RSI | Datasheet

NIST SP 800-171

Special Publication 800-171 was released by the National Institute of Standards and Technology (NIST) to protect against the cybersecurity risks faced by Department of Defense (DoD) contractors. NIST SP 800-171 applies to companies operating in the Defense Industrial Base (DIB) sector that collect, store, process, and transmit Covered Defense Information (CDI) and Controlled Unclassified Information (CUI). All CDI and CUI must be secured as a matter of critical infrastructure operations and national security. Failure to do so risks the loss of DoD contracts.

In 2019, the DoD announced the upcoming release of the Cybersecurity Maturity Model Certification (CMMC). While the CMMC has become the primary compliance framework, it heavily incorporates NIST SP 800-171 as a foundation and source text. Contractors are undergoing their initial compliance efforts and the Accreditation Body overseeing the framework is conducting the first round of approvals for certified third-party assessor organizations (C3PAOs), including for RSI Security, throughout 2021. RSI Security is currently a CMMC-AB Registered Provider Organization with a team of Registered Practitioners.

RSI Security's NIST SP 800-171 Services

RSI Security provides NIST SP 800-171 compliance services and advisory for contractors as a crucial step toward both current DoD requirements and the demands of CMMC certification, moving forward.

NIST SP 800-171 Scope Assessment

RSI Security's scope assessment will identify the storage locations and processes involved with CDI and CUI within your IT environment to determine your company's risk exposure. Scope assessment findings will provide detailed information on security posture, current process and policy implementation, and a roadmap for achieving SP 800-171 specification and best practice implementation.

Security Infrastructure Assessment

RSI Security will scan and assess existing security infrastructure to identify any vulnerabilities and improvements necessary for NIST SP 800-171 adherence, ensuring that recommendations coincide with strategic business aims.

Penetration Testing

RSI Security's penetration testing services will simulate cyberattacks to determine your organization's security posture and incident response. In addition to penetration testing, RSI provides tabletop incident response exercises.

CMMC Mapping and Compliance

For many DoD contractors, CMMC adoption will require mapping existing NIST SP 800-171 implementations to the new framework and assessing and remediating their compliance gap. RSI Security's expertise with both frameworks will facilitate the process. Critically, NIST SP 800-171 involves self-assessment, whereas the CMMC requires third-party validation conducted by a C3PAO.

Risk Management

RSI Security's risk management services cover locating and ranking your organization's CDI and CUI most likely to be targeted by cybercriminals. Risk management assessments will also extend to your third-party service providers to ensure your compliance efforts aren't threatened by partners and vendors.

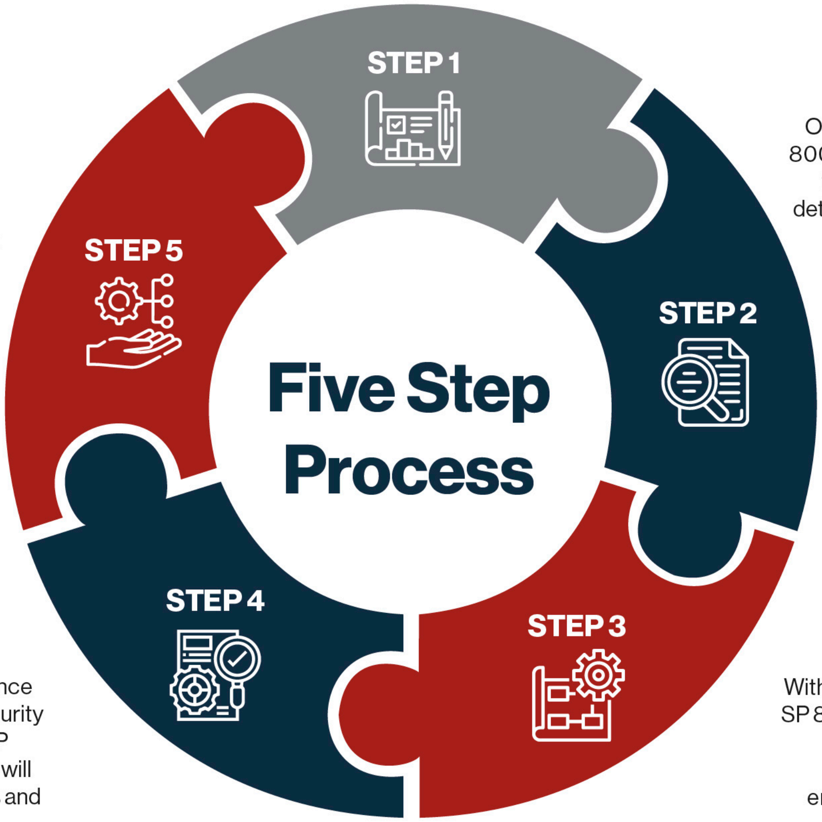
Implementation Advisory

Whether choosing the right vendors for your organization or determining security configurations, RSI Security will assist with and advise on implementation.

Achieving NIST SP 800-171 Compliance

1. Prepare and Review

NIST SP 800-171 compliance begins with an assessment of CDI and CUI environments and existing business processes. Organizations should prepare by compiling all security policy and procedure documentation.



2. Analyze

Once an organization's NIST SP 800-171 scope has been assessed, the data must be analyzed to determine the existing compliance gap. This gap will inform the implementation roadmap.

3. Implement

With the help of RSI Security's NIST SP 800-171 expertise, organizations will begin implementing all necessary controls and IT environment segmentations to achieve compliance.

4. Audit

Following initial compliance gap remediation, RSI Security will conduct a NIST SP 800-171 audit. The audit will determine completeness and validate compliance.

5. Manage

Organizations must continually manage their NIST SP 800-171 compliance. RSI Security will periodically perform gap assessments and services such as penetration testing to help ensure ongoing adherence.

Detection, Response, and Recovery

As a managed security services provider (MSSP), RSI Security will assist your organization with detecting, responding to, and recovering from cyberattacks. Managed detection and response services continuously monitor your IT environment for suspicious or noncompliant activity and execute the defined incident response plan (IRP). Should a data breach occur, RSI Security will assist with and advise on recovery efforts.

About RSI Security

RSI Security is dedicated to helping our partners rethink their cybersecurity efforts and achieve compliance. For NIST SP 800-171, the CMMC, and other frameworks that apply to your organizations, our expertise is backed by over a decade of helping companies successfully assess, implement, maintain, and report their compliance. Contact RSI Security today to learn more about NIST SP 800-171 and CMMC compliance.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com