RUNSAFE SECURITY

Achieving Cyber Trust and Mission Survivability

ALIGN TO NIST AND CSA TO ENSURE SYSTEMS OPERATE THROUGH CYBER THREATS

Defense systems operate in mission-critical environments where trust, resilience, and continuous operation are essential to mission success. Many Department of Defense platforms run on software that cannot be taken offline without impacting readiness. Systems must survive cyber attacks, and continue to operate and complete their mission. Ultimately, defense systems must be both trusted and resilient—ensuring vulnerabilities do not disrupt mission execution.

ACHIEVE CYBER STANDARDS AND MISSION SURVIVABILITY

Defense systems must align to frameworks such as NIST SP 800-53 and NIST SP 800-218, while addressing survivability outlined in the Cyber Survivability Endorsement Implementation Guide. NIST defines trusted software and risk management, while CSEIG and CSA ensure missions continue when that software is challenged by real-world threats.

Systems must demonstrate capabilities across both cybersecurity and mission survivability, including:

- **Secure Software Development**: Follow practices to reduce introduction of vulnerabilities
- **Software Transparency & Risk Awareness**: Maintain visibility into components and vulnerabilities
- **Continuous Risk Assessment & Management**: Identify, assess, and manage vulnerabilities across the lifecycle
- **System Hardening & Attack Surface Reduction**: Minimize exposure and opportunities for exploitation
- **Mission Resilience & Survivability**: Ensure systems operate and complete missions under cyber attack

Together, these require systems to be continuously assessed and resilient in operation.

ENSURING SYSTEMS ARE TRUSTED AND OPERATIONAL

RunSafe strengthens how systems meet NIST and CSA expectations by identifying vulnerabilities, determining which are exploitable, and preventing exploits at runtime, so systems remain trusted and operational.

ACHIEVING TRUSTED SOFTWARE: NIST ALIGNMENT & RISK REDUCTION

- SBOM Generation & Software Transparency: Build-time SBOMs provide full visibility into components and dependencies
- Vulnerability Identification & Prioritization: Analyze CVEs and determine which are relevant to the system
- Exploitability Analysis: Identify which vulnerabilities are exploitable in the deployed environment
- Risk-Based Decision Support: Enable remediation, mitigation, or formal risk acceptance with evidence
- Compliance Evidence Generation: Produce artifacts aligned to NIST to support RMF and ATO

MISSION ASSURANCE UNDER ATTACK: CYBER SURVIVABILITY & RESILIENCE

- Runtime Exploit Prevention: Harden binaries to block memory-based exploits from executing
- Protection Without Source Code Changes: Secure compiled software without redesign or recertification
- Resilience for Unpatchable Systems: Maintain protection when patching is not feasible due to constraints
- Reduced Attack Surface at Runtime: Limit adversary ability to successfully exploit vulnerabilities
- Mission Continuity Assurance: Ensure systems operate and complete missions under cyber attack

A STRONGER CYBERSECURITY POSITION

RunSafe provides technical evidence that supports NIST and CSA standards.

NIST Coverage	Supported by RunSafe
Software Inventory & SBOM Visibility	✓
Vulnerability Identification & Exposure Analysis	✓
Secure Software Development & Supply Chain Risk	✓
RMF / ATO Evidence & Continuous Monitoring	✓
Weapon System Cybersecurity Compliance	✓
Runtime Risk Reduction for Unpatchable Systems	✓
Residual Risk Management	✓
Mission Continuity Support	✓
CSA Coverage	**Supported by RunSafe**
Attack Surface Reduction	✓
Partition Critical Functions to Prevent Compromise from Spreading	✓
Secure Communications & Information Protection	✓
Baseline, Monitoring & Anomaly Detection	✓
Operate While Degraded to Maintain Mission Execution	✓
Recovery & Reconstitution: Restoring Mission Capability	✓
Adaptation to Emerging Threats	✓
Residual Risk & Mission Assurance	✓

WHY RUNSAFE?

Defense systems cannot always be patched on demand, yet vulnerabilities persist. RunSafe helps programs by making those vulnerabilities non-exploitable at runtime while providing visibility to understand and manage risks that align with NIST and Cyber Survivability expectations.