PRESIDIO®
Future. Built.

SERVICES FOR STRENGTHENING NIST COMPLIANCE

When regulatory requirements are critical to winning business, companies need an expert partner in minding (and mending) the compliance gaps.

In its quest to safeguard Confidential Unclassified Information (CUI), the National Institute of Standards and Technology (NIST) lists detailed requirements about which organizations can handle CUI, how, and with what technology. Increasingly, compliance with NIST 800-171 standards is a requirement for doing business with federal agencies and contractors.

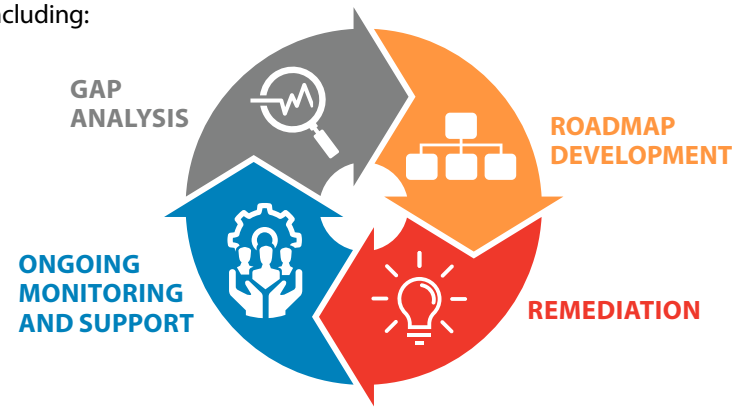
It's a heavy lift for companies not used to this level of formality in managing and controlling data. Information may be hard to locate across systems and storage places. InfoSec teams juggling multiple priorities may be challenged to add NIST compliance—and its data management demands—to their to-do lists. And resources may be limited for achieving the required security controls, maintaining processes and documentation, and training staff.

Presidio can help.

A TURNKEY NIST COMPLIANCE RESOURCE

Our expert teams will work with you to assess NIST 800-171 adherence, address any gaps, and achieve compliance—now and in the future.

Our support extends through the full NIST 800-171 compliance lifecycle, including:



Through a presentation and written report, you'll receive an executive summary of current vulnerabilities and a detailed technical picture of risk, supported by vendor-agnostic recommendations. (This includes additional recommendations for data integrity and availability as needed.)

WE'LL ALSO WORK WITH YOUR TEAM TO:

- *Develop policies and processes for handling CUI*
- *Design and implement technical architecture*
- *Train staff in security awareness*

Whatever your current security state, you'll soon find your operations in full compliance, your staff freed up for other projects, and federal agencies more confident than ever in your ability to protect sensitive information.

PRESIDIO: SERVICES FOR STRENGTHENING NIST COMPLIANCE

Unparalleled expertise in compliance and cyber security

Presidio knows how to navigate NIST's complex compliance requirements, with deep expertise in both NIST 800-171 and its precursor NIST 800-53. We're also experts in overall data protection. Our elite team draws from a pool of cloud, infrastructure, data center, and unified communications specialists.

Proven processes for ensuring adherence

With more than a decade of engaging with clients large and small, we've developed the industry's most thorough, informed assessment process and methodology, involving:

- **A baseline view of compliance** that includes an assessment of risk, business requirements, and strategy
- **Technical verification** through assessment, penetration testing, executive reporting, and more
- **Operational support** in areas such as the prevention, detection, containment, and correction of security violations
- **Planning and execution** for the design, integration, and optimization of compliant architecture and processes

A full-service, fully committed partner

Presidio operates as an extension of your IT department, collaborating with your team at every step. We take the time

to thoroughly understand your risk, resources, and priorities, so we can bring the most informed compliance guidance to your operations and business.

Take steps today to achieve the NIST 800-171 compliant operations that lead to more federal and agency business. Call Presidio for a comprehensive compliance assessment and support.

PLEASE CONTACT:

CyberSecurity@presidio.com

presidio.com

LEARN MORE ABOUT PRESIDIO'S FULL SUITE OF CYBER SECURITY SOLUTIONS:

ADAPTIVE STRATEGY

Get expert guidance on cyber security strategy and governance, regulatory compliance, policy and procedures, security awareness and training, architecture and next generation risk management.

ADAPTIVE TESTING

Gauge risk and preparedness through vulnerability assessments, penetration testing, red & red/blue team scenarios and comprehensive security analyses. Check compliance with HIPAA, PCI, GDPR, (NIST Cyber Security Framework, NIST 800-53, NIST 800-171) and ISO 27001 regulations and standards, plus all 20 CIS controls.

ADAPTIVE ARCHITECTURE

Achieve a scalable security architecture/roadmap, including cloud and IoT security, through firewall analysis, device hardening, control recommendations, active directory analysis and PKI assessment.

Build and strengthen application, network, data, endpoint, cloud and physical security.

ADAPTIVE SECOPS

Get 24x7x365 next generation risk management that includes device management, threat intelligence and incident response, plus security event and information management that uses event correlation and analysis and machine learning technology.