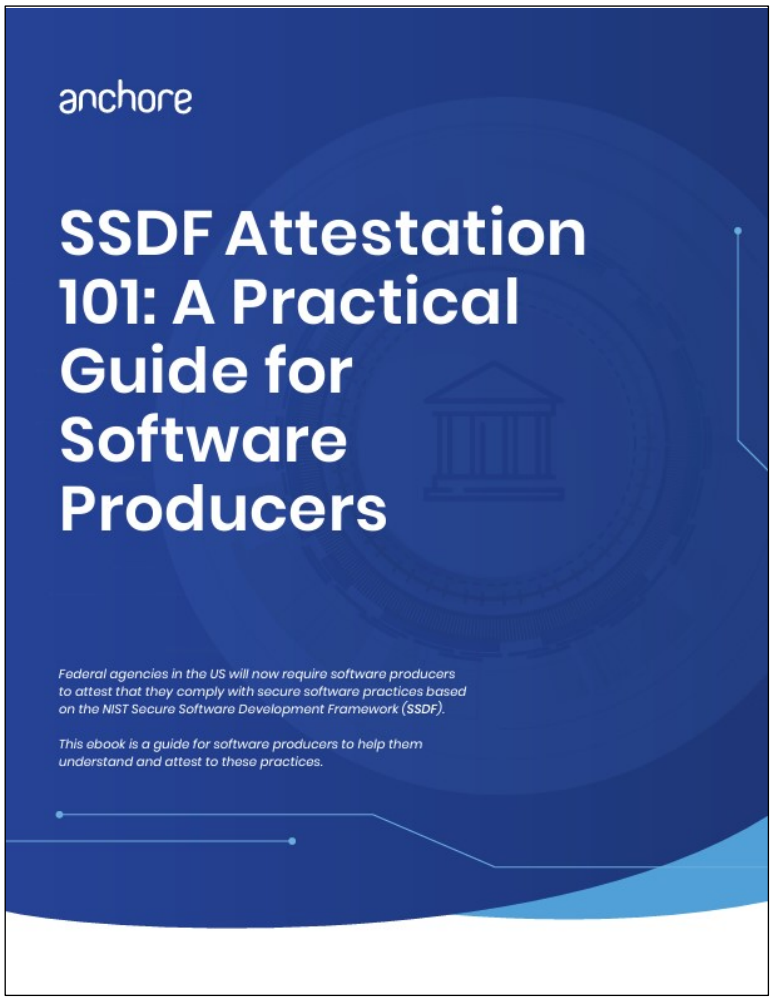
anchore

SSDF Attestation 101: A Practical Guide for Software Producers

eBook



carahsoft

For more information, contact Carahsoft or our reseller partners:
Anchore@carahsoft.com | 877-742-8468

anchore

SSDF Attestation 101: A Practical Guide for Software Producers

*Federal agencies in the US will now require software producers to attest that they comply with secure software practices based on the NIST Secure Software Development Framework (**SSDF**).*

This ebook is a guide for software producers to help them understand and attest to these practices.

