*Technical White Paper*

# *CRA Roles Across the Embedded Processor Supply Chain*

*Josue Zamitiz-Ayala, Frangline Jose, and Amrit Mundra*

## Abstract

The EU Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, imposes cybersecurity requirements on products with digital elements placed on the EU market - including hardware components such as microprocessors sold to product manufacturers for integration. The CRA distributes compliance requirements across the supply chain: component suppliers and product manufacturers each carry a defined set of requirements based on the role they play. This paper explains what TI addresses at the silicon and software development kit (SDK) level as a component manufacturer, and what product manufacturers - including Tier 1 board vendors, system-on-module (SoM) suppliers, and original equipment manufacturer (OEM) system integrators - remain responsible for under the CRA. This paper is not legal advice; readers need to engage their legal and compliance teams for product-specific guidance.

## 1 Introduction

The EU Cyber Resilience Act (CRA) is a mandatory legal framework that establishes uniform cybersecurity requirements for all hardware and software products with digital elements sold in the European Union market. CRA enforcement begins December 11, 2027. Vulnerability reporting requirements took effect, on September 11, 2026. For product manufacturers building connected devices that incorporate third-party semiconductor components, CRA creates a compliance challenge that cannot be solved by looking at silicon or software in isolation: the regulation assigns requirements to each role in the supply chain that places a product with digital elements on the EU market under its own name.

Products sold in the EU must follow secure design principles, stay updated, and maintain a credible vulnerability handling process throughout their support period. The compliance challenge comes from the supply chain structure of most embedded products. An OEM building a connected IoT gateway, industrial controller, or a collaborative robot typically integrates a microprocessor from a silicon vendor, a board support package (software) from a Tier 1 manufacturer or System on Module (SoM) vendor, with its own application software. Each party has placed components on the market, and each carries CRA responsibilities.

A product manufacturer cannot skip the CRA requirements by selecting a component from a supplier who has met the CRA requirements. Compliance from the component supplier does not satisfy the product manufacturer's risk assessment, conformity declaration (a formal statement that the product meets all CRA requirements), or requirement to report to the product manufacturer's national CSIRT (a national cybersecurity incident response team) and ENISA (the EU's cybersecurity agency). The two sets of requirements run in parallel; one does not substitute for the other. Non-compliance carries fines up to 2.5% of a company's global annual revenue. Component suppliers and intermediate integrators are not exempt.

This paper explains TI's reading of the supply chain boundary, what TI addresses at the silicon and SDK level to meet the requirements as a component manufacturer, and what the integrating product manufacturer must address for the complete product. Compliance determinations require qualified legal and compliance counsel.



Copyright © 2026 Texas Instruments Incorporated

# 2 CRA Scope and the Component Supplier Question

## 2.1 What the Regulation Covers

The CRA applies to products with digital elements "made available on the EU market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network."[1] In practice, "indirect" connection covers any device reachable through a USB, serial interface, or local network. Virtually all embedded products qualify. The CRA explicitly includes software or hardware components sold separately - such as a microprocessor sold to an OEM for integration - within its definition of a product with digital elements.

TI's microprocessors and microcontrollers which are sold as components for integration into larger systems are products with digital elements. Both TI and the OEM who integrates TI silicon into a finished device are manufacturers under this definition but for different products and with different requirements.

The CRA excludes several product categories from its scope, including motor vehicles covered by Regulation (EU) 2019/2144, medical devices under Regulation (EU) 2017/745, and civil aviation equipment under Regulation (EU) 2018/1139. Customers whose end products fall under sectoral regulations need to confirm the applicable compliance path with their legal teams.

## 2.2 How the CRA Classifies TI Products

The CRA groups products into four risk categories. Most products with digital elements fall into the default category and face the baseline set of requirements. Higher-risk product types are classified as important - either Class I or Class II. The most sensitive products are designated critical.

