FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Tripwire ExpertOps and NIST 800-171

Federal security managers expect that most federally run systems are actively engaging with FISMA compliance for protecting federal data and systems. However, as we all know, federal information does not remain only in federally operated systems. Data and IT systems connect via the Internet and other networks for business, operations and research. Information about citizens, banking and finance, research and development, and many other federal connected systems transmit data outside the federal networks—and their security compliance standards.

So, it makes sense that FISMA would adapt to address more than the original scope of perceived threats to specifically address systems and data security that inter-agency networks, vendors, contracts and supply chain puts at risk.

In plain English, any company or organization that contracts with the federal government and handles, processes or stores sensitive government information must comply with the security controls described in SP 800-171. This instruction impacts a range of "external service providers," including state and local governments, non-profits, materials vendors, and systems integrators. The effective date was December 2017.

"Controlled Unclassified Information" (CUI) is a categorization of information that encompasses any information that could be considered non-public/ sensitive.

This information used to be known as "Sensitive but Unclassified" (SBU). SBU changed to CUI as part of government-wide efforts to better mark, manage and address risks to this information.

Which Controls are Important for CUI?

There are 110 control requirements in NIST SP 800-171 organized in "families" of controls similar to other NIST-authored guidance. The control requirements are indicated as either "basic" or "derived." The contractor should use NIST guidance FIPS Publication 200 and NIST SP 800-53 rev 4 to examine more details about the controls.

The significant goal is to apply controls as described in the control families. Many of these control requirements can be met with Fortra's Tripwire® ExpertOps$^{\text{SM}}$, along with documentation of processes and procedures.

HIGHLIGHTS

- Quickly achieve compliance for NIST 800-171
- Addresses 11 of the 14 control families
- Support from designated Tripwire Experts
- Cloud-hosted infrastructure combined with consulting services
- Broadest depth and breadth of compliance policy and platform coverage

How Does This Impact Acquisition?

The impact to most federal organizations and contractors is that new guidance (such as NIST 800-171) drives organizations to build additional security rules into contracts and makes compliance to these rules part of the selection process. This could impact both existing and future contracts.

Agency and other federal entities should not assume that procurement processes will be able to advise the buyer organization or the vendor in a timely manner. NIST 800-171 went into effect as of December 2017. It is incumbent on the vendor community to pay close attention to these rules and updated guidance to ensure they are able to meet federal rules, and remain "in sync" with their customers' procurement teams.

Your Solution: Tripwire ExpertOps

Tripwire ExpertOps combines managed services with the industry's best file integrity monitoring (FIM) and security configuration management (SCM) to address multiple NIST 800-171 controls. The solution provides personalized consulting and cloud-based infrastructure to help you achieve and maintain compliance. The solution is easy to deploy and use, with simple subscription pricing and a low total cost of ownership.

Tripwire ExpertOps enables you to rapidly achieve compliance with NIST 800-171 throughout your infrastructure by reducing the attack surface, increasing system integrity and delivering continuous compliance. Plus, because Tripwire ExpertOps includes personalized consulting, you receive ongoing support from a designated Tripwire Expert.

Benefits

- 24/7 compliance visibility via a customized dashboard
- Alerts and reports in your inbox
- Waivers and change requests made easy
- No more awkward or incomplete hand-offs when your staff changes

NIST 800-171 Control Family, Basic Security Requirements	Tripwire ExpertOps Coverage
3.1 – Access Control	◕
3.2 – Awareness & Training	○
3.3 – Audit & Accountability	○
3.4 – Configuration Management	●
3.5 – Identification & Authentication	◕
3.6 – Incident Response	◕
3.7 – Maintenance	◑
3.8 – Media Protection	◑
3.9 – Personnel Security	○
3.10 – Physical Protection	○
3.11 – Risk Assessment	◔
3.12 – Security Assessment	◕
3.13 – System & Communications Protection	◑
3.14 – System & Information Integrity	◕

How it Works

Tripwire ExpertOps provides you with continuous staffing to operate and manage Tripwire-provided NIST 800-171 controls at peak efficiency. The solution adapts to your unique environment—reports and profiling tasks are customized to meet your specific needs. You will receive expert guidance to configure your system and policy configurations to best align with your requirements. And you'll gain visibility via 24/7 access to compliance information via a tailored dashboard and management console.

A Tripwire Expert will act as an extension of your team by prioritizing work efforts and managing critical escalations. Together you will jointly develop a Service Plan that outlines communication practices, escalation procedures and any specialized requests.

The Tripwire Expert will then tune and operate your Tripwire-provided NIST 800-171 controls to provide:

- Prescriptive policy and content guidance to enable NIST 800-171 compliance for your specific network or system security requirements
- Recommendations for maximizing automation capabilities for compliance and event alerting practices, change management process integrations, and audit prep activities
- Prioritized remediation to identify opportunities to efficiently improve compliance posture
- Organizational grading for each accountable department to provide visibility into groups needing additional resources and attention

Ready to Take the Next Step?

Get in touch with your Tripwire Account Manager—or visit www.tripwire.com/contact-us—to develop a custom Service Plan for NIST 800-171 compliance.

Migrating from Tripwire Enterprise?

We can help with migration services and pricing. Contact your Tripwire Account Manager for details.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.