

# NIST 800-171 Compliance

## NIST 800-171 Compliance: Protecting Controlled Unclassified Information (CUI)



NIST SP 800-171 is a set of security standards developed by the [National Institute of Standards and Technology \(NIST\)](#) to protect Controlled Unclassified Information (CUI) in non-federal systems and organizations. This standard is mandatory for contractors and subcontractors working with the [U.S. Department of Defense \(DoD\)](#) who handle CUI.

### What is Controlled Unclassified Information (CUI)?

CUI is information that is not classified but requires safeguarding or protection. It includes a wide range of data, such as:

- Personal information
- Financial data
- Intellectual property
- Critical infrastructure information

### Key Requirements of NIST 800-171

The standard outlines 110 security controls across 14 families, including:

- Access control: Limiting access to CUI to authorized personnel.
- Identification and authentication: Ensuring individuals are who they claim to be.
- Media protection: Protecting physical and electronic media containing CUI.
- Awareness and training: Educating employees about security risks and responsibilities.
- Risk assessment: Identifying and managing security risks.
- Incident response: Having a plan in place to respond to security incidents.



## Why is NIST 800-171 Important?

Compliance with NIST 800-171 is crucial for organizations handling CUI for several reasons:

- Contractual obligations: Many government contracts require compliance.
- Risk mitigation: Protects sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Enhanced security posture: Improves overall cybersecurity practices.
- Customer trust: Demonstrates a commitment to data protection.

## Achieving NIST 800-171 Compliance

Achieving compliance involves a comprehensive approach:





















- Risk assessment: Identify CUI and assess potential risks.
- Gap analysis: Compare current security practices with NIST requirements.
- Implementation: Implement necessary controls and procedures.
- Documentation: Maintain detailed records of compliance efforts.
- Continuous monitoring and improvement: Regularly review and update security measures.

## What's Next?

- ✓ Learn more about [ImmuniWeb Compliance Services](#).
- ✓ Read ImmuniWeb [Cyber Law and Cybercrime Investigation Blog](#).
- ✓ Join ImmuniWeb at the upcoming [Webinars](#) and [Events](#).
- ✓ Follow ImmuniWeb on [LinkedIn](#), [X \(Twitter\)](#), and [Telegram](#).
- ✓ Subscribe to ImmuniWeb [Newsletter](#).
- ✓ Try ImmuniWeb [Community Edition](#) Free Security Tests.
- ✓ See the benefits of ImmuniWeb [Partner Program](#).



The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.

 <a href="#">API Penetration Testing</a>	 <a href="#">Continuous Automated Red Teaming</a>	 <a href="#">Dark Web Monitoring</a>	 <a href="#">Phishing Websites Takedown</a>
 <a href="#">API Security Scanning</a>	 <a href="#">Continuous Breach and Attack Simulation</a>	 <a href="#">Digital Brand Protection</a>	 <a href="#">Red Teaming Exercise</a>
 <a href="#">Attack Surface Management</a>	 <a href="#">Continuous Penetration Testing</a>	 <a href="#">Mobile Penetration Testing</a>	 <a href="#">Third-Party Risk Management</a>
 <a href="#">Cloud Penetration Testing</a>	 <a href="#">Cyber Threat Intelligence</a>	 <a href="#">Mobile Security Scanning</a>	 <a href="#">Web Penetration Testing</a>
 <a href="#">Cloud Security Posture Management</a>	 <a href="#">Cybersecurity Compliance</a>	 <a href="#">Network Security Assessment</a>	 <a href="#">Web Security Scanning</a>

One Platform. All Needs.  
[www.immuniweb.com](http://www.immuniweb.com)

This document is provided "as is" without any warranty of any kind for informational purposes only.