Table of Contents

Introduction to SSDF Attestation

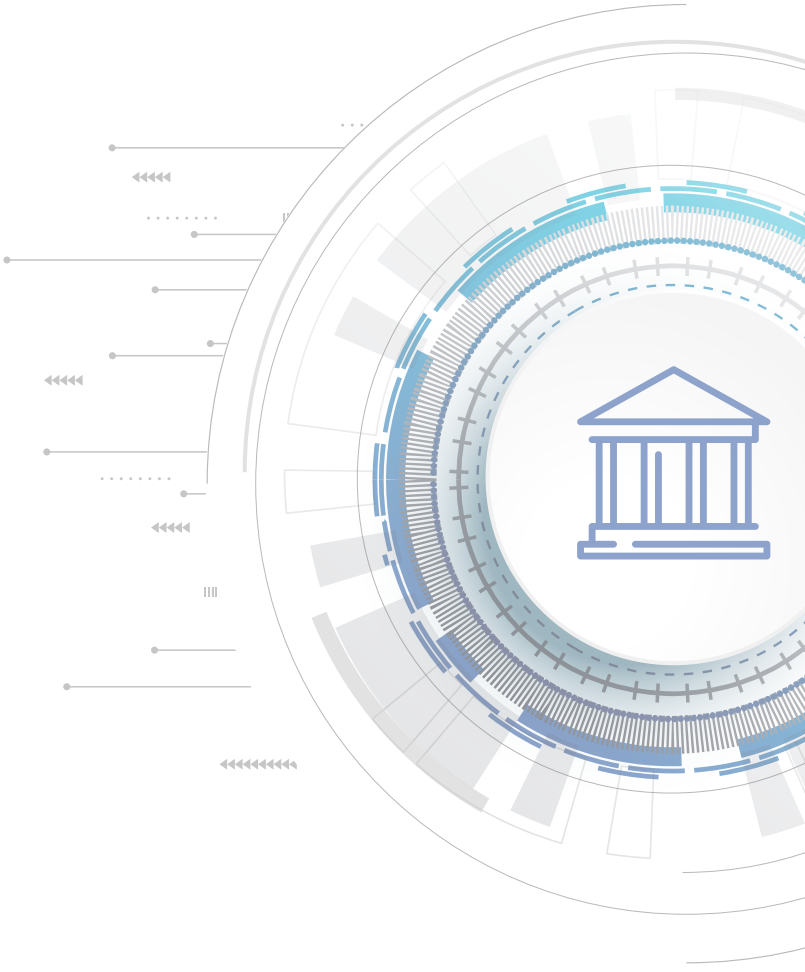
The US government just increased its security requirements for software producers selling to federal agencies. On March 11, 2024, the Cybersecurity & Infrastructure Security Agency (CISA) and the Office of Management and Budget (OMB) published a final version of the **Secure Software Development Attestation Common Form**. With the release of this form, the clock starts ticking for software producers to comply with its mandatory attestation requirements.

Anchore Enterprise is a tool that enables software producers who deliver via containers to comply more quickly and easily with the Secure Software Development Framework (SSDF) and the related NIST guidance. It is used by software producers to streamline compliance with a variety of federal standards, including SSDF, NIST, FedRAMP, CISA, and DoD.

This eBook helps companies understand the details of the new mandatory SSDF attestation requirements and how Anchore Enterprise helps organizations meet those fast.

Did you know?

Leading enterprises use Anchore Enterprise to meet various federal compliance standards, including SSDF, NIST, CISA, HIPAA, and more.



The Risks of Failure to Comply

Starting as early as June 11, 2024, software producers must now provide a signed attestation that they adhere to specific secure software development practices based on guidance from NIST. The implications for software producers can be far-reaching since failure to comply could result in the agency no longer being able to use the software at issue. Willfully providing false or misleading information may violate the False Claims Act, a criminal statute.

Guidance and Regulations for SSDF

The SSDF attestation requirements in the **Secure Software Development Attestation Common Form** originated from the May 2021 Executive Order on Improving the Nation's Cybersecurity[1], which directed NIST to issue guidance *"identifying practices that enhance the security of the software supply chain."* NIST subsequently provided this guidance in NIST Secure Software Development Framework (SSDF) (SP 800-218)[2] and NIST Software Supply Chain Security Guidance[3].

The Executive Order also required that the Director of OMB take appropriate steps to ensure that Federal agencies comply with NIST guidance. To that end, OMB issued two memorandum[4] explaining the steps and deadlines.

[1] Executive Order 14028, Improving the Nation's Cybersecurity

[2] NIST Secure Software Development Framework (SSDF) (SP 800-218)

[3] NIST Software Supply Chain Security Guidance

[4] Memorandum M-22- 18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, OMB Memorandum M-23-16, Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Who, What, When, and How of SSDF Attestation

What type of software does SSDF attestation apply to?

SSDF Attestation is required for all software producers who provide a software end product to federal agencies. The definition of a software producer is broader than you might think. It includes:

- Commercial-off-the-shelf [COTS] product vendors
- Cloud-based (SaaS) software vendors
- Custom software developers.
- Government-off-the-shelf [GOTS] software developers
- Providers of hardware with embedded software of firmware

There are a few exclusions where an SSDF attestation is not required, including:

