**DEPARTMENT OF DEFENSE**

**Defense Acquisition Regulations System**

**48 CFR Parts 212, 225, and 252**

**[Docket DARS-2026-0298]**

**RIN 0750-AL62**

# Defense Federal Acquisition Regulation Supplement: Modifications to Printed Circuit Board Acquisition Restrictions (DFARS Case 2022-D011)

**AGENCY:** Defense Acquisition Regulations System, Department of Defense (DoD).

**ACTION:** Advance notice of proposed rulemaking.

**SUMMARY:** DoD is seeking information that will assist in the development of a revision to the Defense Federal Acquisition Regulation Supplement (DFARS) to implement sections of the National Defense Authorization Acts for Fiscal Years 2021 and 2022 that address the prohibition on the acquisition of covered printed circuit boards from a covered nation.

**DATES:** Comments on the advance notice of proposed rulemaking should be submitted in writing to the address shown below on or before **[INSERT 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, to be considered in the formation of any proposed rule.

**ADDRESSES:** Submit written comments identified by DFARS Case 2022-D011, using either of the following methods:

- *Federal eRulemaking Portal*: *https://www.regulations.gov*.

Search for DFARS Case 2022-D011. Select "Comment" and follow the instructions to submit a comment. Please include "DFARS Case 2022-D011" on any attached documents.

- *Email*: *osd.dfars@mail.mil*. Include DFARS Case 2022-D011 in the subject line of the message.

Comments received generally will be posted without change to *https://www.regulations.gov*, including any personal information provided. To confirm receipt of your comment(s), please check *https://www.regulations.gov*, approximately two to three days after submission to verify posting.

**FOR FURTHER INFORMATION CONTACT:** Kelsey Bramschreiber, telephone 948-245-1544.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

DoD is seeking information from experts and interested parties in Government and the private sector that will assist in the development of a revision to the DFARS to implement section 841 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2021 (Pub. L. 116-283) and section 851 of the NDAA for FY 2022 (Pub. L. 117–81). Section 841 adds 10 U.S.C. 2533d, which prohibits the acquisition of covered printed circuit boards from a covered nation. Section 851 amends 10 U.S.C. 2533d, subsequently renumbered as 10 U.S.C. 4873.

Section 841 of the NDAA for FY 2021 and section 851 of the NDAA for FY 2022 (10 U.S.C. 4873) require the Department of Defense to mitigate supply chain risks by prohibiting the

procurement of covered printed circuit boards from entities located in or controlled by a covered nation (i.e., the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of North Korea). DoD intends to implement this prohibition by focusing on the geographic point of fabrication for bare boards or partially manufactured boards and by utilizing a tiered trust architecture.

Furthermore, any rulemaking that may follow this advance notice of proposed rulemaking (ANPR) would put into operation the mandate in section 224 of the NDAA for FY 2020, which requires DoD to establish trusted supply chain and operational security standards for the procurement of microelectronics and their associated printed circuit boards. By coupling the geographic prohibitions of 10 U.S.C. 4873 with rigorous technical standards, developed through strong Government/industry partnerships, DoD establishes a comprehensive hardware assurance posture that satisfies both statutory directives.

**II. Discussion and Analysis**

The following is a summary of DoD's proposed approach and the feedback DoD is seeking from industry and the public.

*A. Defining the Scope: Statutory Thresholds*

DoD seeks public comment on a proposed regulatory framework, the Independent Hardware Assurance Framework, that utilizes industry standards ISO/IEC 20243, IPC-1782, and IPC-1791 as the

foundational requirements for granting statutory exceptions and waivers. Crucially, this framework uses the statutory definitions of the following terms: "covered printed circuit boards," "specified type," and "defense security systems." This approach ensures the protection of national security while minimizing impact on the commercial marketplace.

To ensure any regulation that may follow this ANPR does not impose unreasonable restrictions on the procurement of commercial products, including commercially available off-the-shelf (COTS) items, DoD adopts the strict statutory definitions provided in 10 U.S.C. 4873(c). DoD emphasizes that this proposed framework is not a blanket prohibition on specific commercial products, including COTS items, or commercial services. These stringent Independent Hardware Assurance Framework requirements are only placed on covered printed circuit boards being integrated into systems in which a compromise could directly threaten military mission, warfighter safety, or national security. For procurements that fall within this critical scope, DoD has established a rigorous, evidence-based waiver process (see section II.B. of this ANPR) to address circumstances of market unavailability and urgent operational need.

