Secure and Comply with Federal Cyber Standards

Strengthen security controls across DoD systems and infrastructure

RUNSAFE SECURITY

Documentation Category	NIST Mapping	Requirements / Example Content	RunSafe	RunSafe Capability/Notes
Software Inventory & SBOM Visibility Support SBOM requirements aligned to SWFT+, NIST SP 800-218, and DoD software acquisition expectations.	NIST 800-218: PO.1, PO.3	Define software inventory requirements for embedded and mission systems		Subject to RunSafe customers' practices
	NIST 800-218: PS.3, PW.4, RV.1 NIST 800-53: SI-7	Generate and maintain complete SBOMs for first-party, third-party, and open-source components	✓	RunSafe generates a buiildtime SBOM, inventoring all software components - third-party software and dependences in the software build.
	NIST 800-218: PS.3, PW.4 NIST 800-53: SI-7	Document software dependencies, versions, and transitive libraries	✓	RunSafe generates a buiildtime SBOM, inventoring all software components - third-party software and dependences in the software build.
	NIST 800-218: PO.3, PS.3, PW.4 NIST 800-53: SI-7 / SR	Maintain software provenance and supplier records	✓	RunSafe helps maintain software provenance by including all software components and dependencies in the software build.
	NIST 800-218: PS.2, PS.3, RV.1 NIST 800-53: SI-2, SI-7	Validate software composition before deployment and updates	✓	Risk Reduction Analysis tool analyzes exposure to CVE and potential zero days that helps to validate software composition by assessing exploitability before deployment.
Vulnerability Identification & Exposure Analysis Identify known vulnerabilities and determine which risks are operationally relevant and exploitable.	NIST 800-218: RV.1 NIST 800-53: SI-2	Map software components to known CVEs and vulnerability databases	✓	Risk Reduction Analysis tool analyzes exposure to CVE and potential zero days, continually incorporating vulnerability sources (such as NVD and vendor advisories) and monitoring for new alerts.
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-4	Assess exploitability of vulnerabilities within the deployed environment	✓	Riskk Reduction Analysis tool shows the residual risk for a runtime SBOM build to determine the impact of vulnerabilities, and urgency to remediate (patch now or soon).
	NIST 800-218: RV.2 NIST 800-53: SI-2	Prioritize vulnerabilities based on mission impact and likelihood of exploitation	✓	Risk Reduction Analysis tool shows the residual risk and urgency to remediate (patch now or soon).
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2	Document compensating controls and unresolved risk	✓	Using RunSafe Protect, the vulnerability can be contained and made non-exploitable. RunSafe records when executable protection was applied and provides documentation and verification materials.
	NIST 800-218: RV.1, RV.2, RV.3 NIST 800-53: SI-2, SI-4, SI-7	Maintain continuous vulnerability review as software changes	✓	RunSafe continually incorporate sources (such as NVD and vendor advisories) to identify vulnerabilities with the SBOM, monitors for new alerts, and analyzes exposure to CVEs and potential zero days; and determines if exploitable
Secure Software Development & Supply Chain Risk Demonstrate secure development practices and software supply chain controls for ATO, RMF, and SWFT+ readiness.	NIST 800-218: PO.1	Define secure software development lifecycle policies and procedures		Subject to RunSafe customers' practices
	NIST 800-218: PO.2	Define security roles and responsibilities within development teams		Subject to RunSafe customers' practices
	NIST 800-218: PO.1, PO.4	Define cybersecurity requirements for embedded and industrial software products		Subject to RunSafe customers' practices
	NIST 800-218: PW.1, PW.2 NIST 800-53: SI-10, SI-16	Conduct threat modeling for software components and system architecture	✓	RunSafe Risk supports threat modeling by providing vthe Risk Reduction Analysis tool to assess residual risk that provides visibility to known vulnerability expore in software compoents and dependencies.
	NIST 800-218: PW.2, RV.2, RV.3 NIST 800-53: SI-2, SI-4, SI-16	Identify potential exploit paths within software architecture	✓	Risk Reduction Analysis tool identifies exposure to CVE and memory-based zero days and assessing how vulnerabilities could impact the software in a deployed environment.
	NIST 800-218: PW.1, PW.2, PW.6 NIST 800-53: SI-10, SI-16	Design security controls to mitigate identified threats	✓	RunSafe Protect can make vulnerabilities non-exploitable, relocating software functions in memory, creating a unique layout of executables at runtime that mitigates identified threats.
	NIST 800-218: PW.4, RV.1, RV.2 NIST 800-53: SI-2, SI-7	Validate third-party and supplier software risk	✓	RunSafe inventories all software components - third-party and supplier software and dependences in the software build, and map them to vulnerabilties to validate supplier software risk
RMF / ATO Evidence & Continuous Monitoring Support DoDI 8510.01 and Authorization to Operate requirements with documented risk posture and continuous monitoring.	NIST 800-53: Control baseline selected aft	Define system security categorization and applicable control baseline		Subject to RunSafe customers' practices
	NIST 800-218: PO.1, PO.3 NIST 800-53: SI-2, SI-4, SI-7	Document implemented cybersecurity controls and inherited controls		Subject to RunSafe customers' practices
	NIST 800-218: RV.1, RV.2, RV.3 NIST 800-53: SI-2	Track vulnerability status, remediation actions, and POA&M items	✓	RunSafe generates reports of the SBOM and known vulnerabilities
