



IPC-1791

# 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-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

## Table of Contents

<b>1 SCOPE</b> .....	1	1.3.25 Procedure .....	3
1.1 Background .....	1	1.3.26 Product-Specific Special Case .....	4
1.1.1 Source Technology and Capability .....	1	1.3.27 Quality .....	4
1.1.2 Interpretation of “Shall” .....	1	1.3.28 Security .....	4
1.1.3 Interpretation of Requirements for the Purposes of this Standard .....	1	1.3.29 Supply Chain Risk Management (SCRM) .....	4
1.1.4 Benefits of Using Organizations Certified to this Standard .....	1	1.3.30 Trust .....	4
1.1.5 Additional Detail .....	1	1.3.31 Trusted Source or Trusted Supplier .....	4
1.2 Certification Types .....	1	<b>2 APPLICABLE DOCUMENTS</b> .....	4
1.2.1 Type 1 – Printed Board Design Organizations ...	2	2.1 IPC .....	4
1.2.2 Type 2 – Printed Board Fabrication Organizations .....	2	2.2 Joint Standards .....	4
1.2.3 Type 3 – Printed Board Assembly Organizations .....	2	2.3 Center for Development of Security Excellence .....	4
1.3 Terms and Definitions .....	2	2.4 National Institute of Standards and Technology (NIST) .....	4
1.3.1 Chain of Custody (ChoC) .....	2	2.5 SAE International .....	5
1.3.2 Confidentiality .....	2	2.6 U.S. Department of Defense (DoD) .....	5
1.3.3 Commercial and Government Entity (CAGE) Code .....	2	2.6.1 Directives and Instructions .....	5
1.3.4 Controlled Technical Information .....	2	2.6.2 Specifications .....	5
1.3.5 Controlled Unclassified Information (CUI) .....	2	2.7 U.S. House of Representatives Office of the Law Revision Council .....	5
1.3.6 Covered Contractor Information System .....	2	2.8 U.S. Office of the Federal Register – Code of Federal Regulations (CFR) .....	5
1.3.7 Covered Defense Information .....	2	<b>3 REQUIREMENTS</b> .....	5
1.3.8 Cyber Incident .....	2	3.1 Quality Requirements .....	5
1.3.9 Department of Defense (DoD) Prime Contractor .....	2	3.1.1 Type 1 – Printed Board Design Organization ...	5
1.3.10 Department of State Proforma for Permanent Export (DSP-5) .....	2	3.1.2 Type 2 – Printed Board Fabrication Organization .....	5
1.3.11 Deemed Export .....	2	3.1.3 Type 3 – Printed Board Assembly Organization .....	6
1.3.12 Export Administration Regulations (EAR) .....	2	3.2 Supply Chain Risk Management (SCRM) Policy .....	6
1.3.13 Federal Bureau of Investigation (FBI) Channeler .....	3	3.2.1 Commercial and Government Entity (CAGE) Code .....	7
1.3.14 Foreign Person .....	3	3.3 Security .....	7
1.3.15 Information Technology (IT) .....	3	3.3.1 Responsible Security Officer and Team .....	7
1.3.16 International Traffic in Arms Regulations (ITAR) Registered .....	3	3.3.2 Personnel Security Requirements .....	7
1.3.17 Organization .....	3	3.3.3 Publication Approval .....	8
1.3.18 Policy .....	3	3.3.4 Physical Protection .....	8
1.3.19 Printed Board Assembler .....	3	3.4 Chain of Custody (ChoC) for Type 1, 2 and 3 Organizations .....	9
1.3.20 Printed Board and Assembly Design .....	3	3.4.1 Traceability Records .....	9
1.3.21 Printed Board and Assembly Design Organization .....	3	3.4.2 Serialization and Identification .....	9
1.3.22 Printed Board Trusted Assembler .....	3	3.4.3 Sample Materials .....	9
1.3.23 Printed Board Trusted Design Organization .....	3		
1.3.24 Printed Board Trusted Fabricator .....	3		

3.4.4	Destruction of Scrap (In-Process or Finished Design Data, Layers and Panels, Subassemblies and Assemblies) .....	9
3.4.5	Repeat Orders .....	10
3.4.6	Shipping .....	10
3.4.7	Training .....	10
3.5	Additional Chain of Custody (ChoC) Requirements for Type 1 Organizations .....	10
<b>APPENDIX A</b>	<b>Defense Background</b> .....	<b>11</b>
<b>APPENDIX B</b>	<b>Export Control Compliance</b> .....	<b>12</b>
<b>APPENDIX C</b>	<b>NIST SP 800-171 Security Framework Explanation</b> .....	<b>13</b>
<b>APPENDIX D</b>	<b>Acronym Index</b> .....	<b>14</b>

**Figures**

Figure 3-1	Printed Board Design Schema .....	10
------------	-----------------------------------	----

**Tables**

Table 3-1	Supply Chain Risk Management (SCRM) Policy and/or Procedure Guidelines .....	6
Table 3-2	Supplier Assessment Procedure Requirements .....	7
Table C-1	NIST SP 800-171 Security Requirement Families .....	13

# Trusted Electronic Designer, Fabricator and Assembler Requirements

## 1 SCOPE

This standard provides minimum requirements, policies and procedures for printed board design, fabrication and 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).

Demonstration of the ability to meet and maintain the requirements of this standard as trusted design, fabrication or assembly organization 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 delivered product and process integrity assurance by printed board designers, fabricators and 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 U.S. Department of Defense (DoD) facility clearance unless compelled by customer-specific requirements and pursued independent of this standard.

### 1.1 Background

**1.1.1 Source Technology and Capability** Design, fabrication and 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 "Shall"** The imperative form of the verb "**shall**" is used throughout this standard whenever a requirement is intended to express a provision that is mandatory. Deviation from a "**shall**" requirement may be considered if sufficient data are supplied to justify the exception. To assist the reader, the word "**shall**" is presented in bold characters.

The words "should" and "may" are used whenever it is necessary to express nonmandatory provisions.

"Will" is used to express a declaration of purpose.

**1.1.3 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-2000 series, IPC-6000 series, IPC-A-600, IPC-A-610, MIL-PRF-31032, AS9100, National Aerospace and Defense Contractors Accreditation Program (Nadcap), etc.) **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.

**1.1.4 Benefits of Using Organizations Certified to this Standard** By using designers, printed board fabricators and printed board assemblers that have been 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

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

**1.2 Certification Types** To ensure cost-effective use of trusted suppliers, this standard provides three types of certification (see 1.2.1 through 1.2.3). Certification types are based on the function of the organization.