Application Brief

Fortifying Compliance: Streamlining Cybersecurity Vulnerability Management

Daniel Ogilvie — *Portfolio Marketing Engineer, Worldwide Marketing*
Bhargavi Nisarga — *SMTS Systems manager, Application Specific MCUs TI PSIRT Co-chair*

At a glance

This paper provides an overview of TI's vulnerability management approach, its alignment with CRA requirements, and how PSAP supports TI and its customers in meeting compliance obligations collaboratively across the supply chain.

1 Vulnerability management

A foundational cybersecurity practice encompassing the identification, analysis, risk-based prioritization, remediation, and coordinated disclosure of security vulnerabilities.

2 European Union Cyber Resilience Act (CRA)

Establishes binding obligations for hardware and software product developers, organizations must implement robust vulnerability management and a processes for coordinated vulnerability disclosure (CVD) or face steep financial penalties and reputational damage.

3 Texas Instruments' (TI) PSIRT (Product Security Incident Response Team)

TI's long maintained mature process to manage vulnerability reports across its semiconductor product portfolio. Building on this foundation, TI is deploying the Product Security Advisory Portal (PSAP)—a purpose-built platform that streamlines vulnerability intake, triage and remediation, coordinated disclosure, and regulatory reporting.

How Texas Instruments Supports EU Cyber Resilience Act Compliance Across the Manufacturing Supply Chain

Modern electronic products are built on complex, multi-tiered supply chains that potentially involve multiple IP suppliers, tier-2 semiconductor manufacturers, tier-1 system integrators, and finally the end-product by OEMs (original equipment manufacturer). A vulnerability at any link in this chain—whether in silicon, firmware, or software—can propagate to the finished product and its end users. Effectively, managing these risks demands frameworks that enable timely, reliable, and collaborative vulnerability handling across all stakeholders.

The EU Cyber Resilience Act, which enters enforcement in phases—with reporting obligations taking effect on 11 September 2026 and full compliance required by 11 December 2027—establishes legally binding vulnerability management requirements for products with digital elements sold in the European market. Manufacturers must implement coordinated vulnerability disclosure processes, maintain software bills of materials (SBOMs), and meet prescribed incident-reporting timelines—including 24-hour early warnings to the relevant Computer Security Incident Response Teams (CSIRT) upon becoming aware of actively exploited vulnerabilities or severe incidents.

As a global semiconductor supplier, TI occupies a critical position in this supply chain. This paper describes how TI's vulnerability management practices—anchored by a mature PSIRT process and a new Product Security Advisory Portal—are designed to meet CRA obligations and enable customers to satisfy their own regulatory requirements.

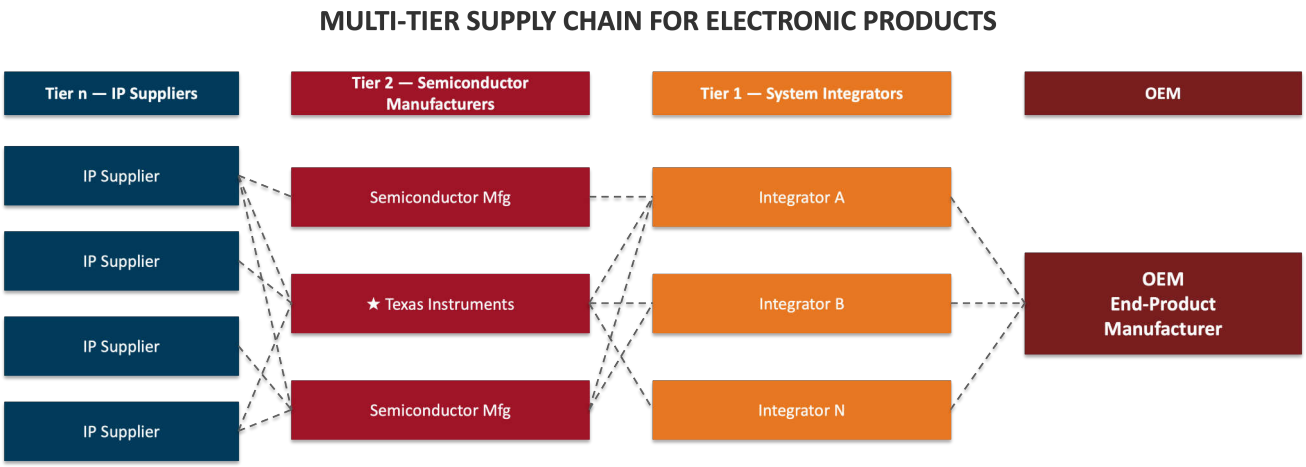

Figure 1. A Vulnerability at Any Tier Can Propagate Downstream to the Finished Product and End Users