	NIST 800-218: PO.3, PS.3, RV.1, RV.2 NIST 800-53: SI-2, SI-4, SI-7	Maintain evidence for continuous authorization and ATO reviews	✓	RunSafe tracks known vulnerabilities and affected components, providing documentation how protection applied to memory-based vulnerabilities.
	NIST 800-218: RV.1, RV.2, RV.3 NIST 800-53: SI-2, SI-4, SI-7	Establish continuous monitoring and periodic reassessment processes	✓	RunSafe continuously incorporates vulnerability sources (such as NVD and vendor advisories), monitors for new alerts, and analyzes exposres to CVEs and ptoential zeros days; and determines if exploitable.
Weapon System Cybersecurity Compliance Align embedded and mission-critical systems to DoDI 5000.83 requirements.	NIST 800-218: PO.1, PW.1	Identify mission-critical functions and cyber mission dependencies		Subject to RunSafe customers' practices
	NIST 800-218: PO.1, PW.1	Define security boundaries for weapon system components		Subject to RunSafe customers' practices
	NIST 800-218: PO.3, PS.3, RV.1 NIST 800-53: SI-2, SI-7	Document cybersecurity controls for embedded and deployed systems		Subject to RunSafe customers' practices
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16, SI-17	Validate resilience requirements for systems with limited patching windows	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and memory-based zero days, showing residual risk to determine urgency to remediate (patch now or soon). If exposed and patching is limited, RunSafe Protect can harden and make vulnerabilities non-exploitable.
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-4, SI-16	Demonstrate operational risk management for long-life platforms	✓	RunSafe Risk Reduction Analysis tool quantifies residual risk of the exploit, where RunSafe Protect can make a vulnerability non-expoitable to support the continued operation of long-life platforms where patching vulnerabilities cannot happen immediately.
Runtime Risk Reduction for Unpatchable Systems Reduce exploitability when vulnerabilities cannot be rapidly patched due to certification, uptime, or mission constraints.	NIST 800-218: RV.1, RV.2 NIST 800-53: SI-2	Identify systems where patching is delayed or operationally constrained		Subject to RunSafe customers' practices
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16	Define compensating controls for known vulnerabilities		Subject to RunSafe customers' practices
	NIST 800-218: PW.6, RV.2 NIST 800-53: SI-16	Implement runtime protections for memory-based exploits	✓	RunSafe Protect makes vulnerabilities non-exploitable, randomizing memory layouts of executables at runtime.
	NIST 800-218: PW.6, RV.2 NIST 800-53: SI-16	Reduce attack paths without requiring source code access or redesign	✓	RunSafe Protect reduces attack paths, hardening binaries by randomizing the location of software functions in memory each time the application runs
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16	Validate protections for deployed legacy systems	✓	RunSafe Protect makes vulnerabilities non-exploitable, randomizing memory layouts of executables at runtime. The Risk Reduction Analyzer tool validates the protection by quantifying the residual risk.
Residual Risk Management Justify accepted risk and demonstrate compensating controls when vulnerabilities cannot be fully removed.	NIST 800-218: PO.1	Define residual risk acceptance criteria		Subject to RunSafe customers' practices
	NIST 800-218: RV.1, RV.2 NIST 800-53: SI-2	Document known vulnerabilities that cannot be immediately remediated	✓	Risk Reduction Analysis shows which CVEs remain exploitable vs mitigated. RunSafe Protect makes vulnerability non-expliotable.
	NIST 800-218: PO.1	Establish formal risk acceptance and approval processes		Subject to RunSafe customers' practices
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16	Demonstrate compensating controls and exploitability reduction	✓	RunSafe Protect makes vulnerability non-exploitable by randomizing the location of software functions in memory each time the application runs
	NIST 800-218: RV.1, RV.2, RV.3 NIST 800-53: SI-2	Maintain traceability between vulnerabilities and accepted operational risk	✓	RunSafe maintains an SBOM with a full dependency tree, known CVEs, and quantification of residual risk from exploit.
Mission Continuity Support Ensure operational systems remain functional while vulnerabilities are managed and remediation is planned.	NIST 800-218: PO.1, PW.1	Identify mission-essential functions that must remain operational		Subject to RunSafe customers' practices
	NIST 800-218: PW.1, RV.2 NIST 800-53: SI-17	Define degraded-mode operations and survivability expectations		Subject to RunSafe customers' practices
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16, SI-17	Maintain operational readiness during vulnerability remediation cycles	✓	RunSafe Protect can make a vulnerability non-expoitable while being patched and remediated by randomizing the location of software functions in memory each time the application runs
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-2, SI-16, SI-17	Prevent disruption from software updates or delayed patching	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and memory-based zero days, showing residual risk to determine urgency to remediate (patch now or soon). If exposed and patching is limited, RunSafe Protect can harden and make vulnerabilities non-exploitable.
	NIST 800-218: RV.2, RV.3 NIST 800-53: SI-16, SI-17	Support continuous mission execution under cyber risk conditions	✓	RunSafe Protect makes the vulnerability non-expoitable, preventing the expoit to be weaponized during during operations and preserving the continued execution of the mission.