COMPLIANCE

REDSEAL

SUPPORT FOR DFARS NIST 800-171

SECURITY CONTROLS REQUIREMENT

THE FOUNDATION FOR RESILIENCE

BACKGROUND

On December 30, 2015, the U.S. Department of Defense (DoD) published a three-page interim rule to the Defense Federal Acquisition Regulation Supplement (DFARS), revising its earlier August 2015 interim rule on Safeguarding Covered Defense Information. The new interim rule gives contractors a deadline of December 31, 2017 to implement all of the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.

NIST Special Publication 800-171 provides federal agencies with requirements for protecting Controlled Unclassified Information (CUI) when:

- The CUI is resident in non-federal information systems and organizations
- The information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies
- There are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry.

If you are a federal contractor and have access to CUI you MUST follow this framework. In fact, agencies have been prescribing this in contracts and RFPs for the past several months. We recommend that you review any outstanding contracts and/or bids to see how many require you to meet the requirements of NIST 800-171.

These new requirements have forced security departments to spend an inordinate amount of time collecting, organizing, monitoring and reporting in order to detect and manage control-related activity. It is therefore no surprise that cybersecurity and compliance teams are searching for technology to automate this necessary but taxing process.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SUPPORT FOR DFARS NIST 800-171 SECURITY CONTROLS REQUIREMENT

According to NIST SP 800-39, commercially available automated tools must "support situational awareness, or [maintain] awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes." However, NIST also cites that those tools, as well as corresponding processes designed to generate risk data, are not being deployed in a timely fashion. As a result, system security assessments and authorizations are usually based on infrequently conducted vulnerability scans or audits that test security controls at a single point in time, leaving security professionals unable to measure the real risk to systems between security control test cycles. Organizations are finding that it is one thing to implement the 800-53 controls, but quite another to implement and monitor them continuously. Most struggle to do so.

There are 14 specific security objectives contained in the NIST 800-171 that need to complied with, each with a variety of unique controls:

NIST 800-171 SECURITY REQUIREMENT FAMILIES	
Access Control *	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 Communication Protection *	System and Information Integrity *

*RedSeal supported security requirement family

SUPPORT FOR DFARS NIST 800-171 SECURITY CONTROLS REQUIREMENT

REDSEAL AND FEDERAL GOVERNMENT CYBERSECURITY

RedSeal has a history of supporting federal government cybersecurity initiatives. The company's innovative software platform is installed in numerous DoD, intelligence, and civilian organizations for the purpose of continuous monitoring. At the highest level, RedSeal delivers three core security controls:

- **Visibility:** Automated network mapping and situational awareness
- **Verification:** Continuous comparison of network security architecture against desired posture
- **Prioritization:** Analysis of vulnerability scan data and network architecture to identify the highest risk vulnerabilities that must be remediated immediately

REDSEAL SUPPORT FOR NIST SP 800-171 CONTROLS

RedSeal's cybersecurity capabilities closely align with many of the controls in NIST 800-171. RedSeal supports a total of 26 controls in 7 of the 14 NIST 800-171 security requirements families. At a high level, RedSeal supports 800-171 control areas as follows:

NIST CONTROL AREA	REDSEAL SUPPORT
Configuration Management	Continuous validation of actual system configurations versus desired state across multi-vendor infrastructure.
Risk Assessment and Incident Response	Prioritization of vulnerabilities for efficient and effective remediation and response.
Network Security Architecture and Access Control	Network map and situational awareness for risk assessment, systems categorization and segmentation validation.
Security Assessment and Continuous Monitoring	Analysis of actual, deployed information flow architecture and continuous comparison with desired architecture and policy.
Planning, Program Management and Acquisition	Inventory, audit and analysis of network security architecture for legacy, new deployments, and acquired systems.

SUPPORT FOR DFARS NIST 800-171 SECURITY CONTROLS REQUIREMENT

With RedSeal, federal system integrators can significantly reduce the cost associated with enforcing compliance with SP 800-171 by automating assessment of many of the SP 800-171 controls. Certain controls have traditionally been very difficult to automate, and so are resource intensive to maintain and audit. However, RedSeal's unique technology can automate and prioritize these troublesome controls, greatly decreasing resource requirements while actually improving the quality of the control. For example:

- **Network Segregation:** Internal and external network isolation based on router ACLs and firewall rules is a fundamental control in SP 800-171 and in many other compliance regimens. But testing the control at scale is a massive task, especially in multi-vendor environments. Many thousands of rules on hundreds of devices may be deployed to create just one isolated domain. Analyzing these against a security policy is a huge effort with lots of potential for error. RedSeal can not only automate this analysis in preparation for an audit, it can also continuously monitor the control and provide daily reporting on control integrity. This significantly improves threat defense posture while not requiring additional personnel or technical resources.

