Achieve NIST 800-171 compliance with Nipper

TITANIA NIPPER

NIST

Any organization that processes or stores Controlled Unclassified Information (CUI) for government agencies must be compliant with **NIST 800-171**

110 NIST 800-171 security requirements

are organized into **14 families.**

14

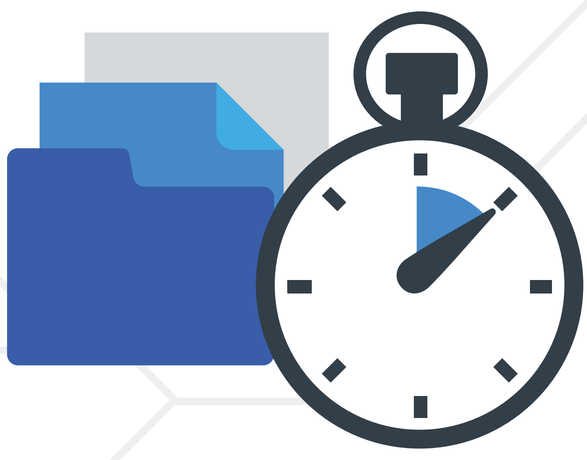
1. Access Control
2. Awareness & Training
3. Audit & Accountability
4. Configuration Management
5. Identification & Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personal Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System & Communications Protection
14. System & Information

Using the Nipper NIST 800-171 Module,

you can assess compliance with up to **60%** of NIST 800-171 core network security requirements across **6** control families.

Other Nipper reporting modules can meet a further **29%** of the total NIST 800-171 requirements.

Prioritize remediation advice based on ease of fix and likelihood of exploitation



Consolidate all relevant NIST 800-171 findings in a report that can be **generated in minutes**

Nipper is in service with all **four** arms of the DoD, to automate the configuration audits of core network devices against standards and frameworks, such as **DISA STIG, DISA RMF, CMMC** and **CIS benchmarks.**

CIS SECURITY BENCHMARKS CERTIFIED

TITANIA Assured Accuracy

TITANIA NIPPER

Find out more about our NIST 800-171 auditing solution

titania.com/nist-800-171