

# NIST SP 800-171 Security Assessment Services

*Protect the Federal Controlled Unclassified Information (CUI) In Your Care.*

- Assure your government customers that their information is safe with you
- Keep from losing vital federal and defense contracts
- Establish and maintain a CUI-specific risk management and compliance program
- Get to compliance quickly with the leader in NIST standards

Organizations that store, process, or transmit federal controlled unclassified information are required to follow NIST SP 800-171, the federal standard for handling CUI in non-government systems. If they don't, they will be disqualified from bidding on or holding federal and defense contracts.

If you aren't sure whether the federal data and records you handle are CUI, or if you aren't sure whether you have the right safeguards in place to protect that CUI, contact Telos® Corporation. We're the leading experts in the NIST way of managing risk and ensuring security compliance for federal IT systems and information.

We'll help you identify the federal information you hold that might qualify as CUI and show you what you need to do to follow and enforce the controls specified by NIST SP 800-171. Our Xacta® solution for NIST assessments streamlines and automates many of the steps involved for NIST SP 800-171 requirements so our security experts can get you compliant faster and help you stay compliant.

## Federal controlled unclassified information includes:

- Health information
- Legal documents
- Financial data
- Law enforcement records
- Personally identifiable information
- Technical specifications
- Geospatial imagery
- Proprietary business information  
...and more.

## Take the first step toward NIST SP 800-171 compliance with Telos.

The first step is being able to show that you're putting a compliance plan in place. Then you need to demonstrate that you're staying compliant over the long term. There's a lot involved — but no matter where you are on your NIST 800-171 journey, Telos can help you create and maintain a program that safeguards the federal information in your care.

## Over a Hundred Security Controls Across 14 Categories: Are You Ready?

NIST SP 800-171 specifies 110 security controls organized into 14 categories. We'll help you take control of the challenge by identifying which controls apply to your requirements and guide you to meeting them.

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authorization
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

## Telos offers the experience and capabilities you need for NIST SP 800-171 compliance.

Using our proven methodologies and certified security personnel, Telos can provide the level of support necessary to exceed your requirements, resulting in exceptional results. Our professionals will:

**Scope the situation.** First, Telos will help you identify any federal information in your custody that falls into one of the National Archive's 22 categories of CUI. Then we'll assess the systems in your organization that store, process, or transmit CUI or provide security and administration to the CUI in your care.

**Identify the security controls you need.** NIST SP 800-171 specifies 110 security controls organized in 14 families to assure best practices in protecting CUI. Using our Xacta solution, Telos will identify the controls you need to comply with, supplemented by best-practice configuration requirements for the hardware, software, and networks involved. We'll document the security safeguards you have in place, mapping each mechanism for securing and protecting the CUI to the relevant security controls.

**Review and define your security architecture.** We'll evaluate the current architecture of your CUI-related systems and recommend any modifications needed to meet the requirements of NIST SP 800-171. Afterward, we'll document that the new security architecture properly separates corporate and government client information to isolate CUI into its own security domain.

**Assess your compliance with security controls.** We start by assessing your current state of

compliance with the identified security controls. We then plan and conduct the assessment, which will include compliance and vulnerability testing of technical controls and evaluation of security policies, procedures, and administrative controls through interviews, reviews, and inspections.

**Address anything that needs remediation.** After identifying any vulnerabilities or non-compliant controls, we'll assess the residual risk of the system and recommend steps for remediation or mitigation documented in a comprehensive action plan (POA&M, or Plan of Action and Milestones).

### About Telos Corporation

Telos Corporation delivers solutions that empower and protect the world's most security-conscious enterprises. Whether we're investigating vulnerabilities, testing your security against external and internal threats, or engineering a hardened IT environment, Telos delivers the capabilities you need for information security and assurance.

For almost three decades, we've provided information security services that protect leaders in financial services, healthcare, technology and other industries, including members of the Fortune 500. We also serve government agencies and contractors who need to ensure that their systems meet federal cyber security standards. Our customers return to us year after year for the in-depth assessment they know they need to stay vigilant in the face of increasing and ongoing threats.

Our cleared and credentialed security experts offer the skills, capabilities, and background to ensure you're ready to meet the terms of NIST SP 800-171.



**Contact us for more information.**

Call: 800-708-3567

Email: [info@telos.com](mailto:info@telos.com)