- **Open-source software that is freely and directly obtained by a Federal agency**
- **Third-party components (open source and proprietary) that are incorporated into the software end product used by the agency**
  - While a software producer does not need to attest to the secure software development practices of open source or third-party proprietary components, they are not entirely off the hook. "*They must follow best practices for minimizing risk from such components, as articulated in NIST's SSDF. Best practices include "taking consistent and reasonable steps to document and minimize use of software products that create undue risk; maintaining provenance data for internal and third-party code; and maintaining trusted source code supply chains.*"
- **Software (including proprietary software) that is freely obtained and publicly available**
  - "*A significant number of core software applications, such as web browsers, to which Federal agencies must have access, are offered for use to members of the public at no cost. Users of this software have no opportunity to negotiate with the producer, and therefore it will not be feasible for agencies to obtain attestations from the producers of such software.*"
- **Software developed by Federal agencies**
  - While agency-developed software is currently out of scope for SSDF attestation requirements, whether software developed under a Federal contract constitutes agency-developed software "*depends on whether the contracting agency is able to ensure that secure software development practices are followed throughout the entire software development lifecycle (i.e., requirements, design, development, testing, deployment, and maintenance).*" If there are questions regarding whether software developed by Federal contractors should be considered agency-developed, "*agency CIOs are required to make that determination on behalf of the agency.*"

Which versions of software require SSDF attestation?

SSDF attestation is required based on the timing of when the software was developed or updated. SSDF attestation is mandatory for the following software:

- Software developed after September 14, 2022
- Software developed prior to September 14, 2022, but modified by major version changes after September 14, 2022 (e.g., using a semantic versioning schema of Major. Minor.Patch, the software version number goes from 2.5 to 3.0)
    - According to semantic versioning rules, a major version **MUST** be incremented if any backward incompatible changes are introduced to the public API.
    - There has been some discussion that some software producers may try to "game the system" by not updating the "major" part of the semantic versioning and instead delivering "minor updates." This is not recommended, as it doesn't follow the rules of semantic versioning, and an agency using the software might call it out.
- Software products where the producer delivers continuous changes to the software code (as is the case for **software-as-a-service** products or other products using continuous delivery/continuous deployment).

Who must sign the SSDF attestation?

The SSDF attestation form must be signed by the software producer's chief executive officer (CEO) or designee. However, any designee *"must be an employee of the software producer and have the authority to bind the corporation."* It can make sense to have a designee sign who is more familiar with the details of whether the SSDF requirements have been met. However, the implication is clear: even if the signee is not the CEO, the attestation binds the entire company.

However, there is an alternative to signing the attestation. The software producer may instead provide a third-party assessment documenting conformance with the requirements. The assessment must be performed by a Third Party Assessor Organization (3PAO) that has either been FedRAMP certified or approved in writing by an appropriate agency official.

The 3PAO option is a no-brainer for SaaS companies that are already using a 3PAO for FedRAMP compliance. Most 3PAOs will likely offer SSDF assessments as an add-on service. The 3PAO route is also likely to appeal to many larger companies who want to reduce the risk of providing incorrect information in their attestation.

When is the deadline for providing SSDF attestations?

The OMB extended the original deadline for providing SSDF attestations in its M-23-16 update memorandum[5].

The deadline varies for critical and non-critical software. These dates only apply to software that is *subject to SSDF attestation requirements*. See the above sections for more information.

See the NIST definition of critical software.

Type of Software	Time after publication of the SSDF Attestation Common Form	Actual Date
Critical software subject to the SSDF requirements	3 months after OMB PRA approval of the Common Form	Jun 11, 2024
All software subject to the SSDF requirements	6 months after OMB PRA approval of the Common Form	Sep 11, 2024

How are SSDF attestations submitted?

CISA has created a **Self-Attestation Common Form and instructions** for submitting SSDF attestations. However, *agencies may add agency-specific instructions* for software producers, in which case the software producer may include these agency-specific requirements as an addendum.

Software products should use CISA's **online form** to submit SSDF attestations. These SSDF attestation forms will go into a central Repository for Software Attestation and Artifacts (RSAA).

If a software producer is unable to submit via the online form, they may email a PDF version of the form to the respective agency.

[5] OMB M-23-16 update

About SSDF Extensions, Exceptions, and POA&Ms

The OMB has **documented the requirements** for extensions, waivers, and exceptions, including the use of POA&Ms.

Are extensions available for SSDF requirements?

The OMB has created a process for *agencies* to request an extension to comply with SSDF attestation requirements. The agency must submit the extension request to the OMB at least 30 days before any relevant deadline and must accompany it with a plan for meeting the underlying requirements.

Are waivers available for SSDF requirements?

There is also a process for *agencies* to request a waiver for any specific requirements. Still, the waiver will be *"only in the case of exceptional circumstances and for a limited duration."* Once again, the request must be submitted 30 days before the relevant deadline and must be accompanied by a plan for mitigating any potential risks.

