

**IPC-1792**

**2022 - November**

**Standard for the Management and  
Mitigation of Cybersecurity Incidents  
in the Manufacturing Industry  
Supply Chain**

*An international standard developed by IPC*



**BUILD ELECTRONICS BETTER**

---

## IPC Mission

IPC is a global trade association dedicated to furthering the competitive excellence and financial success of its members, who are participants in the electronics industry.

In pursuit of these objectives, IPC will devote resources to management improvement and technology enhancement programs, the creation of relevant standards, protection of the environment, and pertinent government relations.

IPC encourages the active participation of all its members in these activities and commits to full cooperation with all related organizations.

## About IPC Standards

IPC standards and publications are designed to serve the public interest through elimination of 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 IPC standards and publications shall not in any respect preclude any entity from manufacturing or selling products not conforming to such IPC standards and publication, nor shall the existence of such IPC standards and publications preclude their voluntary use.

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

## IPC Position Statement on Specification Revision Change

The use and implementation of IPC standards and publications are voluntary and part of a relationship entered into by customer and supplier. When an IPC 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. IPC recommends the use of the latest revision or amendment.

## Standards Improvement Recommendations

IPC 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 IPC Status of Standardization page at [www.ipc.org/status](http://www.ipc.org/status).



IPC-1792

# Standard for the Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain

Developed by the Cybersecurity Protection Standard Task Group (2-12c)  
of the Electronic Product Data Description Committee (2-10) of IPC

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

Contact:

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

This Page Intentionally Left Blank

## Acknowledgment

Any document involving a complex technology draws material from a vast number of sources. While the principal members of the Cybersecurity Protection Standard Task Group (2-12c) of the Electronic Product Data Description Committee (2-10) of IPC are shown below, it is not possible to include all of those who assisted in the evolution of this standard. To each of them, the members of the IPC extend their gratitude.

<b>Electronic Product Data Description Committee</b>	<b>Cybersecurity Protection Standard Task Group</b>	<b>Technical Liaisons of the IPC Board of Directors</b>
Chair Michael Ford Aegis Software UK	Chair Hiroyuki Watanabe NEC Platforms  Vice Chair Kathy Nargi-Toth Bowhead	Bob Neves Microtek (Changzhou) Laboratory

IPC recognizes this A-Team for their exceptional leadership and effort in the development of this standard. IPC A-Teams are dedicated groups of volunteers who undertake a significant amount of work in standards development on behalf of their group.

### Cyber Key Holders

Radu Diaconescu Swissmic	Kathy Nargi-Toth Bowhead	Hiroyuki Watanabe NEC Platforms
Michael Ford Aegis Software UK	Toshiyuki Sawada NEC Platforms	Kazuhiro Yoshinaga NEC Platforms

### Cybersecurity Protection Standard Task Group

Bobby Bean Collins Aerospace	Thomas Geißinger Continental Automotive Technologies GmbH	Marc Peo Heller Industries Inc.
Peter Bigelow IMI Inc.	Stephen Golemme JITX Inc.	Chris Peters U.S. Partnership for Assured Electronics (USPAE)
Gerald Bogert Bechtel Plant Machinery, Inc.	Ife Hsu Intertek	Randy Reed R. Reed Consultancy LLC
Neil Bolding MacDermid Alpha Automotive	Jennie Liwang H-Technologies Group	Robert Roessler ABB Power Electronics Inc.
Christine Bunke IBM Corporation	Asaf Jivilik Cybord	Toshiyuki Sawada NEC Platforms
Zhiman Chen ZHUZHOU CRRC TIMES ELECTRIC CO., LTD	Michael Kimpton Fuji America Corporation	Raminder Singh NSWC Crane
Radu Diaconescu Swissmic	Mark Kirkman SAIC	Richard Snogren Bristlecone LLC
Don Dupriest Lockheed Martin Missiles & Fire Control	Vincent Levannier SYNEO, LLC	Hiroyuki Watanabe NEC Platforms
Michael Duffan Mentor Graphics Corporation	Thomas Marktscheffel ASM (Assembly Systems) GmbH & Co. KG	Jarrold Webb Lockheed Martin Missiles & Fire Control
Michael Ford Aegis Software UK	Lim Ming Jabil Circuit Sdn. Bhd.	Eyal Weiss Cybord
Dennis Fritz MacDermid Enthone Electronics Solutions	N. Nagaraj Papros, Inc.	Ting Yu Wong Sierra Wireless Hong Kong Limited
	Kathy Nargi-Toth Bowhead	Kazuhiro Yoshinaga NEC Platforms