The EU Cyber Resilience Act and Vulnerability Management

The CRA enforces comprehensive cybersecurity requirements on products with digital elements throughout their lifecycle. For vulnerability management, the regulation mandates that manufacturers:

- Implement and maintain a coordinated vulnerability disclosure (CVD) policy
- Provide a mechanism for external parties to report vulnerabilities
- Generate and maintain SBOMs for their products
- Report applicable actively exploited vulnerabilities and severe incidents to the **corresponding national CSIRT** and ENISA, within prescribed timelines
- Provide security updates for the product's support period
- **Publicly disclose validated and verified vulnerabilities within prescribed timelines**

Non-compliance with these obligations can result in administrative fines of up to EUR 15 million or 2.5% of global annual turnover (whichever is higher). For semiconductor suppliers and their OEM customers alike, meeting these obligations requires tightly integrated processes and tooling across the supply chain.

Corresponding National CSIRT

The CRA requires manufacturers to identify and engage a "corresponding national CSIRT" — the CSIRT designated by their EU Member State as coordinator for coordinated vulnerability disclosure purposes. Manufacturers must notify this CSIRT without undue delay upon becoming aware of an actively exploited vulnerability and must keep it informed of all new information, mitigation measures, and their schedules throughout the CVD process. Manufacturers should designate the same national CSIRT consistently across all vulnerability handling engagements. For manufacturers operating under German jurisdiction, such as Texas Instruments, the expected designated national CSIRT is **CERT-Bund**, operated by the Federal Office for Information Security (BSI).

TI's Product Security Incident Response Team

TI's PSIRT serves as the single point of contact for receiving, coordinating, tracking, and responding to reports of potential security vulnerabilities in TI semiconductor products. TI PSIRT representatives and the respective product technical teams handle the technical analysis, remediation and disclosure of product vulnerabilities providing consistent, company-wide vulnerability handling.

PSIRT Process Overview

The TI PSIRT process follows established industry practices aligned with international standards including ISO/IEC 30111 (Vulnerability handling processes) and ISO/IEC 29147 (Vulnerability disclosure). Key PSIRT stages include:

1. **Intake and acknowledgment**: Vulnerability reports are received through designated channels and acknowledged in a timely manner.
2. **Triage and analysis**: Reports are triaged, classified, and assigned to the appropriate product team for technical investigation. Product teams analyze and verify the reported vulnerabilities and assess its potential impact.
3. **Remediation**: Fixes, mitigations, or workarounds are developed and tested by the responsible product teams.
4. **Coordinated disclosure**: Advisories are prepared, reviewed by cross-functional stakeholders (quality, legal, communications), and published through TI's advisory channels.
5. **Regulatory reporting**: Where required by the CRA or other regulations, incident notifications are submitted to the relevant CSIRT using the CRA Single Reporting Platform within prescribed timelines.