Any microprocessor or microcontroller that includes built-in security features is Class I under the CRA. Class I applies to microprocessors with cryptographic accelerators, hardware secure boot, or protected key storage. A separate, stricter Class II category applies to chips with hardware tamper resistance features such as physical protection designed to prevent an attacker from extracting secrets or modifying behavior even with direct physical access to the device. Microprocessors without tamper resistance are Class I, even if these microprocessors support virtualization. The hypervisor software running on the device is classified separately.

TI's Jacinto™ and Sitara™ processor families are Class I. The TDA54x SoC/processor is also Class II because this device incorporates tamper-resistance features.

Class I and Class II products must go through a more rigorous approval process before being sold in the EU.The regulation describes three ways to demonstrate compliance. The first method is through a self-assessment process (only for Class I) based on formally recognized European technical standards called harmonized standards (EN50765 under development). The second is through a notified body. For example, an EU-notified third-party lab can review and certify the product (includes both Class I and Class II). Module H is the third option. A notified body audits the manufacturer's design, development, and vulnerability handling processes once. Once approved, the manufacturer certifies future products without additional review. Module H applies to Class I and Class II products, and critical products.

This classification applies to TI's products and to TI's conformity obligations, not to the OEM's finished product. An OEM integrating a default or Class I/II TI component into a connected system must separately determine the classification of their end product.

## 2.3 The Integration Boundary

Product manufacturers integrating a TI component and placing the finished system on the EU market do not inherit TI's component-level compliance.

The CRA applies to any entity that places a product on the EU market under its name. When an OEM places a connected device incorporating a TI processor on the EU market, the OEM becomes the manufacturer of that device and carries the full set of compliance requirements for the product as a whole. TI's requirements as a component manufacturer are additional, not a substitute.

TI provides compliance artifacts and hardware capabilities that feed directly into the product manufacturer's evidence package. The OEM's product-level SBOM builds on TI's SBOM and covers the full product. TI CVE advisories feed into the OEM's vulnerability handling process as inputs.



Copyright © 2026 Texas Instruments Incorporated

# 3 Shared Responsibility Model

## 3.1 The Supply Chain Stack

Most embedded products incorporating TI silicon follow a layered supply chain: TI silicon at the foundation, TI SDK providing the firmware and software stack above the silicone, a Tier 1 manufacturer or SoM vendor integrating silicon and SDK into a board or module, and the OEM building the final product on top. The supply chain responsibility stack maps this stack and aligns the CRA requirements alongside each layer.