This Page Intentionally Left Blank

Currently in preview, click buy full version

# Table of Contents

<b>1</b>	<b>SCOPE</b> .....	1	2.4	United States Department of Defense (DoD) ..	5
1.1	Purpose .....	1	<b>3</b>	<b>OPERATIONAL MODEL</b> .....	5
1.1.1	Industry Background .....	1	3.1	Preparation .....	5
1.1.2	Key Elements of This Standard .....	2	3.2	Normal Operation .....	5
1.2	IPC Product Classification .....	2	3.3	Cyberattack Detection at the Factory .....	5
1.2.1	Relation Between IPC Classification and Urgency of Cyber Incident Impact Detection ..	2	3.4	Cybersecurity Incident in the Supply Chain ..	5
1.2.2	Risk Assessment and the Urgency of Cyber Incident Impact Detection .....	2	<b>4</b>	<b>REQUIREMENTS FOR CYBERSECURITY FOR FACTORIES</b> .....	6
1.2.3	Levels of Cybersecurity Management .....	3	4.1	Factory Requirements .....	6
1.3	Definition of Requirements .....	3	4.1.1	Preparation .....	6
1.4	Order of Precedence .....	3	4.1.2	Cybersecurity Detection Requirements .....	6
1.4.1	Conflict .....	3	4.1.3	Requirements for Normal Operation .....	7
1.4.2	Clause References .....	3	4.1.4	CIQA Requirements .....	8
1.4.3	Appendices .....	3	4.1.5	Cybersecurity Incident Response Requirements .....	8
1.5	Acronyms .....	3	4.1.6	Supply Chain Cybersecurity Incident Response Requirements .....	9
1.6	Terms And Definitions .....	3	4.1.7	Response Time Requirements .....	9
1.6.1	Certified Material .....	4	4.2	Cybersecurity Service Provider Requirements ..	9
1.6.2	Certified Product .....	4	4.2.1	Cybersecurity Diploma Manager .....	9
1.6.3	Cyberattack .....	4	4.2.2	Cybersecurity Auditor .....	9
1.6.4	Cybersecure Factory .....	4	4.2.3	Cybersecurity Supply Chain Manager .....	9
1.6.5	Cybersecurity Audit .....	4	4.3	Digital Certificate .....	9
1.6.6	Cybersecurity Auditor .....	4	4.3.1	General Requirements for Digital Certificates ..	9
1.6.7	Cybersecurity Certification Authority ..	4	4.3.2	Architectural Concepts .....	9
1.6.8	Cybersecurity Diploma .....	4	4.3.3	Basic Description of Data Type .....	10
1.6.9	Cybersecurity Diploma Manager .....	4	4.3.3.1	JSON Schemas .....	10
1.6.10	Cybersecurity Incident .....	4	4.3.3.2	CMS Signed Data .....	10
1.6.11	Cybersecurity Intrusion .....	4	4.3.4	Digital Diploma Interface (Data Structure) ..	11
1.6.12	Cybersecurity Supply Chain Manager .....	4	4.3.4.1	Common Structures and General Requirements .....	11
1.6.13	Digital Certificate .....	4	4.3.4.1.1	Version information .....	11
1.6.14	Final Certified Product .....	4	4.3.4.1.2	Digital Diploma (Factory) Specific Information .....	11
1.6.15	Supplier .....	4	4.3.4.1.3	Key Information .....	12
1.6.16	Supply Chain Entity .....	4	4.3.4.1.4	Date of issue .....	12
1.6.17	Supply Chain Risk .....	4	4.3.5	Interface (Data Structure) of Product/Material Digital Certificate .....	12
1.6.18	Uncertified Material .....	4	4.3.5.1	Common Structures and General Requirements .....	12
1.6.19	Declaration of Conformance .....	5	4.3.5.2	Version Information .....	12
	<b>APPLICABLE DOCUMENTS</b> .....	5	4.3.5.3	Factory Information .....	13
2.1	IPC .....	5			
2.2	International Organization for Standardization (ISO) .....	5			
2.3	National Institute of Standards and Technology (NIST) .....	5			

4.3.5.4 Certified Material Specific Information. . . . . 13

4.3.5.5 Certified Material Specific Information. . . . . 13

4.3.6 Interface (Data Structure) of Tag information Exchanged Between Factories . . . . . 13

4.3.6.1 Common Structures and General Requirements . . . . . 13

4.3.6.1.1 Version information. . . . . 14

4.3.6.1.2 Certificate or Warning . . . . . 14

4.3.6.1.3 Key Information. . . . . 14

4.3.6.1.4 Original Data Body (Including Digital Signature) Received From Upstream in the Supply Chain . . . . . 14

4.3.6.1.5 Date of Production/Incident. . . . . 15

**5 REQUIREMENTS FOR CYBERSECURITY SERVICE PROVIDERS OPERATIONS . . . . . 15**

5.1 Cybersecurity Diploma Manager. . . . . 15

5.2 Cybersecurity Auditor . . . . . 15

5.3 Cybersecurity Supply Chain Manager. . . . . 15

**6 COMPLIANCE GUIDANCE . . . . . 15**

**Appendix A Index of Acronyms and Abbreviations . . . . . 18**

**Figures**

Figure 3-1 Common Modeling of Cyber Incident Quick Identification (CIQI) . . . . . 6