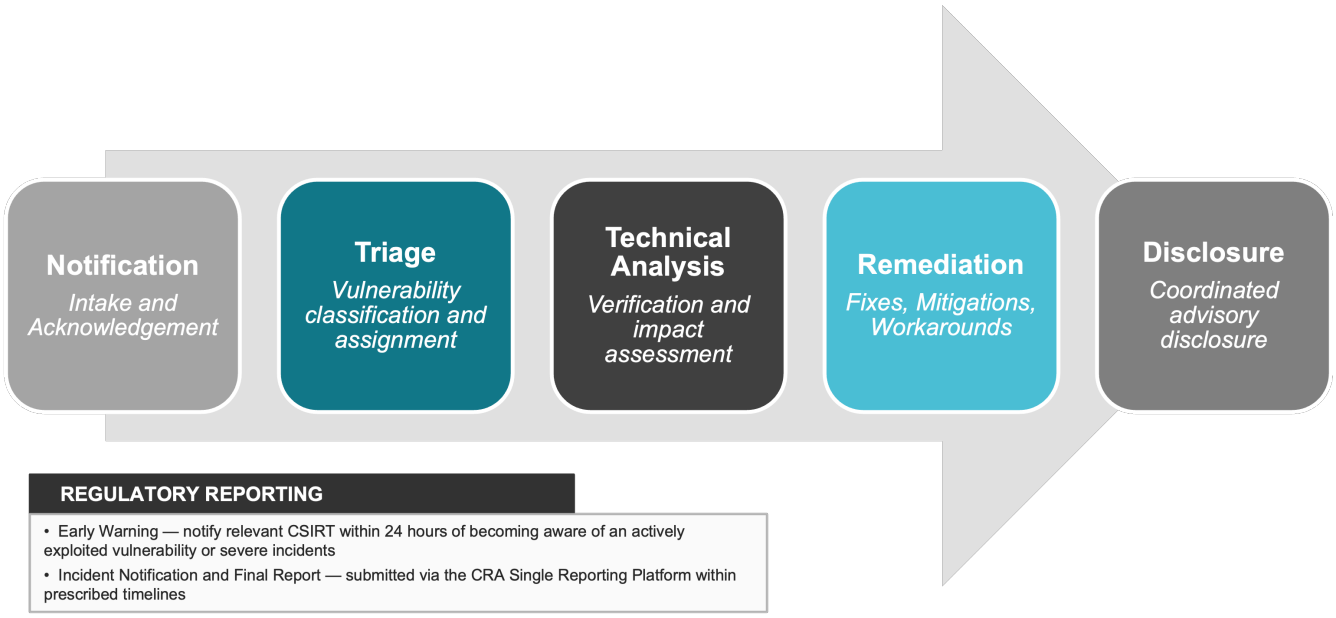

Figure 2. The PSIRT Process

The PSIRT's responsible handling policy (SSZO001) is publicly available and defines the expectations for external researchers and reporters engaging with TI on vulnerability matters.

Product Security Advisory Portal (PSAP)

To scale its vulnerability management capabilities to meet CRA requirements and the growing complexity of the multi-tiered supply chain, TI has developed the Product Security Advisory Portal (PSAP). PSAP is a purpose-built web application that provides a unified interface for vulnerability reporting, tracking, communication, and disclosure for both internal teams and external stakeholders.

For Customers and External Reporters

PSAP provides customers and external reporters with the following capabilities:

- **Vulnerability reporting**: Submit vulnerability reports securely and directly to TI through a structured form accessible through myTI™ on-line information services accounts, providing a clear and traceable reporting channel.

- **Secure communication**: Exchange private messages and files with TI PSIRT teams throughout the technical analysis and remediation phases.
- **Advisory notifications**: Subscribe to public security advisory notifications and access published disclosures through the PSAP dashboard.
- **Machine-readable advisories**: Access disclosures in CSAF v2.0 format, enabling automated ingestion into customers' own vulnerability management systems.

PSAP also equips TI internal product teams to adhere to EU CRA vulnerability management in a structured and collaborative way, including support for:

- Automated CRA deadline tracking
- Coordinated communication handling for the full vulnerability lifecycle—from notification through triage, technical analysis, remediation, and disclosure
- Escalation mechanisms to ensure CRA incident reporting timelines are met
- Disclosure authoring tools that generate advisories in both human-readable (HTML) and machine-readable (CSAF v2.0) formats
- Multi-stakeholder review and approval workflows involving quality, legal, and communications teams before publication

security.txt publication

In accordance with BSI TR-03183-3 and RFC 9116, TI publishes a security.txt file at https://www.ti.com/.well-known/security.txt. This file includes:

- TI PSIRT contact email address (psirt@ti.com)
- Link to TI's public vulnerability reporting web page
- OpenPGP public key URIs for both PSIRT and CSIRT functional mailboxes
- URI of TI's CVD policy
- URI of the CSAF provider-metadata.json for machine-readable advisory access
- Expiry date (set no more than one year in the future, reviewed quarterly)

The security.txt file is accessible to web crawlers and is not blocked by firewall or DDoS protection rules. The corresponding OpenPGP public key used for signing is published on TI's vulnerability reporting web page.