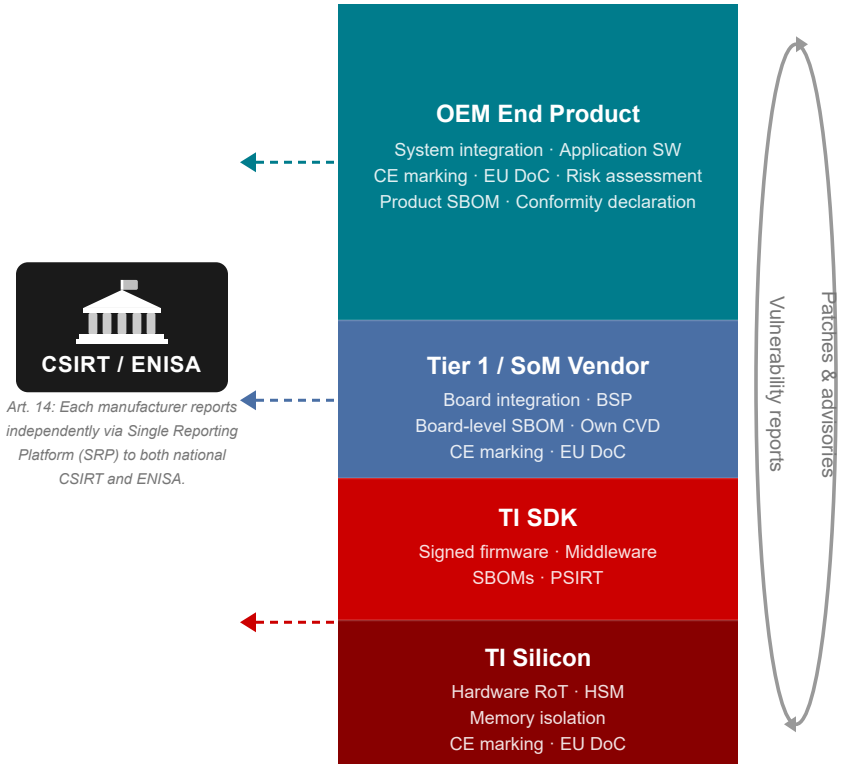



**Figure 3-1. CRA Shared Responsibility Across the Supply Chain**

Section 3.1 shows how the CRA responsibilities are shared throughout the supply chain. TI addresses hardware- and component-level requirements (bottom two layers). Tier 1 suppliers and SoM vendors carry intermediate integration requirements. The OEM holds full product-level conformity responsibilities. Patches, advisories, and vulnerability reports form a circular disclosure loop (right oval, clockwise). Article 14 requires each manufacturer in the supply chain to independently report actively exploited vulnerabilities; national CSIRT and ENISA are notified concurrently at each manufacturer level (dashed arrows) - see Article 14 - Reporting Obligations for Manufacturers for reporting timelines and obligations by layer. Regulation (EU) 2024/2847 (Cyber Resilience Act).

The vulnerability disclosure chain in the supply chain responsibility stack shows how security advisories and patch obligations flow upward through the stack:

1. TI issues a CVE advisory through TI-PSIRT
2. The Tier 1 or SoM vendor incorporates that advisory into a board-level update and passes the advisory to their OEM customers
3. The OEM patches the product and delivers the update to end users. If the vulnerability is being actively exploited, TI notifies the national CSIRT and ENISA concurrently under Article 14.

The Tier 1 or SoM vendor and the OEM carry the same obligation independently if either party becomes aware of an actively exploited vulnerability in the end product.


Copyright © 2026 Texas Instruments Incorporated

The CRA requires manufacturers to report two types of security events, each with a three-step notification sequence. The first - Track 1 - applies to actively exploited vulnerabilities such as known flaws in the product that attackers are using against users. Track 2 applies to severe incidents with a security impact on the product such as events that affect, or can affect, the ability of the product to protect the availability, authenticity, integrity, or confidentiality of data or functions, or that have led or can lead to the introduction or execution of malicious code in the product or in a user's systems. All notifications under both tracks are submitted simultaneously to the national CSIRT designated as coordinator and to ENISA through the CRA Single Reporting Platform.

**Table 3-1. Article 14 - Reporting Obligations for Manufacturers**

| Deadline | Content (verbatim) |
|---|---|
| **Track 1: Actively Exploited Vulnerability (Art. 14(1)-(2))** | |
| Within 24 hours of becoming aware | "an early warning notification of an actively exploited vulnerability...indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available" |
| Within 72 hours of becoming aware | "a vulnerability notification...which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take" |
| No later than 14 days after a corrective or mitigating measure is available | "a final report...including at least: (i) a description of the vulnerability, including its severity and impact; (ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability; (iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability" |
| **Track 2: Severe Incident with Impact on Security (Art. 14(3)-(4))** | |
| Within 24 hours of becoming aware | "an early warning notification of a severe incident having an impact on the security of the product with digital elements...including at least whether the incident is suspected of being caused by unlawful or malicious acts" |
| Within 72 hours of becoming aware | "an incident notification...which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take" |
| Within 1 month of the 72h incident notification submission | "a final report...including at least: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures" |

Track 1 applies when a known flaw in the product is being actively exploited, and the reporting clock is tied to vulnerability discovery and remediation. Track 2 applies when a security event has already affected the product or the users, regardless of whether a specific vulnerability has been identified. The reporting clock for Track 2 is tied to the occurrence of the incident. The two tracks are not mutually exclusive. An actively exploited vulnerability that results in a security breach triggers both simultaneously, and each event requires an independent set of notifications.