*B. Proposed Framework for Exceptions and Waivers*

For covered printed circuit boards requiring a waiver to source from a covered nation under 10 U.S.C. 4873, DoD proposes establishing an Independent Hardware Assurance Framework to satisfy the statutory requirement of 10 U.S.C. 4873(b)(1). This

statutory requirement demands a written determination that there are no significant national security concerns regarding counterfeiting, quality, or unauthorized access. Recognizing that facilities within covered nations cannot legally or practically guarantee the protection of controlled unclassified information (CUI), this waiver process will not rely on attestations from suppliers.

While contractors may propose alternative mitigation strategies, DoD assesses that compliance with a four-pillar framework, which ensures supply chain security, data traceability, facility trust and secure handling, and cybersecurity, provides the standardized evidentiary baseline necessary to satisfy these statutory waiver criteria. Furthermore, this framework meets or exceeds the trusted supply chain and operational security requirements mandated by section 224 of the NDAA for FY 2020. Therefore, DoD proposes that demonstrating compliance with the following four pillars will serve as the primary mechanism for contractors seeking a waiver:

1. *Enterprise-Level Supply Chain Integrity (ISO/IEC 20243).* The Open Trusted Technology Provider Standard (O-TTPS) is an international standard that establishes best practices for secure product development, secure engineering, supply chain security, and lifecycle management to prevent maliciously tainted and counterfeit products. For any printed circuit board requiring a waiver, the contractor must hold a current ISO/IEC 20243 (O-TTPS) certification. This ensures the contractor

utilizes secure engineering practices and aggressive downstream supplier vetting to mitigate the risk of maliciously tainted raw materials and COTS subcomponents entering the bare board fabrication process.

2. *Granular Provenance and Traceability (IPC-1782)*. IPC-1782 is a comprehensive traceability standard that strengthens electronics supply chain integrity, supports counterfeit prevention, and provides a flexible framework for capturing and analyzing critical manufacturing and component data. For any covered printed circuit board requiring a waiver, the contractor must deliver standardized, machine-level manufacturing traceability data in accordance with IPC-1782 (Level 3 or 4). This evidentiary audit trail must document the origin of the board's base materials (e.g., laminate, copper foil) and the specific machinery used during fabrication. This data will be heavily scrutinized by DoD to verify the exact geographic points of manufacturing.

3. *Facility Trust and Secure Handling (IPC-1791)*. DoD's strong preference is that facilities involved in the design, fabrication, and assembly of covered printed circuit boards be certified to IPC-1791 (Trusted Electronic Designer, Fabricator and Assembler Requirements). IPC-1791 provides minimum requirements, policies, and procedures for facilities to become trusted sources for markets requiring high levels of confidence in the integrity of delivered products. These trusted sources

must ensure quality, supply chain risk management, security (information and physical), and chain of custody.

IPC-1791 certification is only available to non-U.S. facilities via sponsorship. A facility in a covered nation likely cannot achieve IPC-1791 certification. Therefore, any bare board granted an exception and imported from a covered nation must be routed through a domestic (or approved allied) facility certified as an IPC-1791 Trusted Assembler, or a DoD Hardware Assurance Laboratory, prior to system integration. This Trusted Facility will utilize the IPC-1782 data to conduct independent, blind hardware assurance testing (e.g., automated optical inspection, x-ray) to verify the manufactured printed circuit board exactly matches the trusted digital design files and that no unauthorized modifications were introduced during fabrication in a covered nation.

4. *Protection of Digital Design Data (Cybersecurity)*. The contractor must identify and protect all unclassified digital design data (e.g., Gerber files, netlists, schematics) associated with the covered printed circuit board as CUI. To qualify for a waiver, the contractor and all applicable lower-tier subcontractor facilities handling this unclassified digital data must comply with the applicable contract cybersecurity requirements. (Note: The manufacture of classified printed circuit boards remains subject to the National Industrial Security Program Operating Manual (NISPOM) and is ineligible for foreign sourcing waivers under this framework).

DoD recognizes that standards evolve. However, for the purposes of qualifying for a waiver under 10 U.S.C. 4873, the contractor (including facilities) must actively hold the formal, third-party certifications (ISO/IEC 20243 and IPC-1791) and generate the standardized data schemas (IPC-1782). The contractor’s attestation or claims of internal corporate equivalency will not satisfy the requirements of the Independent Hardware Assurance Framework.