What if a software producer cannot meet the SSDF requirements?

The **OMB has also defined a process** to follow if a software producer can't yet attest to one or more of the SSDF requirements. The *"agency shall require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks, and require a Plan of Action & Milestones (POA&M) to be developed."* NIST **defines a POA&M** as a document that *"identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones."*

If the agency finds the documentation and POA&M satisfactory, they may continue to use the software.

In this case, where the software producer can't yet sign the attestation, the OMB is adamant that the software producer **must not publicly post any documentation or POA&Ms**. This protects against possible exploits based on the documented gaps.

The Four Main Requirements for SSDF Attestation

SSDF attestation includes four main requirements. The following sections will provide an overview of each requirement.

1. Software developed after September 14, 2022
2. Trusted Source Code Supply Chains
3. Maintaining Provenance
4. Vulnerability Checking

It's important to note that the SSDF attestation currently only includes a subset of the practices in the NIST Secure Software Development Framework (SSDF) (SP 800-218).

1 Secure Development Environments

The first requirement is to ensure the software is developed and built-in secured environments, protecting from compromise of the toolchain or development environments. This requirement includes:

- documenting the toolchain
- securing the development toolchain, including separating and protecting each environment
- managing authorization and access and using MFA
- securing the endpoints
- encrypting sensitive data like credentials
- responding to vulnerabilities in your development toolchain
- continuous monitoring of development systems to respond to any attempted or actual cyber incidents
- and more

2 Trusted Source Code Supply Chains

The second requirement is to use automated tools or comparable processes to maintain the security of the software supply chain. This requirement includes:

- defining policies for the use of open source and other 3rd party components
- repository to host sanctioned and vetted open-source components
- using commit signing and code signing
- protecting release integrity verification and provenance information
- obtaining provenance information (e.g., SBOM, source composition analysis, binary software composition analysis) for each software component and analyzing it to assess risk
- automatically checking for known vulnerabilities in the toolchain
- regularly checking for public vulnerabilities that are not fixed
- ensuring that software components are actively maintained and not EOL
- gathering information from software users and public sources on potential vulnerabilities
- and more

3 Maintaining Provenance

The third requirement is maintaining provenance (e.g., SBOMs) for internal code and third-party components. This requirement includes:

- using existing tooling to create an audit trail of secure development-related actions
- providing provenance data (e.g., SBOMs) to software acquirers in standards-based formation
- using provenance data to aid response teams in mitigating new software vulnerabilities
- updating provenance data each time software components are updated
- protect the integrity of provenance data
- identify and confirm vulnerabilities on an ongoing basis using provenance data

4 Vulnerability Checking

The fourth requirement is to use automated tools to check for security vulnerabilities. This requirement includes:

- automatic vulnerability checking of software components at any stage of your software development process, including source code repositories, CI/CD pipelines, container registries, and container runtime environments
- using provenance and software composition data (e.g., SBOMs) for all software components to identify any new vulnerabilities they have
- assessing, prioritizing, and remediating vulnerabilities
- monitoring vulnerability databases for new vulnerabilities
- and more

Accelerating SSDF Attestation with Anchore Enterprise

Anchore Enterprise capabilities and features address essential requirements of SSDF attestation, including SBOM generation and management, vulnerability checking, and automated policy enforcement.

Track Software Provenance with SBOMs

Anchore Enterprise automates the generation of detailed SBOMs for container images or filesystems at each step in the development process by integrating into your existing toolchain. It provides a complete inventory of the software components, including your direct and transitive dependencies. It provides visibility into all container image layers, not just the base image. It can "crack open" multiple nested levels of binary files (such as .jar, .war, .ear files) to find hidden dependencies and vulnerabilities. This approach provides peace of mind because you know that vulnerabilities or security risks are not hidden in nested files.

What is an SBOM?

A software bill of materials (SBOM) is a critical foundation for secure software development. In order to secure software, you must first know what open-source and third-party software it contains. SBOMs are highlighted in SSDF as a means of tracking software provenance.

SSDF practices highlight the need to *"safeguard, maintain, and share provenance data for all components of each software release."* As you create more SBOMs during your development process, managing them can quickly become overwhelming. To address this challenge, Anchore Enterprise stores all SBOMs in an SBOM repository, which helps you meet SSDF requirements for a trusted software supply chain and track the provenance of any software components.