## 3.2 Responsibility Allocation by CRA Requirement

Section 3.2 lists the main CRA requirements to each party in the supply chain. Where a manufacturer is not physically established in the EU, the CRA requires them to appoint an authorized EU representative. This representative is a locally registered entity that can receive regulatory communications and act on the behalf of the manufacturer. The allocation reflects TI's interpretation of a typical embedded product supply chain. Specific products and supply chain arrangements can result in different allocations, however, Section 3.2 is not a substitute for product-specific compliance analysis.

**Table 3-2. CRA Obligation Allocation Across the Supply Chain**

| CRA Requirement | Regulation Reference | TI (Component Manufacturer) | Tier 1 / SoM Vendor | OEM Product Manufacturer |
|---|---|---|---|---|
| Cybersecurity risk assessment | Art. 13(2) | Chip-level threat model; security datasheet | Board-level risk assessment | Product-level risk assessment covering the full system |
| SBOM - top-level dependencies | Annex I, Part II, item 1 | SBOMs (SPDX, CycloneDX); secure SW using MySecure | Board-level SBOM | Product SBOM integrating all supplier SBOMs and own application software |



Copyright © 2026 Texas Instruments Incorporated

**Table 3-2. CRA Obligation Allocation Across the Supply Chain (continued)**

| CRA Requirement | Regulation Reference | TI (Component Manufacturer) | Tier 1 / SoM Vendor | OEM Product Manufacturer |
|---|---|---|---|---|
| No known exploitable vulnerabilities at release | Annex I, Part I, item 2(a) | SDK scanned before each release | Board (BSP) software scanned before release. Vendors also provide the SDK and other SW. | Full product scanned for known vulnerabilities before EU market placement |
| Secure by default configuration | Annex I, Part I, item 2(b) | Hardware root of trust and secure boot capability available; ROM-enforced on security-enforced device variants | Board defaults configured | Product shipped in secure default state; customer instructions provided; customer forced to change defaults like password |
| Security updates possible | Annex I, Part I, item 2(c) | Firmware patches delivered through the CI/CD pipeline or secure folder (based on sensitivity). PSIRT/PSAP tracks and communicates patch status. | Board update mechanism | Delivery of updates to end users; free of charge |
| Protection from unauthorized access | Annex I, Part I, item 2(d) | Hardware access control; debug port control | Board-level authentication | Product-level authentication and access management |
| Integrity protection | Annex I, Part I, item 2(f) | Signed firmware architecture supports boot integrity; cryptographically enforced on security-enforced device variants | Firmware signing for board components | System-level integrity verification |
| Limit attack surfaces | Annex I, Part I, item 2(j) | Hardware isolation | Board interface configuration | Product interface minimization and hardening |
| Security test reports for product security testing and vulnerability handling | Annex I Part I, Annex I Part II & Annex VII(6) | Test reports covering component-level security features. Updated reports for each component-level vulnerability fix. | Test reports covering board-level security integration. Updated reports for each board-level vulnerability fix. | Test reports covering end product security features. Updated reports for each product-level vulnerability fix. |
| CE marking | Art. 29-30 | Required on TI components placed on the EU market | Required if Tier 1 places module on EU market independently | Required on the end product |
| Authorized EU representative | Art. 18 | TI maintains EU presence | Required if Tier 1 is not established in EU | Required if OEM is not established in EU |
| Coordinated vulnerability disclosure (CVD) policy | Annex I, Part II, item 5 | TI PSIRT policy | Tier 1 own CVD policy | OEM own CVD policy for their product |
| Vulnerability reporting contact | Annex I, Part II, item 6 | psirt@ti.com | Tier 1 security contact | OEM security contact published to end users |
| Report actively exploited vulnerabilities | Art. 14 | TI notifies national CSIRT and ENISA concurrently using the CRA Single Reporting Platform - see Article 14 - Reporting Obligations for Manufacturers for the full notification sequence. | Tier 1 notifies national CSIRT and ENISA concurrently - see Article 14 - Reporting Obligations for Manufacturers for the full notification sequence. | OEM notifies national CSIRT and ENISA concurrently - see Article 14 - Reporting Obligations for Manufacturers for the full notification sequence. |
| Support period declaration | Annex II, item 7 | Lifecycle guide per device family | Module support period declared | Product support period declared to end users |
| Technical documentation | Art. 31 | Component-level technical documentation | Module-level technical documentation | Full product technical documentation |

