NIST 800-171 Security Assessment & Compliance Services

United States Department of Defense contractors that collect, store, or transmit Covered Defense Information (CDI) or Controlled Unclassified Information (CUI) are required to comply with NIST regulations 800-171 by December 31, 2017. All prime contractors and their subcontractors must comply with NIST 800-171 or risk losing their government contracts.

At RSI we are experts in guiding you through the process of achieving NIST 800-171 compliance via deep examination and distilling of your company's specific CUI scope. Our compliance solution involves upfront discussion and insightful consultation that leads to efficient definition of scope, reducing our client's overall cost of compliance.

Our security experts assist government contractors understand the risks of storing CUI data in their system, and identify potential liability if CUI is mishandled. RSI's thorough consultation and gap analysis services, augmented by intensive vulnerability scans and penetration tests, will result in fully informed understanding of current posture. We will guide you through NIST 800-171 so that your systems are either out of liability scope or are fully compliant with regulations.

Consultation and Gap analysis

RSI's security team will assess current compliance status and scope of CUI exposure and potential liability. Findings will encompass security posture, verification of current policies and procedures to safeguard CUI, and a detailed roadmap on recommended measures for NIST 800-171 compliance.

IT Infrastructure Assessments

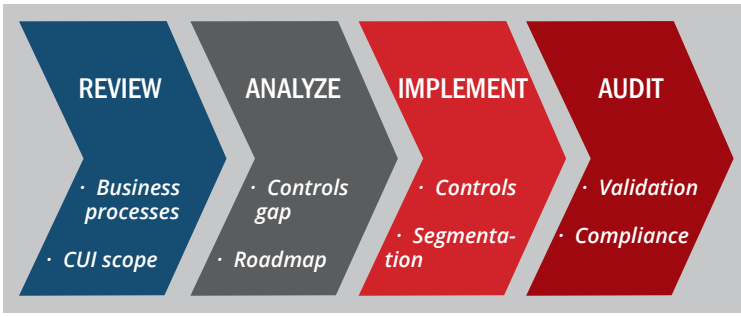
Regular review of your organization's existing IT infrastructure helps you identify opportunities for improvement, allowing for more informed and strategic business decisions to take place.

Vulnerability Assessments

Our vulnerability assessment analysis identifies, quantifies and prioritizes all potential hazards that might affect your energy supply systems.

Penetration Testing

RSI can simulate real-world attacks to assess our client's external applications, network, and mobile applications vulnerabilities in addition to running independent, automated security scans encompassing the Open Web Application Security Project (OWASP) Top 10 vulnerabilities. Our network level penetration test reveals system vulnerabilities that can be easily exploited by real world attackers.



Our NIST 800-171 assessment service include the following subset of NIST 800-171 controls:

- Access Controls
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information integrity

4370 La Jolla Village Drive, Suite 200 • San Diego, CA 92122 • www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com

Services

Identification
Identification services provide control and protocols for managing Cybersecurity. At RSI, we have management tools that capture, track, and compare a client's Cybersecurity asset inventory with their risk tolerance for clients of any size (Tier 1-4).

Protection
RSI offers many IT services that range from simple IT helpdesk support to Cybersecurity and forensics. We understand the importance of setting up an end users' IT network with the adequate security measures and software that will provide them with the highest level of protection for their individual IT setup.

Detection
In the event that a RSI client experiences any form of an intrusion or breach to their endpoint system, we have the ability to detect any adverse or negative Cybersecurity events, determine if our protective solutions have successfully mitigated the matter, and notify the client.

Response & Recovery
In the confirmed event that a RSI client has experienced a security breach, RSI can and will support and advise them through the Incident Response lifecycle. If the breach is complex, and requires additional services (AD Hoc services), RSI will provide the client with our base support and guidance services and provide the client with an IRP (Incident Response Plan).

About RSI

RSI is the nation's premier information security and compliance provider dedicated to helping organizations achieve risk-management success. We work with some of the world's leading companies, institutions and governments to ensure the safety of their information and their compliance with applicable regulation. We also are a security and compliance software ISV and stay at the forefront of innovative tools to save assessment time, increase compliance and provide additional safeguard assurance. With a unique blend of software based automation and managed services, RSI can assist all sizes of organizations in managing IT governance, risk management and compliance efforts (GRC).

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
APPROVED SCANNING VENDOR

858.999.3030

info@rsisecurity.com
www.rsisecurity.com

4370 La Jolla Village Drive
Suite 200 • San Diego, CA 92122