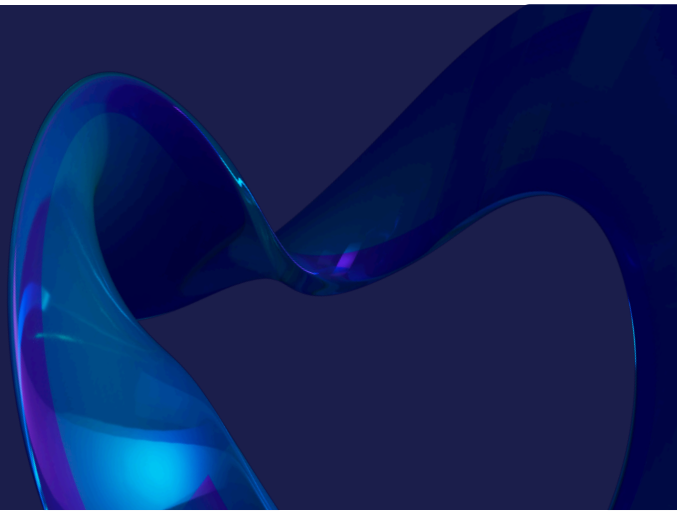
Contrast SECURITY

Meet OMB 22–18 Requirements with Contrast Security



In 2023, application attacks and attacks against application programming interfaces (APIs) are surging. As agencies digitally transform, they must do so with vigilance. The federal mandates for "zero trust" and continuous monitoring must extend to software development and application security.

OMB 22–18

Requires all government agencies to request self-attestations about the security posture of the software they consume. These self-attestation forms should be provided by the agency, but it's time for those software organizations selling to the government to start preparing their internal teams to respond to these requests.

Contrast helps with

- **4e(i)(F) -** operational monitoring and incident detection and response
- **4e(ii) -** Artifacts from 4e(i)
- **4e(iv) -** Check software for vulnerabilities and remediate them
- **4e(v) -** Artifacts from 4e(iv)
- **4e(vii) -** SBOM for each product
- **4e(viii) -** participate in vulnerability discovery program
- **4e(ix) -** Attest to conformity with secure software development practices (testing) — SEE NIST 800-218 SSDF
- **4e(x) -** Attest to integrity and provenance of open-source components — check hash on all libraries (unknowns)

Details on what must be in attestation

SSDF Practices Corresponding to EO 14028 Subsections

EO 14028 Subsection	Subsection Summary (Refer to the next coolumn for a complete list)	SSDF Practice and Task Reference Numbers
4e(i)	Have secure software development environments, including:	*[See rows below]*
4e(i)(A)	administratively separate build environments;	PO.5.1
4e(i)(B)	trust relationship auditing;	PO.5.1
4e(i)(C)	multi-factor, risk-based authentication and conditional access;	PO.5.1, PO.5.2
4e(i)(D)	minimized dependencies on enterprise products products in development environments;	PO.5.1
4e(i)(E)	data encryption; and	PO.5.2
4e(i)(F)	operational monitoring and incident detection and response	PO.3.2, PO.3.3, PO.5.1, PO.5.2
4e(ii)	Provide artifacts from 4e(i) upon request.	PO.3.2, PO.3.3, PO.5.1, PO.5.2
4e(iii)	Maintain trusted source code supply chains.	PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4
4e(iv)	Check software for vulnerabilities and remediate them.	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.2.1, RV.2.2, RV.3.3
4e(v)	Provide artifacts from 4e(iii) and 4e(iv) upon request, and make a summary description of risks assessed and mitigated publicly available.	PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.1.2, PW.2.1, PW.7.2, PW.8.2, RV.2.2
4e(vi)	Maintain provenance data for internal and 3rd party components.	PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.1.2, PW.2.1 PW.7.2, PW.8.2, RV.2.2
4e(vii)	Provide a software bill of materials (SBOM) for each product.	PS.3.2
4e(viii)	Participate in a vulnerability disclosure program.	RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3
4e(ix)	Attest to conformity with secure software development practices.	All practices and tasks consistent with a risk-based approach
4e(x)	Attest to the integrity and provenance of open-source software components.	PS.2.1, PS.3.1, PS.3.2, PW.4.1, PW.4.4

Contrast SECURITY

Contrast Security offers public sector and government agencies working with limited security resources full transparency of their application risk layer while also protecting against targeted attacks and zero-day events. By embedding security sensors within the code itself, the Contrast Security platform shifts security left in application development, empowering DevOps to secure as they code and to dramatically reduce application security incidents.

Contrast Security is committed to protecting American cyberspace. See how the Contrast Secure Code Platform can help your business defend against entire classes of application attacks and build SBOMs in minutes. Visit www.contrastsecurity.com/federal to learn more.

Sources:

https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

https://energycentral.com/c/pip/advice-software-vendors-prepare-omb-m-22-18-requirements

Contrast SECURITY