U.S. Office of the Federal Register – Code of Federal Regulations (CFR)</b> .....	6
1.6.13	Foreign Person .....	3	<b>2.9</b>	<b>U.S. Office of the Federal Registrar – Defense Acquisition Regulation Supplement (DFARS)</b> .....	6
1.6.14	Information Technology (IT) .....	4	<b>2.10</b>	<b>U.S. Congress</b> .....	6
1.6.15	International Traffic in Arms Regulations (ITAR) Registered .....	4	<b>3</b>	<b>REQUIREMENTS</b> .....	7
			<b>3.1</b>	<b>Quality Requirements</b> .....	7
			3.1.1	Type 1 – Printed Board Design Organization.....	7
			3.1.2	Type 2 – Printed Board Fabrication Organization.....	7

3.1.3	Type 3 – Printed Board Assembly Organization... 7	<b>4.3</b>	<b>Empowered Official</b> ..... 13
3.1.4	Type 4 – Cable and Wire Harness Assembly Organization..... 7	<b>4.4</b>	<b>Export-Controlled Data on Portable Electronic Devices</b> ..... 13
<b>3.2</b>	<b>Supply Chain Risk Management (SCRM) Policy</b> ... 7	<b>5</b>	<b>NIST SP 800-171 and CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) EXPLANATION</b> ..... 13
3.2.1	Supplier Assessment ..... 7	<b>5.1</b>	<b>Compliance with NIST SP 800-171 Cybersecurity Regulations</b> ..... 13
3.2.2	Outsource Process Suppliers ..... 7	5.1.1	NIST SP 800-171 Scope ..... 13
3.2.3	Commercial and Government Entity (CAGE) Code/NATO Commercial and Government Entity (NCAGE)..... 7	5.1.2	Application of NIST SP 800-171 Requirements..... 13
<b>3.3</b>	<b>Security</b> ..... 8	5.1.3	Families of Security Requirements ..... 13
3.3.1	Responsible Security Officer and Team ..... 8	5.1.4	Cyber Incident Reporting ..... 13
3.3.2	Personnel Security Requirements..... 8	<b>5.2</b>	<b>Cybersecurity Maturity Model Certification (CMMC) Framework</b> ..... 13
3.3.2.1	Nondisclosure Agreements (NDAs) ..... 8	5.2.1	Data Safeguarding ..... 13
3.3.2.2	Background Checks ..... 8	5.2.2	CMMC Requirements/Practices ..... 13
3.3.2.3	Citizenship ..... 9	5.2.3	CMMC Certification..... 14
3.3.2.4	Training..... 10	5.2.4	CMMC Implementation..... 14
3.3.3	Publication Approval ..... 10	<b>6</b>	<b>REQUIREMENTS FOR TRUST CERTIFICATION OF NON-U.S. ELECTRONIC DESIGN, FABRICATION AND ASSEMBLY ORGANIZATIONS</b> ..... 14
3.3.4	Physical Protection ..... 10	<b>6.1</b>	<b>Certification</b> ..... 14
3.3.4.1	Reception Area ..... 10	6.1.1	Non-U.S. Organizations..... 14
3.3.4.2	Information Processing ..... 10	6.1.2	Length of Certification..... 14
3.3.4.3	Data Center and Storage Areas ..... 10	6.1.3	Ownership or Management Change Notification ..... 14
3.3.4.4	Perimeter Security, Entrances and Exits ..... 10	6.1.4	Certification Duration..... 14
3.3.4.5	Excluded Electronics ..... 10	<b>6.2</b>	<b>Security Requirements</b> ..... 14
3.3.4.6	Security Guards ..... 10	6.2.1	Responsible Security Officer and Team ..... 14
3.3.4.7	Foreign Person Access ..... 11	6.2.2	Personnel Security Requirements..... 15
3.3.4.8	Removing Data from the U.S..... 11	6.2.2.1	Nondisclosure Agreements (NDA) ..... 15
3.3.4.9	Restricting Export-Controlled Data..... 11	6.2.2.2	Background Checks ..... 15
3.3.4.10	Visitors..... 11	6.2.2.3	Personnel..... 15
<b>3.4</b>	<b>Chain of Custody (ChoC) for Type 1, 2, 3 and 4 Organizations</b> ..... 11	6.2.2.4	Training..... 15
3.4.1	Traceability Records..... 11	6.2.3	Publication Approval ..... 15
3.4.2	Serialization and Identification ..... 11	6.2.4	Physical Protection ..... 15
3.4.3	Managing Sample Materials..... 11	6.2.4.1	Reception Area ..... 15
3.4.4	Destruction of Scrap (In-Process or Finished Design Data, Layers and Panels, Subassemblies and Assemblies) ..... 11	6.2.4.2	Information Processing ..... 15
3.4.5	CUI Chain of Custody – Customer Orders..... 12	6.2.4.3	Data Center and Storage Areas ..... 15
3.4.6	Shipping ..... 12	6.2.4.4	Perimeter Security, Entrances and Exits ..... 15
3.4.7	Training ..... 12	6.2.4.5	Excluded Electronics ..... 16
<b>3.5</b>	<b>Additional Chain of Custody (ChoC) Requirements for Type 1 Organizations</b> ..... 12	6.2.4.6	Security Guards ..... 16
<b>4</b>	<b>EXPORT CONTROL COMPLIANCE</b> ..... 13	6.2.4.7	Unauthorized Access..... 16
<b>4.1</b>	<b>Compliance with Export Control Laws</b> ..... 13		
<b>4.2</b>	<b>Export</b> ..... 13		

6.2.4.8 Removing Data from Non-U.S. Subcontractor Organizations..... 16

6.2.4.9 Restricting CUI and Export-Controlled Data..... 16

6.2.4.10 Visitors..... 16

**APPENDIX A Defense Background..... 17**

**APPENDIX B IPC-1791 Compliance to NDAA 2020 Section 224 ..... 18**

**B.1 Overview ..... 18**

**B.2 IPC-1791 Compliance Confirmation Details ..... 18**

B.2.1 NDAA 2022, Section 851 ..... 18

B.2.2 Quantifiable Assurance..... 19

B.2.3 IPC-1791 Meets Quantifiable Assurance..... 19

B.2.4 IPC-1791 Complies with NDAA 2020, Section 224..... 19

**APPENDIX C Marking Controlled Unclassified Information (CUI) ..... 22**

**APPENDIX D Index of Acronyms and Abbreviations ..... 23**

**Tables**

Table 3-1 Supply Chain Risk Management (SCRM) Policy and/or Procedure Guidelines ..... 9

Table 3-2 Supplier Assessment Procedure Requirements ... 9

**Figures**

Figure 3-1 Printed Board Design Schema ..... 12

# 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 will start gradually, accelerating in Fiscal Year 2025. 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 Purpose and Background

**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 **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

In addition, this standard is in compliance with NDAA 2020 Section 224 for printed boards and printed board assemblies. See Appendix B for details.

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