## 3.3 The Tier 1 and SoM Vendor Layer

Many TI customers operate through a Tier 1 board manufacturer or SoM vendor that bridges between TI and the OEM. When the Tier 1 or SoM vendor places a board or module on the EU market under its name, that vendor is a manufacturer and carries CRA requirements. When the vendor operates as a contract manufacturer under OEM direction without placing a product on the market under their name, CRA manufacturer obligations fall entirely on the OEM. Similarly, in a chip-down design, the OEM integrates TI silicon directly with no Tier 1 or SoM vendor in between, so the OEM alone carries product level obligations.


Copyright © 2026 Texas Instruments Incorporated

A Tier 1 or SoM vendor acting as a manufacturer must generate a board-level SBOM that incorporates TI's SDK SBOM, maintain its own CVD policy and disclosure contact, and provide security documentation to downstream integrators.

Selecting a board or module from a Tier 1 vendor with CRA compliance processes does not remove the OEM's requirement to perform a product-level risk assessment, produce a product-level SBOM, and declare conformity for the finished product. Each role's requirements attach to the product they place on the market under their name.

# 4 TI's Security Capabilities Relevant to CRA

TI designs security-capable device families to address hardware and component-level requirements of Annex I. For device-specific implementation guidance, see the applicable device datasheet, security user guides, and *Securing the Future: CRA Compliance With TI's Jacinto and Sitara Processors* technical white paper.

## 4.1 Hardware Security Capabilities

Security-capable TI processors include a dedicated security subsystem that runs on cores isolated from the main application processors and enforces the hardware root of trust through TI-supplied firmware (TI Foundational Security - TIFS). On newer-generation devices, a second dedicated security core is available for customer HSM software stacks, enabling cryptographic services without exposing key material to application-domain software.

A public key permanently provisioned into the silicon at production time anchors secure boot. On security-enforced (HS-SE) device variants, the boot ROM verifies a digital signature on the primary firmware image before execution and rejects images that fail verification, providing hardware-enforced integrity and authenticity verification from power-on.

Hardware access control partitions on-chip memory into zones assigned to each processing domain, preventing unauthorized reads or writes across workload boundaries.

On security-capable device variants, the debug interface can be permanently disabled for production units, or restricted to access only after a request is authenticated through a signed certificate, closing common attack vectors that exploit debugging tools.

Each chip carries a unique die ID alongside the part number, enabling precise identification of the specific silicon instance and supporting product identification requirements.

## 4.2 SDK and Software Security

TI provides SBOMs in SPDX and CycloneDX formats for all products for which public source code is available as part of SDK on ti.com. SBOMs for secure software components are available through TI's MySecure access program.

TI processor SDKs are scanned for known vulnerabilities before each release. TI manages the full vulnerability handling lifecycle through PSIRT: notification intake, triage, technical analysis, remediation, and coordinated public disclosure with CVSS v3.1 severity scoring and CVE assignment. The process aligns to ISO/IEC 30111 and ISO/IEC 29147. TI provides security patches free of charge with advisory messages.

