SOLUTION BRIEF

TENABLE FOR DFARS

Defense Federal Acquisition Regulation Supplement

REQUIREMENTS FOR DOING BUSINESS WITH THE U.S. DEPARTMENT OF DEFENSE

The Defense Federal Acquisition Regulation Supplement (DFARS) governs all aspects of data protection in unclassified environments. DFARS 252.204-7012 requires all Department of Defense (DoD) system integrators, contractors, subcontractors and service providers in the supply chain to implement National Institute of Standards and Technology **(NIST) Special Publication (SP) 800-171** data security guidance by December 31, 2017. Permission to exchange certain information with DoD will be granted only to vendors that can document protection of their IT systems in accordance with the mandated levels of security specified in SP 800-171 standards, *"Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."*

Companies currently engaged in DoD contracts or interested in bidding on new opportunities must comply with these requirements by the end of 2017. Failure to comply, and to demonstrate continuing compliance, will prevent authorization to participate in these federal programs. Solution requirements include self-reporting capabilities, an organizational process framework for secure operations, single-pane-of-glass vulnerability management, role-based access control, ubiquitous data source interface, situational awareness, scalability and customization.

DEMONSTRATE COMPLIANCE **NOW** TO ENSURE ACCESS TO $50 BILLION DOD MARKET

The increasingly volatile cyber threat landscape has prompted the government to mandate more stringent security requirements to address third-party vendor risk and minimize data breaches. Compliance is a dynamic and complex process in today's dispersed information sharing and collaboration environment. Government security standards — and vendor IT systems — are always changing. While achieving continuous compliance with DFARs may seem like a daunting task, keep in mind that NIST standards, including 800-171, are based on best-practice standards that many organizations already have in place. In any case, achieving, maintaining and documenting consistent compliance will require an organized and disciplined approach that encompasses the following steps:

Establish a baseline: Access current level of compliance with the specific security standards and reporting procedures that apply to your company's DoD contracts.

Automate assessment: Conduct security assessments to demonstrate safeguards that comply with required technical controls.

Continuously monitor: Track controls on an ongoing basis to ensure effectiveness; implement corrective action as necessary.

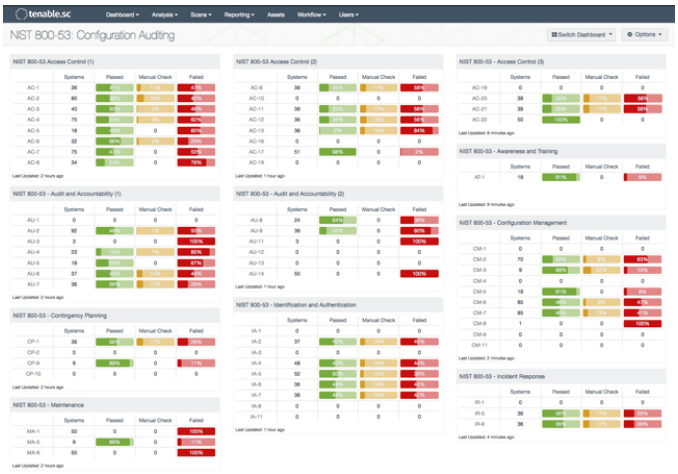
TENABLE.SC™ (FORMERLY SECURITYCENTER)

Automated Monitoring and Assessment: Continuously measure, visualize, demonstrate and communicate adherence to NIST SP 800-171 technical controls to ensure proper implementation, intended operation and desired outcome. Instantly assess federal data you process and quickly evaluate security gaps to accelerate the path to DFARs compliance.

Continuous Monitoring: Gain continuous visibility of data systems, networks and processes across on-premise, mobile, cloud and virtual environments to detect all unauthorized, inappropriate or suspicious access and activity. Trigger DFARS-required incident reporting, immediate investigation and accelerated response designed to thwart potential attacks. A combination of active scanning, agent scanning, passive listening, intelligent connectors to third-party systems, and host data monitoring assess the protection status of your entire infrastructure.

Assurance and Reports: Rely on out-of the- box customizable reporting tools and technologies, including interactive dashboards and Assurance Report Cards (ARCs), that monitor, measure and display real-time security status and alignment with NIST SP 800-171 requirements. Correlate and simplify audit, assessment and reporting processes to enhance security posture and facilitate compliance.

SOLUTION BRIEF



TENABLE.SC AUTOMATES NIST SP800-171 SECURITY REQUIREMENTS

Tenable.sc automates many of the NIST SP 800-171 controls, offering broad coverage of vulnerabilities, including the following control categories:

- Access Control (22 controls)
- Media Protection (9 controls)
- Awareness and Training (3 controls)
- Personnel Security (2 controls)
- Audit and Accountability (9 controls)
- Physical Protection (6 controls)
- Configuration Management (9 controls)
- Risk Assessment (3 controls)
- Identification and Authentication (11 controls)
- Security Assessment (3 controls)
- Incident Response (3 controls)
- System and Communications Protection (16 controls)
- Maintenance (6 controls)
- System and Information Integrity (7 controls)

NIST SP 800-171 SAMPLE REQUIREMENTS

- Assess risk to organizational operations, assets and individuals and the associated processing, storage or transmission of CUI
- Scan for and remediate vulnerabilities in systems and apps
- Continuously assess and monitor security controls
- Implement plans to correct deficiencies and reduce or eliminate vulnerabilities
- Develop and update system security plans

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **publicsectorsales@tenable.com** or visit **tenable.com/contact**