

# CISA Secure Software Development Attestation Form (SSDAF)

SSDAF provides a standardized self-attestation for software producers to declare adherence to secure development practices and improve supply chain transparency.



## What it is

### At a glance

|                                                                                         |                                                            |                                                          |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------|
| <div>PUBLISHER</div> <div>Cybersecurity and Infrastructure Security Agency (CISA)</div> | <div>TYPE</div> <div>Guidance</div>                        | <div>VERSION</div> <div>2024</div>                       |
| <div>EFFECTIVE</div> <div>March 11, 2024</div>                                          | <div>DOMAIN</div> <div>Software Security</div>             | <div>FAMILY</div> <div>Other</div>                       |
| <div>REGION</div> <div>United States</div>                                              | <div>ADOPTION MODEL</div> <div>Regulatory Compliance</div> | <div>IMPLEMENTATION COMPLEXITY</div> <div>Moderate</div> |

Source: <https://www.cisa.gov/secure-software-attestation-form>

## Why it matters

- Support stronger supply chain security** Require software providers to attest to secure development, limiting risks from third-party software procurement and integration.
- Enhance regulatory compliance** Enable organizations to demonstrate alignment with federal cybersecurity standards, improving their ability to meet compliance obligations during audits.
- Increase software transparency** Promote greater visibility into suppliers' development practices, enabling informed risk management and procurement decisions.
- Improve incident response readiness** Mandate secure development controls that reduce exploitable vulnerabilities and support more effective detection and remediation of software-based threats.

How SmartSuite supports CISA SSDAF

Secure Development Requirement Library

Structure SSDAF secure software development requirements with mapped controls and responsible owners.

Secure Software Development Lifecycle Governance

Track security activities across design, coding, testing, and deployment stages of software development.

Vulnerability and Dependency Management

Monitor software vulnerabilities, open-source dependencies, and remediation workflows across development pipelines.

Build Integrity and Release Governance

Document build processes, code signing, artifact integrity checks, and release approvals.

Third-Party Software and SBOM Tracking

Track third-party software components, vendor security attestations, and SBOM documentation.

SSDAF Federal Software Security Attestation Readiness

Provide dashboards showing SSDAF requirement coverage, evidence status, and readiness for federal software security attestations.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST SP 800-161 Rev.1

NIST 800-218 SSDF

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

CISA Secure Software Development Attestation Form

Defines self-attestation requirements for secure software development under U.S. CISA guidance.

[cisa.gov/resources-tools/resources/secure-software-development-attestation-form](https://cisa.gov/resources-tools/resources/secure-software-development-attestation-form)

CISA Secure Software Development Framework

Provides guidelines for employing secure software development practices to enhance security resilience.

[csrc.nist.gov/projects/ssdf](https://csrc.nist.gov/projects/ssdf)

CISA Cybersecurity and Infrastructure Security Guidance

Outlines implementation guidance focused on cybersecurity best practices for infrastructure security.

[cisa.gov/topics/cybersecurity-best-practices](https://cisa.gov/topics/cybersecurity-best-practices)

Frequently asked questions

What is the CISA Secure Software Development Attestation Form (SSDAF) used for?

The SSDAF is used to confirm that software producers have implemented secure software development practices as required under U.S. federal guidance, particularly for software provided to federal agencies. The form is designed to promote transparency and accountability by requiring organizations to self-attest to their software security practices.

Is completion of the SSDAF mandatory for software vendors?

Yes, completion and submission of the SSDAF is mandatory for organizations wishing to provide software to U.S. federal agencies, in line with Executive Order 14028 and OMB Memorandum M-22-18. Non-compliance can result in disqualification from federal procurement processes.

Which organizations or software products fall within the scope of the SSDAF?

The SSDAF applies to all software producers whose products are used by U.S. federal agencies, including both commercial off-the-shelf and custom-developed software. It covers both new and existing software that is subject to federal acquisition.

### **What key requirements or artifacts are needed to fulfill the SSDAF?**

Organizations must provide a completed attestation form and demonstrate adherence to secure software development practices, such as threat modeling, code review, vulnerability remediation, and supply chain security. Evidence may include documentation of policies, procedures, and technical controls supporting secure development.

### **How should organizations implement SSDAF requirements?**

Organizations should align their software development lifecycle with secure-by-design principles, integrating security controls such as secure coding standards, automated security testing, and third-party component risk assessments. Regular training and process reviews are also essential to ensuring continued compliance.

### **How does the SSDAF relate to other security frameworks or standards?**

The SSDAF draws on requirements from frameworks such as NIST SP 800-218 (Secure Software Development Framework) and aligns with federal security mandates, but it does not replace other certification regimes (like FedRAMP or FISMA). Organizations may reference existing controls and processes already implemented under these standards when completing the SSDAF.

### **What are the ongoing compliance requirements after submitting the SSDAF?**

Organizations must maintain secure software development practices continuously and update their attestation as changes occur. Periodic review, monitoring for emerging threats, and ongoing documentation are required to remain compliant with SSDAF obligations.

### **How would SmartSuite support U.S. CISA Secure Software Development Attestation Form (SSDAF)?**

SmartSuite can assist organizations in managing SSDAF compliance by providing centralized tracking of risks and controls, managing evidence collection across development teams, and supporting audit readiness with robust documentation. Automated workflows and reporting capabilities streamline ongoing compliance and demonstrate adherence to SSDAF requirements to auditors and regulators.

License included / downloadable: Yes CISA publishes the SSDAF on its website and is publicly available for free download from the U.S. CISA. License included with platform

Full framework page and mappings: [smartsuite.com/frameworks/cisa-secure-software-development-attestation-form-ssdaf](https://smartsuite.com/frameworks/cisa-secure-software-development-attestation-form-ssdaf)