To support the Secretary of Defense's waiver determination under 10 U.S.C. 4873(b), DoD anticipates that contractors seeking a waiver will be required to submit a comprehensive waiver request package to the contracting officer. In addition to providing valid, third-party certifications demonstrating full compliance with the Independent Hardware Assurance Framework (ISO/IEC 20243 and IPC-1791), as well as complete traceability data pursuant to IPC-1782, a waiver request must include the following: a Trusted Assembler verification report, market availability justification, component identification (IPC-1782 Traceability), system application and impact, transition strategy, and waiver scope.

For any bare printed circuit board manufactured or partially manufactured in a covered nation, the waiver request must include a certified verification report from a domestic or allied IPC-1791 Trusted Assembler. This report must demonstrate that the board underwent blind testing and validation prior to

population or final assembly to ensure no unauthorized logic, malicious alterations, or counterfeits are present.

The DoD component head (or their designated official) will have the discretion to determine whether this Trusted Assembler verification report is sufficient, or if the report (including IPC-1782 traceability data), verification imagery, digital design files, and/or associated hardware must be submitted to a DoD Hardware Assurance Lab for supplementary validation prior to signing and submitting the waiver to the Secretary of Defense.

If the Trusted Assembler is a subsidiary, an affiliate, or otherwise under the corporate control or influence of the contractor, then the verification report, all verification imagery, digital design files, and/or associated physical hardware must be submitted to a DoD Hardware Assurance Lab for independent validation prior to the DoD component head signing and submitting the waiver request. This validation may be conducted by a designated DoD Hardware Assurance activity, the National Security Agency (NSA), Department of Energy National Laboratories, Federally Funded Research and Development Centers (FFRDCs), or University Affiliated Research Centers (UARCs), at the Government's discretion (DoD component head or Hardware Assurance Lab).

If the Trusted Assembler is a wholly independent third party with no financial or corporate affiliation with the contractor, the DoD component head retains the discretion to accept the report or require a DoD Hardware Assurance Lab review. This

discretionary validation will be conducted by a designated DoD Hardware Assurance activity, which may leverage the NSA, National Laboratories, FFRDCs, or UARCs to execute the review.

The market availability justification must include documented evidence that printed circuit boards of satisfactory quality and sufficient quantity cannot be procured from non-covered nations at a reasonable cost or within the required timeframe. The component identification (IPC-1782 Traceability) must include specific part numbers, quantities, and the exact facility and covered nation of origin for the requested printed circuit boards. With regard to system application and impact, the end-item defense security system must be identified. There must also be a detailed assessment of the schedule and cost impacts to the program if the waiver is denied. The transition strategy must include a time-phased plan detailing the contractor's strategy to qualify alternative domestic or allied sources and eliminate reliance on covered nations for future production. The scope of the waiver must identify the requested duration of the waiver or specific production lot to which the waiver will apply.

*C. Data Delivery, Retention, and Inspection Rights*

To ensure the Government maintains visibility, auditability, and the ability to verify compliance with the Independent Hardware Assurance Framework, DoD proposes the following data requirements. Upon request by the contracting officer, the DoD Program or DoD Hardware Assurance Laboratories, or as specified in the Contract Data Requirements List (CDRL), the contractor

must deliver IPC-1782 manufacturing traceability logs and IPC-1791 independent hardware assurance test reports in a standardized, machine-readable format within a specified timeframe (e.g., five business days).

The contractor must grant the Government the right to access, duplicate, analyze, and utilize the generated provenance, traceability, and verification data strictly for the purposes of inspection, audit, and verifying compliance with 10 U.S.C. 4873 and section 224 of the NDAA for FY 2020. DoD will treat this data as proprietary and will not use it for competitive reprocurement. Contractor assertions of proprietary information or trade secrets will not restrict or delay the Government's verification efforts. At the discretion of the DoD component head or the designated DoD Hardware Assurance activity, this data and the associated Trusted Assembler reports may be shared with the NSA, FFRDCs, UARCs, and Department of Energy National Laboratories supporting DoD hardware assurance, provided such entities are bound by appropriate nondisclosure obligations.

The contractor and the independent verification facility must retain all verification imagery (e.g., automated optical inspection, x-ray) and traceability logs for a period of not less than 10 years following final delivery of the covered printed circuit board, or for the operational lifespan of the defense security system, whichever is longer. In addition, the contractor must provide the Government direct access to audit these records upon request.