TI delivers patches and advisories through the product security advisory portal (PSAP) at ti.com/psap. PSAP gives customers a structured channel to report vulnerabilities through myTI accounts, subscribe to advisory feeds scoped to the TI products in their designs, and access disclosures in CSAF v2.0 machine-readable format. CSAF v2.0 advisories reference the specific software components affected, enabling customers to automate correlation against their SBOMs and assess exposure within their CRA reporting timelines.

TI publishes a security.txt file at ti.com/.well-known/security.txt per BSI TR-03183-3 and RFC 9116. The text file contains the PSIRT contact address, CVD policy URI, and CSAF provider metadata. TI operates under German jurisdiction, and TI's designated national CSIRT for Article 14 reporting is CERT-Bund, operated by the German Federal Office for Information Security (BSI). TI submits incident notifications through the CRA Single Reporting Platform within the required timelines.

Article 14 requires manufacturers to notify the appropriate national CSIRT within 24 hours of "becoming aware" of an actively exploited vulnerability. The regulation does not define the moment awareness is established in a multi-person organization. Manufacturers define in advance what constitutes awareness in their organization,



Copyright © 2026 Texas Instruments Incorporated

whether at intake acknowledgment or when the responsible technical team member first reviews the report, however, an undefined clock creates compliance risk. The 24-hour window starts at that defined moment, not when an individual engineer reviews the report. The automated deadline tracking from PSAP enforces this by escalating reports before the window closes. Any actively exploited vulnerability known to TI triggers this 24-hour deadline, whether the information arrives from a security researcher, a customer, or internal discovery. The 72-hour notification follows with a fuller assessment, submitted simultaneously to the national CSIRT and ENISA through the CRA Single Reporting Platform.

### 4.3 Documentation and Lifecycle Artifacts

TI publishes a detailed datasheet for each device family documenting hardware security features and interface specifications. A dedicated update policy describes when and how TI delivers firmware patches. The lifecycle guide for each device specifies the support period and warranty scope.

User guides cover secure boot setup, debug port configuration, and HSM integration.

## 5 Conclusion

CRA compliance for connected products with digital elements requires coordinated action across the supply chain. Each party has distinct requirements; none substitutes for another's.

TI addresses its role as a component manufacturer: hardware root of trust and memory isolation on security-capable device variants, signed firmware, SBOMs, a PSIRT process aligned to CRA Article 14 reporting timelines, and device-level documentation covering the information requirements of the CRA. Product manufacturers and Tier 1 vendors incorporate these capabilities and artifacts into their compliance work. They remain responsible for the product-level compliance that TI cannot address on their behalf.

The product manufacturer placing a connected device on the EU market must conduct a product-level cybersecurity risk assessment, generate a product-level SBOM, declare conformity, apply CE marking, and appoint an authorized EU representative if not established in the EU. They must also maintain processes to notify the national CSIRT and ENISA concurrently within 24 hours of becoming aware of an actively exploited vulnerability, with a fuller assessment due within 72 hours - see Article 14 - Reporting Obligations for Manufacturers for the complete notification sequence. TI's PSIRT advisories and SBOMs feed into that process.

To evaluate how TI's device capabilities map to your CRA requirements, engage TI's security team and review the PSIRT policy at ti.com/quality-reliability/quality/ti-psirt.html. Consult your legal and compliance teams for product-specific guidance. Vulnerability reporting requirements under Article 14 are already in effect. Full CRA enforcement arrives December 2027; product manufacturers building connected devices for the EU market need their compliance assessment underway now.

## 6 References

1. European Parliament and Council of the European Union (2024, November 20). "Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).". Official Journal of the European Union, L series.
2. Texas Instruments. "TI PSIRT." webpage
3. Texas Instruments. "Cyber Resilience Act (CRA)." webpage
4. Texas Instruments, *Securing the Future: CRA Compliance With TI's Jacinto and Sitara Processors* technical white paper
5. Texas Instruments, *Fortifying Compliance: Streamlining Cybersecurity Vulnerability Management* application brief


Copyright © 2026 Texas Instruments Incorporated

# IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025