It enables you to:

- store generated SBOMs, as well as SBOMs imported from 3rd parties
- review and report on SBOMs
- create an application-level SBOM for each release with a list of software components
- get an application-level view of vulnerabilities and compliance state
- store SBOMs for each release and version
- export SBOMs for entire applications in standard formats to share with customers
- monitor released applications for any new or zero-day vulnerabilities that arise
- identify SBOM drift (changes to software components) that could indicate malicious activity

Automated Vulnerability Checks

With Anchore Enterprise teams can implement automated processes that identify and remediate vulnerabilities in your software on an ongoing basis. This includes:

1. Automatic vulnerability checking of software components at any stage of your software development process, including source code repositories, CI/CD pipelines, container registries, and container runtime environments
2. Using provenance and software composition data (e.g., SBOMs) for all software components to identify any new vulnerabilities they have
3. Assessing, prioritizing, and remediating vulnerabilities
4. Monitoring vulnerability databases for new vulnerabilities

Anchore Enterprise produces comprehensive, detailed SBOMs as the starting point for vulnerability checking. Each software component is then compared to a broad set of vulnerability feed sources, including the National Vulnerability Database, GitHub Security Advisories, feeds for popular Linux distros and packages, and an Anchore-curated dataset for suppression of known false-positive vulnerability matches. Anchore Enterprise applies a best-in-class precision matching algorithm to select vulnerability data from the most accurate feed source.

When a zero-day vulnerability arises, Anchore Enterprise can instantly identify which components and applications are impacted by simply re-analyzing your stored SBOMs. You don't need to re-scan applications or components. You can also search the SBOM repository to find applications containing the vulnerable components.

Anchore Enterprise streamlines remediation by automatically alerting developers of issues through their existing tools, such as Jira or Slack. It provides automated remediation recommendations and lets security teams define actionable remediation workflows.

Continuous, Automated Policy Enforcement

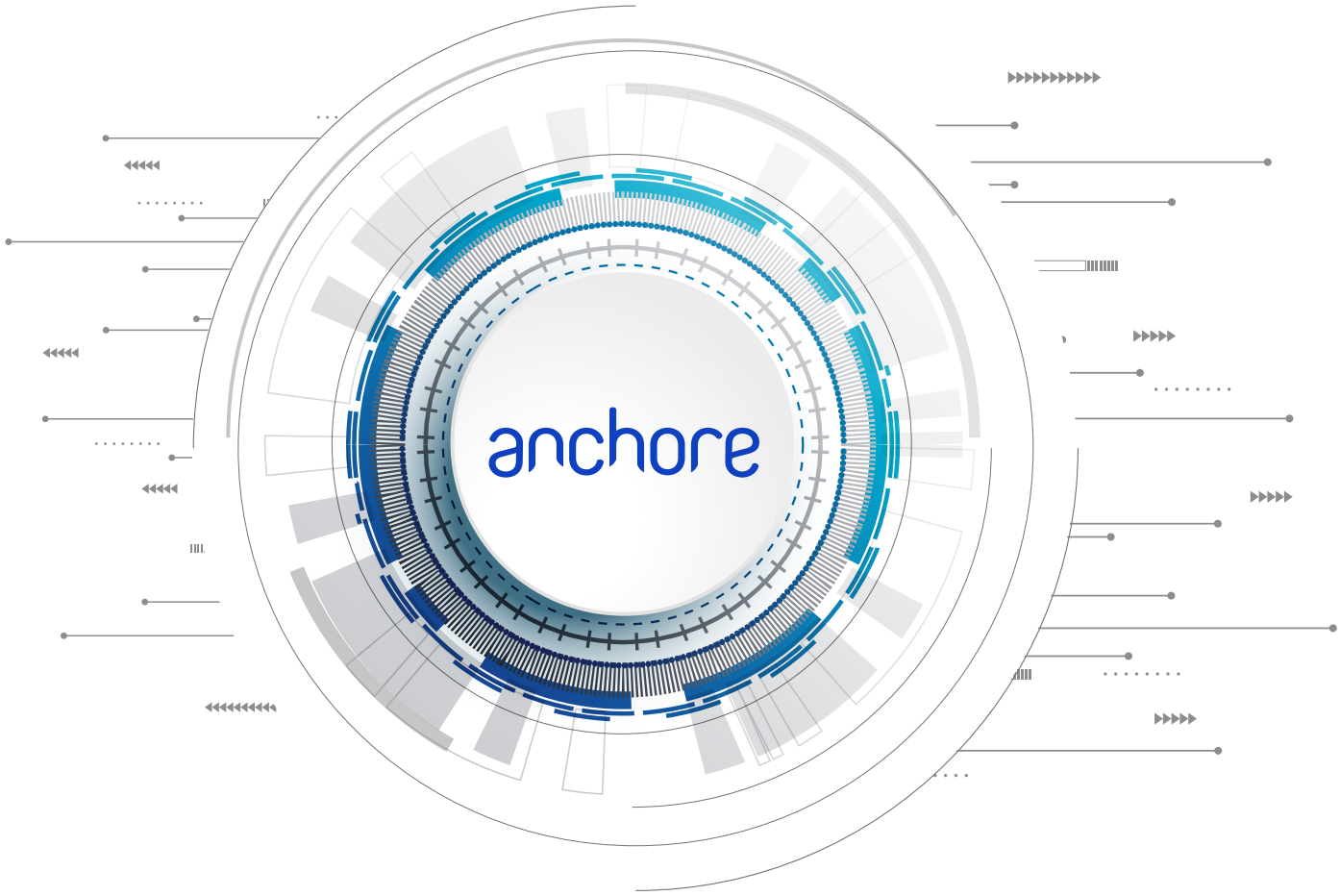
Anchore Enterprise has a customizable policy engine that can identify and alert on the most important vulnerabilities and security issues and meet compliance requirements. It includes pass/fail policy reports that provide evidence of your applications' current compliance status.