Figure 4-1 Stakeholder Relationship Diagram Example . . . . . 10

Figure 4-2 Data Fields Structure . . . . . 11

Figure 4-3 Common Structure . . . . . 12

Figure 4-4 Common Structures and General Requirements . . . . . 13

**Tables**

Table 1-1 Guide for Response Levels Based on IPC Classification . . . . . 2

Table 1-2 Typical Risk Assessment Matrix. . . . . 3

Table 4-1 Required Response Times. . . . . 9

Table 4-2 Version Information . . . . . 11

Table 4-3 Digital Diploma (Factory) Specific Information . . . . . 11

Table 4-4 Combination of Private and Public Keys . . . 12

Table 4-5 Date of Registration . . . . . 12

Table 4-6 Versioning Specific Information. . . . . 12

Table 4-7 Factory Specific Information . . . . . 13

Table 4-8 Certified Product/Material Specific Information . . . . . 13

Table 4-9 Date of Certificate. . . . . 13

Table 4-10 Version information . . . . . 14

Table 4-11 Certificate or Warning (Incident Occurrence) Information . . . . . 14

Table 4-12 Certified Product / Material-Specific Information . . . . . 14

Table 4-13 Notification of Warnings (Incidents) . . . . . 14

Table 4-14 Public Key . . . . . 14

Table 4-15 Data Body . . . . . 14

Table 4-16 Date of Production/Incident . . . . . 15

Table 6-1 IPC-1792 Compliance Guidance . . . . . 15

# Standard for the Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain

## 1 SCOPE

This standard establishes requirements for companies to provide assurance that their products have been manufactured in cybersecure environments, ensuring that there has been no risk of impact to the product due to any cybersecurity incident. Requirements are specified covering actions that need to be taken in the event that a cybersecurity incident is detected, identifying all possibly affected products.

The target audiences for this standard are companies within the electronics manufacturing industry, cybersecurity supply chain managers and related organizations. This standard applies to the manufacture of final products as well as all component materials, paths and storage areas. External logistics processes are also covered via their responsibility to their customer.

This standard also defines levels of cybersecurity management that provide a choice when adopting this standard to meet the appropriate need. Pathways exist to enable progression from a basic level of cybersecurity maturity to higher levels. Appropriate levels for companies to adopt may be determined based on IPC Product Classification as well as risk that is across all possible use cases of products.

This standard also includes mechanisms for third-party assessment to the cybersecurity levels defined in this standard.

**1.1 Purpose** As technologies related to Smart Cities and Internet of Things (IoT) advance, there is an increased risk that cybersecurity incidents will have serious impacts on society. Many cyberattacks are enabled through unauthorized manipulation of smart devices during manufacture, which creates opportunities for third parties to exploit vulnerabilities. The intent of this standard is to eliminate the opportunity for the manipulation of software and hardware throughout the end-to-end manufacturing process, ensuring that products are built as intended by the original designer. Application of this standard provides continued assurance against evolving cybersecurity threats in end-products as technology advances.

The use of this standard helps companies identify those products that may have been affected as a result of a cybersecurity incident during manufacture, ensuring all products released into the market are free from any risk of tampering related to hardware and software content.

This standard represents guidance to the various entities in the electronics manufacturing supply chain to provide a continuous cybersecurity focus, building on existing and evolving information technology (IT). Procedures and requirements provide manufacturing companies the ability to manage the effects of cybersecurity incidents, should they occur within their organization or upstream in the supply chain, with propagation of information in a timely manner, downstream in the supply chain.

Adoption of this standard enables companies to ensure appropriate practices and procedures related to required data management are established that identify the impact of Cybersecurity Incidents, involving, for example, preventing the leakage or alteration of critical information, to secure the product owner's supply chain. In the event of any cybersecurity incident, methodologies described in this standard identify the specific potential effect to the supply chain and how to minimize effects.

**1.1.1 Industry Background** The electronics manufacturing supply chain is multitiered, with multiple companies supplying individual products that ultimately create the final end-product for the customer. This distributed supply chain presents numerous opportunities where information created to and used by manufacturing operations can be intercepted and used for unauthorized or unlawful purposes, potentially significantly compromising the safety of the end-product. It is vital that each entity in the supply chain is able to provide assurance that such information has not been tampered with, intercepted or stolen, via interoperable exchange of information without compromise of privacy with other members of the supply chain as required. Should any cyberattack events be discovered, whether from outside of the secure environment or from within, it is essential to have documentation that proves how such attacks and any potential consequences have been addressed, as this allows the product owner to determine who is responsible for effects of the incident and which corrective actions have taken place.

The manufacturing supply chain is increasingly being targeted by individuals and entities seeking to obtain product-related information, with the intention of disrupting manufacturing operations, creating cloned or counterfeit products or to introduce Trojan horses that undermine the security in end-products. Supply chain risk is a key contributor to overall security risk with, for example, procurement of hardware or software that has been compromised, either by the creation of counterfeits or by being illegally obtained, or where the source has been subject to industrial espionage.

Product owners should expect their products to be manufactured in a secure supply chain and that the capability exists to detect and take appropriate action should a cybersecurity incident occur. To meet this expectation, the whole supply chain needs to be secured, as it is only as strong as its weakest participant. Failure to do so has been documented in numerous cases of cybersecurity breaches that have had serious consequences.