*D. Mandatory Flow-down Requirement*

To ensure the prohibitions of 10 U.S.C. 4873 are enforced throughout the entire supply chain, any resulting DFARS contract clause will include a strict, mandatory flow-down requirement. The contractor will be required to insert the substance of the contract clause into all subcontracts and other contractual instruments at every tier, including subcontracts for the acquisition of commercial products and commercial services.

The contractor will not merely flow down this requirement, but will retain affirmative, ultimate responsibility for collecting, verifying, and maintaining valid, third-party certifications (ISO/IEC 20243 and IPC-1791) and complete IPC-1782 traceability data from all lower-tier suppliers and/or facilities prior to integrating covered printed circuit boards into end-item deliverables. This requirement legally obligates all commercial lower-tier entities—including bare board fabricators, contract manufacturers, and independent testing facilities—to comply with the geographic restrictions and technical standards, ensuring a secure, unbroken, and verifiable supply chain from initial materials to final system integration.

The requirement to flow down commercial certifications (ISO/IEC 20243, IPC-1791, IPC-1782) will not apply to subcontracts, interagency agreements, or direct utilization of designated DoD Hardware Assurance Laboratories, FFRDCs, or UARCs performing independent verification testing under this

framework. These entities operate under superseding Federal security and assurance directives.

**III. Specific Questions for Public Comment**

DoD invites input on the following specific questions, particularly from the defense industrial base, commercial printed circuit board manufacturers, and standards bodies:

- *Definitional Clarity:* Do the intersecting definitions of "covered printed circuit board," "specified type" (focusing on data routing/networking), and "defense security system" provide an unambiguous boundary that protects standard commercial/COTS supply chains from unreasonable regulatory burden?
- *Certification Burden:* What is the estimated financial and operational burden for a facility to maintain the proposed four-pillar framework (ISO/IEC 20243, IPC-1782, and IPC-1791) specifically for covered printed circuit board production lines?
- *Certification Timelines:* DoD estimates that achieving IPC-1791 certification requires 8 to 16 months, while IPC-1782 and ISO/IEC 20243 require 3 to 11 months. Are these estimates accurate? What phase-in period (e.g., 12, 18, or 24 months) should DoD consider before making these standards a mandatory condition for an exception?
- *COTS Item Applicability:* ISO/IEC 20243 is widely adopted in the commercial sector. However, to what extent can COTS bare board manufacturers support the data logging requirements of IPC-1782 Level 3 or 4 without causing severe economic disruption?

- *Facility vs. Enterprise:* DoD proposes that IPC-1791 would apply to the specific physical verification facility, while ISO/IEC 20243 would apply to the contractor's enterprise. Does this bifurcation create conflicting obligations for multinational original equipment manufacturers (OEMs)?
- *Data Sovereignty:* How will contractors ensure the protection of CUI (bare board design data) in accordance with NIST SP 800-171 when transmitting manufacturing requirements to a facility located in a covered nation under an approved waiver?
- *Data Rights and Inspection:* DoD proposes limiting its data rights for IPC-1782 traceability logs and IPC-1791 hardware assurance reports strictly to inspection and compliance verification, rather than seeking Government purpose rights (see the clause at DFARS 252.227-7013, -7014, or -7018 for the definition of Government purpose rights). This is applicable to printed circuit boards manufactured or partially manufactured in a covered nation, without IPC-1791 certification. Does this limitation sufficiently protect proprietary manufacturing processes while allowing the Government to audit supply chain provenance?
- *Waiver Mitigation and Section 224 Compliance:* Does the requirement for independent verification at an IPC-1791 facility, combined with IPC-1782 traceability, constitute a feasible and sufficient strategy to meet the operational security requirements of section 224 of the NDAA for FY 2020 when sourcing from a high-risk geographic location?

- *Market Segmentation:* DoD requests that commercial information technology vendors provide the percentage of their current DoD sales that would likely fall under the statutory definition of a "defense security system," versus the percentage used for routine business applications that would be exempt from the definition of this term.

**List of Subjects in 48 CFR Parts 212, 225, and 252**

Government procurement.

**Kimberly R. Ziegler,**

*Editor/Publisher, Defense Acquisition Regulations System.*

[FR Doc. 2026-13375 Filed: 7/1/2026 8:45 am; Publication Date: 7/2/2026]