Teams can define automated rules that alert based on the risk. For example, an organization may raise policy violations for vulnerabilities scored as Critical or High with a fix available or those on CISA's list of Known Exploited Vulnerabilities. You can customize policies to generate alerts and notifications, stop builds in the CI/CD pipeline, or prevent code from moving to production.

Anchore Enterprise offers an out-of-the-box policy pack with pre-built rules for NIST 200-218 SSDF to jump-start your SSDF attestation efforts. Anchore also provides policy packs for CISA, FedRAMP, DoD, DISA, and other NIST standards.

Next Steps: Use Anchore Enterprise to Accelerate SSDF Attestation

With SSDF attestation deadlines looming, organizations that sell software to the federal government must implement tools that will help them meet SSDF requirements and provide the evidence needed for attestation. Leading enterprises, including Cisco, ServiceNow, Nvidia, and Infoblox, use Anchore Enterprise today to ease their path to federal compliance.



Book a demo **Start a Free Trial**

Resources

How to Perform STIG checks with Anchore Federal 3.1	View our demo on YouTube to learn how you can perform STIG compliance checks with Anchore Federal
DISA STIGs Document Library	A complete library of DISA STIGs maintained by the DoD
DoD DevSecOps Enterprise Container Hardening Guide	Download and read the latest version of the DoD DevSecOps Enterprise Container Hardening Guide
Download the STIG Viewer	Download the latest version of the STIG Viewer
Kubernetes Hardening Guidance	Kubernetes hardening guidance from the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA)
Anchore Federal Webpage	Learn more about how Anchore solutions can help the DoD and public sector agencies

About Anchore

Anchore enables organizations to speed digital transformation and reduce risks by streamlining the development of secure and compliant cloud-native applications. Anchore's solutions integrate with existing DevOps toolchains to automate security and compliance checks throughout the software development lifecycle. Organizations can reduce costs and accelerate time to market by remediating security and compliance issues early and continuously. Headquartered in California with offices also in Boston and the UK, Anchore's customers include large enterprises and government agencies that require secure and compliant cloudnative applications. To learn more about Anchore's solutions, visit **Anchore.com**.

anchore

sales@anchore.com

anchore.com

© 2024 Anchore, Inc. All rights

anchore

Thank you for downloading this Anchore resource! Carahsoft serves as the Master Government Aggregator® and Distributor for Anchore, offering expertise in government procurement processes and practices with purchasing available via ITES-SW and other contract vehicles.

To learn how to take the next step toward acquiring Anchore's solutions, please check out the following resources and information:

For additional resources:
carah.io/AnchoreResources

For upcoming events:
carah.io/AnchoreEvents

For additional Anchore solutions:
carah.io/AnchoreSolutions

For additional Open Source solutions:
carah.io/OpenSourceSolutions

To set up a meeting:
Anchore@carahsoft.com
877-742-8468

To purchase, check out the contract vehicles available for procurement:
carah.io/AnchoreContracts