LEGIT SECURITY

DATASHEET

Addressing CISA Attestation

What

To be compliant with the NIST Secure Software Development Framework (SSDF), the Cybersecurity and Infrastructure Security Agency (CISA) requires high-level executives at organizations to sign an attestation form.

There are four main areas that need to be attested to:

- Secure Development Environments
- Secure Software Supply Chain
- Maintain Code and Artifact Provenance
- Check for Vulnerabilities

When

The form came out of commenting and was officially released on March 11th. There are now 3 and 6 month windows from that date for critical and non-critical respectively.

How Legit Can Help

Secure Development Environments

- **Secrets Detection** – Legit utilizes proprietary AI/LLM technology to find secrets across your entire SDLC, not just in code.
- **Developer Identification & Permissions** – The Legit platform can instantly tell you what collaborators are working on your products at all times, and can also give you a complete list of permissions associated with each collaborator.
- **SDLC Visibility** – Legit automatically and continuously discovers and maps all build tools and production environments, AI/LLMs, etc. across your entire development organization.

Secure Software Supply Chain

- **SDLC Hardening** – Legit offers the deepest and most comprehensive list of policies and best practices around protecting all the assets found in a software factory, including code repos, CI/CD systems, pipeline controls, IaC, and more.
- **SDLC Graph** – Legit enables you to fully understand how code progresses through your pipelines for complete traceability in all your products – from code repo > build tools > artifact registry > deployment.
- **Code to Cloud** – Legit instantly traces any issue found in production back to the associated code in seconds for easy and fast remediation.

Maintain Code and Artifact Provenance

- **Artifact Provenance** – Legit enables you to view and download provenance records instantly to verify and provide evidence that artifacts haven't been manipulated during the build process.
- **Complete Inventory** – Legit tracks all resources being used in development, in the build process, as well as in production, such as repos, container images, Kubernetes resources, packages, and more.

Check for Vulnerabilities

- **Single Source of Truth** – Legit aggregates, prioritizes, and remediates all issues from a single platform. With Legit, you can integrate with your existing application security tooling, which provides additional context about your business and development environments for better understanding of risk.
- **Control Mapping** – Legit provides complete visibility into where you have proper controls in place and, more importantly, where you are missing controls in order to get full coverage using your existing tools.
- **Extended Risk Visibility** – Legit provides additional vulnerability, misconfiguration, and risk identification into areas of the SDLC largely ignored by existing application security tools.

Get more details on CISA Attestation.

Contact us to get more information or request a demo.

Learn More About Legit Security

Visit our website and Book a Demo

LEGIT
SECURITY

About Legit Security

Legit Security provides an application security posture management platform that secures application delivery from code to cloud and protects an organization's software supply chain from attacks. The platform's unified application security control plane and automated SDLC discovery and analysis capabilities provide visibility and security control over rapidly changing environments and prioritize security issues based on context and business criticality to improve security team efficiency and effectiveness.