PSIRT Advisories

PSIRT advisories include vulnerability details (CVE identifiers where available), reviewed CVSS Base Scores, impacted products (hardware and software), and suggested mitigations, consistent with ISO/IEC 29147 (vulnerability disclosure) and the security advisory definition in BSI TR-03183-3. Advisories are published in both human-readable (HTML) and machine-readable (CSAF v2.0) formats, with the CSAF distribution conforming to the provider metadata requirements of BSI TR-03183-3 and ISO/IEC 20153:2025.

Software Bill of Materials and Supply Chain Transparency

The CRA requires manufacturers to produce and maintain Software Bills of Materials for their products. An SBOM is a machine-readable inventory of software components, their versions, provenance, license information, and dependency relationships. SBOMs enable downstream users to (i) track and comply with SW components' licensing requirements, (ii) identify which components are present in a product and to rapidly assess exposure when new vulnerabilities are disclosed, and (iii) ensure adherence to industry standards and regulations.

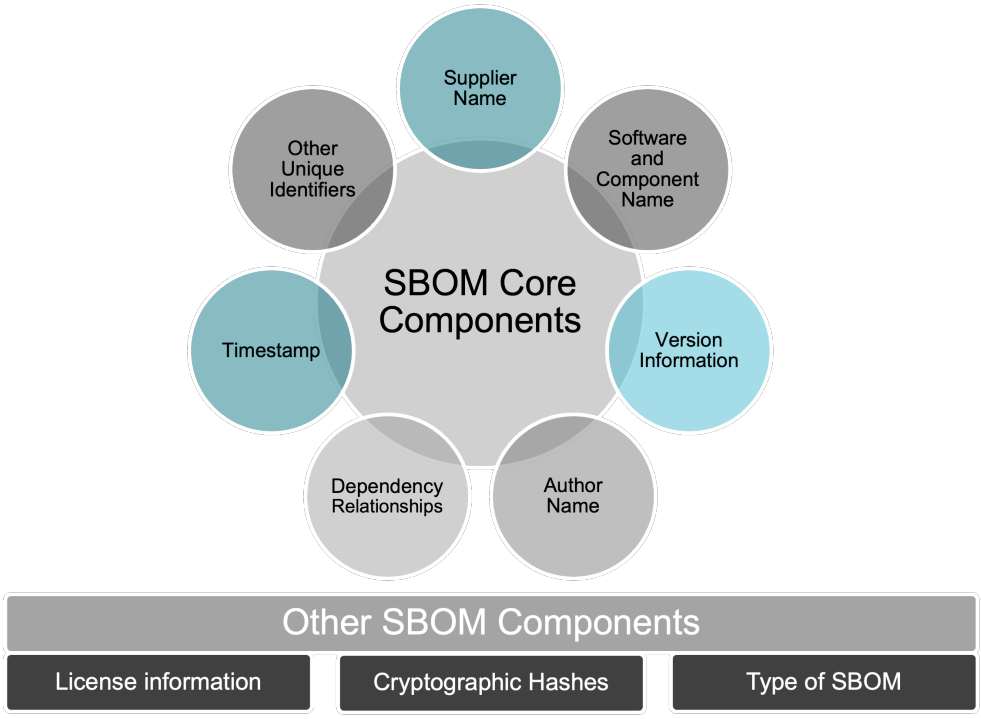

Figure 3. The Components of an SBOM

TI is advancing its SBOM capabilities to support industry-standard formats—including SPDX and CycloneDX—across its software portfolio. TI's PSIRT advisory process is being integrated with SBOM data so that published advisories, delivered in CSAF v2.0 format, can be directly correlated against SBOMs by customers' automated vulnerability management tooling. Where a vulnerability is disclosed, TI's CSAF advisories reference the specific software components affected, enabling customers to rapidly determine whether their designs are in scope—a capability that directly supports their own CRA compliance obligations.

The use of SBOMs is endorsed by multiple global regulatory and cybersecurity authorities, reflecting a convergent international trend toward software supply chain transparency:

- European Union: Required under the CRA for products with digital elements sold in the EU market
- Germany (BSI): BSI TR-03183-3 requires SBOM data to be integrated with machine-readable CSAF v2.0 advisory distribution to enable downstream CVD compliance
- United States: Mandated by the U.S. Executive Order on Improving the Nation's Cybersecurity (May 2021) and endorsed by CISA as a foundational software supply chain security practice
- UK, Australia, Canada: National cybersecurity agencies in these countries have each published guidance endorsing SBOM adoption as part of broader software supply chain transparency initiatives

This global convergence means that TI's investment in SBOM capabilities and CSAF-based advisory distribution serves compliance obligations across multiple jurisdictions simultaneously—not only the EU CRA.

