LEGIT SECURITY

DATASHEET

Complying With NIST SSDF

What It Is

The National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF) is "a set of fundamental, sound practices for secure software development."

NIST created the SSDF standard as a result of the President's 2021 Executive Order (EO) on "Improving the Nation's Cybersecurity."

SSDF requirements are now mandatory for companies that want to sell their software to the government.

How Legit Can Help

Legit's platform is ideally suited to help organizations address the NIST SSDF requirements.

Legit helps organizations:

- Map policies directly to the SSDF framework.
- Perform automated gap analysis of SSDF compliance.
- Detect and alert on specific SSDF policy violations.
- Automate remediation workflows in response to SSDF policy violations.
- Establish automated guardrails to prevent future SSDF violations.

Practice Group and Control Policies Covered	Sample Policies
Prepare the Organization (PO): Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.	
PO 1 (1.1, 1.2) Define security requirements for software development. PO 2 (2.1) Implement roles and responsibilities in the SDLC. PO 3 (3.1, 3.2, 3.3) Implement supporting toolchains. PO 4 (4.1, 4.2) Define and use criteria for software security checks. PO 5 (5.1) Implement and maintain secure environments for software development.	Legit helps fulfill multiple components of PO 1. The platform performs automatic discovery to identify gaps in coverage and has specific policies in place to detect and alert on SSDF compliance violations. For example: • Ensure that recommended security practices to deploy, operate, and maintain tools and toolchains are followed. • Ensure that access logging is enabled. • Ensure that secure environments for software development are implemented and maintained.
Protect the Software (PS): Protect all components of the software from tampering and unauthorized access.	
PS 1 (1.1) Protect all forms of code from unauthorized access and tampering. PS 3 (3.1) Archive and protect each software release.	Legit has specific policies aligned to PS 1 to help protect code throughout the SDLC from improper access and tampering. For example: • Ensure default permissions exist for new repositories. • Ensure owners cannot approve their own pull requests.
Produce Well-Secured Software (PW): Produce well-secured software with minimal security vulnerabilities in its releases.	
PW 1 (1.2) Design software to meet security requirements and mitigate security risks. PW 4 (4.1, 4.2, 4.4) Reuse existing, well-secured software when feasible instead of duplicating functionality. PW 7 (7.1, 7.2) Review and/or analyze human-readable code to identify vulnerabilities and verify compliance with security requirements.	Legit helps enforce secure software design and development standards addressed in PW 4, with specific policies to ensure that recommended practices are followed. For example: • Verify that third-party/open-source software components have been scanned for vulnerabilities. • Ensure code is reviewed by one or more reviewers.
Respond to Vulnerabilities (RV): Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.	
RV 1 (1.2) Identify and confirm vulnerabilities on an ongoing basis. RV 2 (2.1) Assess, prioritize, and remediate vulnerabilities. RV 3 (3.1) Analyze vulnerabilities to identify their root causes.	Legit has extensive capabilities related to addressing RV 1 requirements. For example, policies include: • Identify and confirm vulnerabilities on an ongoing basis. • Analyze vulnerabilities to identify their root causes.

Learn more about how Legit is helping organizations comply with security regulations.
Visit our website and Book a Demo

LEGIT SECURITY

About Legit Security

Legit is a new way to manage your application security posture for security, product and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security, and address risks from code to cloud. Built for the modern SDLC, Legit tackles the toughest problems facing security teams, including GenAI usage, proliferation of secrets and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the success of the security program. This new approach means teams can control risk across the business – and prove it.