- **Penetration Testing:** Comprehensive penetration testing involves a combination of automated and manual procedures. A typical pen testing control activity calls for re-testing when there is any change to the controls being tested (e.g. perimeter defenses). When this scales to a large environment where a large number of changes are taking place, blanket manual processes are no longer realistic. RedSeal lets you focus the pen testing on the boundaries most likely to be affected by a change and with the highest risk potential.

- **Vulnerability Scanning:** All vulnerability scanning control activities are implemented for the purpose of identifying and remediating vulnerabilities; identifying the vulnerabilities is just the start of the process. But like pen testing, vulnerability scanning doesn't scale easily and can get expensive quickly. You need to determine where to launch scans

SUMMARY

With more emphasis on leveraging technology to improve intra-agency and inter-agency collaboration (specified in current FISMA guidelines), the federal government is placing a greater sense of urgency on real-time situational awareness and continuous monitoring to improve the efficiency and effectiveness of responses to emerging security threats. While a laudable goal, implementing complex control sets and frameworks such as NIST SP 800-171 at scale is a major challenge, even for periodic audits. RedSeal was designed to cope with the difficulties of achieving of continuous monitoring of key NIST 800-53 and 800-171 controls such as topology mapping, network segmentation and vulnerability scanning. By implementing RedSeal, organizations can lower the cost of compliance, increase situational awareness, and improve control activity efficacy in an operationally efficient manner.

SUPPORT FOR DFARS NIST 800-171 SECURITY CONTROLS REQUIREMENT

APPENDIX

RedSeal NIST SP 800-171 Detailed Control Support

NIST 800-171 FAMILY	SUPPORTED CONTROLS	RELEVANT CONTROL REQUIREMENT SUMMARY	REDSEAL CONTROL ACTIVITY SUPPORT
AC-Access Control	3.1.3, 3.1.14, 3.1.20	Information flow enforcement: Regulation of where data is allowed to travel, including remote access and extranets. Commonly implemented using network enforcement	Analysis of actual, deployed information flow architecture and continuous comparison with desired architecture & policy. Identification of failure of information flow enforcement controls.
CM-Configuration Management	3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.6, 3.4.7, 3.4.8,	Management of system configurations for consistency and highest possible security. Security impact analysis for proposed changes.	Continuous evaluation of actual system configurations versus desired state as defined by information policy. Recommendations for high security configuration settings across multi-vendor infrastructure. Full customization for environment specific requirements. What-if analysis of proposed configuration versus policy.
IR-Incident Response	3.6.1, 3.6.2	Adequate and appropriate incident handling	Rapid analysis of network architecture and attack vectors specific to the targets(s) of the incident.
RA-Risk Assessment	3.11.1, 3.11.2, 3.11.3	Enterprise architecture and risk management strategy	Network map of enterprise architecture. Prioritization of vulnerabilities based on network architecture to inform risk management

SUPPORT FOR DFARS NIST 800-171 SECURITY CONTROLS REQUIREMENT

RedSeal NIST SP 800-171 Detailed Control Support continued

NIST 800-171 FAMILY	SUPPORTED CONTROLS	RELEVANT CONTROL REQUIREMENT SUMMARY	REDSEAL CONTROL ACTIVITY SUPPORT
SA-Security Assessment	3.12.1, 3.12.2, 3.12.3	Security control assessment and continuous monitoring. System interconnections documentation and policy alignment, including internal classified non-classified, public network and extranets. Continuous monitoring of vulnerabilities and information security. Remediation plan for control deficiencies. Penetration testing.	Automated creation and maintenance of network map. Evaluation and continuous monitoring of system interconnections within and between domains or missions. Prioritization of vulnerabilities for efficient and effective remediation.
SC-System and Communications Protection	3.13.1, 3.13.2, 3.13.3, 3.13.5, 3.13.6, 3.13.7	Monitoring and audit of privacy controls	Auditing of network level privacy controls.
SI- System and Information Integrity	3.14.1, 3.14.6	Appropriate developer security architecture and testing	Assist developers of networked systems to design, implement and test appropriate security architecture.