SBOM Integration With the CVD Process

TI is integrating its SBOM capabilities directly with the PSAP advisory workflow so that:

- When a vulnerability is reported and validated, the affected software components can be identified from the relevant SBOM and automatically scoped into the advisory
- CSAF v2.0 advisories published through PSAP reference affected component versions in a format directly consumable by customers' SBOM-aware vulnerability management tools
- Customers who maintain SBOMs for their own products incorporating TI software are able to automate the correlation of TI advisories against their component inventory, reducing manual triage effort and accelerating their own CRA reporting timelines

This approach is consistent with the CSAF provider requirements of BSI TR-03183-3 (§4.2.8) and the ISO/IEC 20153:2025 standard for machine-readable security advisory distribution.

Enabling Customer Compliance

Under the CRA, compliance obligations flow through the supply chain. OEMs and integrators who incorporate TI components into their products are themselves required to manage vulnerabilities and report incidents. TI's approach is designed to make this downstream compliance practical and efficient:

- **Timely advisories**: Customers receive vulnerability details and suggested mitigations in a timely manner so they can assess impact and take actions within their own CRA timelines.
- **Machine-readable data**: CSAF v2.0 advisories and SBOMs allow customers to automate vulnerability correlation and risk assessment rather than relying on manual processes.
- Subscription-based notifications: Customers can subscribe to advisory feeds relevant to the TI products in their designs, reducing noise and receiving only the information that matters to them.
- **Coordinated disclosure**: TI's CVD process notifies customers and supply chain partners before public disclosure where appropriate, allowing time for mitigation.
- **Secure collaboration**: PSAP's private messaging capabilities enable confidential, traceable communication between customers and TI throughout the vulnerability lifecycle.
- **CVD policy transparency**: TI's CVD policy (SSZO001) is publicly available, clearly dated, and reviewed at least annually. The policy sets out TI's assurances to reporting entities, providing customers and researchers with a clear and predictable engagement framework

Conclusion

The EU Cyber Resilience Act marks a significant shift in regulatory expectations for cybersecurity across the product lifecycle. For semiconductor suppliers and their customers, compliance requires not only robust internal processes but also effective collaboration across the supply chain.

TI's approach—built on a mature PSIRT process and operationalized through the Product Security Advisory Portal—is designed to meet these requirements while enabling customers to manage their own compliance obligations. By combining vulnerability monitoring, structured incident response, machine-readable advisories, SBOM support, and secure communication channels, TI is committed to advancing cybersecurity resilience across the semiconductor supply chain.

For more information about TI's product security practices, visit ti.com/psap or contact the TI PSIRT at psirt@ti.com.

References

1. BSI (Bundesamt für Sicherheit in der Informationstechnik). (2025). *Cyber resilience requirements for manufacturers and products, Part 3: Vulnerability reports and notifications* (Technical Guideline TR-03183-3, v1.0.0).
2. European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*.International Organization for Standardization. (2018). *Information technology — Security techniques — Vulnerability disclosure* (ISO/IEC 29147:2018).
3. European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.
4. European Union Agency for Cybersecurity (ENISA). (2025). *European Vulnerability Database (EUVD)*. Retrieved July 21, 2026
5. International Organization for Standardization. (2019). *Information technology — Security techniques — Vulnerability handling processes* (ISO/IEC 30111:2019).
6. International Organization for Standardization. (2018). *Information technology — Security techniques — Vulnerability disclosure* (ISO/IEC 29147:2018).

7. National Institute of Standards and Technology. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). U.S. Department of Commerce.
8. OASIS Open. (2022). *Common Security Advisory Framework (CSAF) Version 2.0* (OASIS Standard).
9. Texas Instruments Incorporated. (2023). *TI PSIRT Responsible Handling Policy*
10. U.S. Executive Office of the President. (2021). *Executive Order 14028: Improving the nation's cybersecurity*. Federal Register, 86(93), 26633–26647.

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.

Last updated 10/2025