



# 5NINES CYBER SECURITY SERVICES

## NIST 800-171 REQUIRED COMPLIANCE

### WHAT IS NIST 800-171?

NIST 800-171 is a business-oriented cybersecurity standard that provides technical specifications, guidelines, recommendations and annual reports to help keep business's information safe. This standard became a requirement in January 2018 for companies working with controlled unclassified information (CUI) anywhere along the Department of Defense (DoD) supply chain. DoD affiliates that fail to meet compliance standards risk losing their federal contracts and face increased vulnerability to cyber-attacks, which can severely damage or even destroy a business.

### WHAT WE OFFER

#### 1. Comprehensive Vulnerability Assessment (CVA)

- First step in addressing security vulnerabilities
- Identifies next steps

#### 2. Remediation

- Address and correct each vulnerability

### WHY WORK WITH 5NINES?

Since opening in 2001, we pride ourselves on our extensive security expertise. 5NINES cares about your compliance and cyber security and we have the reliable tools you need to get your company on track.

- We are proud to partner with the WMEP and the WICMP
- We work with top cybersecurity partners like CheckPoint, VMWare and Cisco
- We are audited annually by NIST security controls
- We believe in and apply the strict NIST 800-171 standards

#### 3. Managed Services

- Evaluate your needs, order, update, install and maintain systems within your budget and on your timeline

#### 4. Ongoing Assessments

- Ensures you maintain compliance as time goes on


Analyze Impact and Determine Scope

Assess the current state of security

Develop a plan to achieve compliance and mitigate existing shortfalls

Define responsibilities and policy that maintains sustained NIST 800-171 compliance

Engage third parties to provide a thorough, unbiased review of practices and processes





# YOUR PERSONALIZED PATH TO NIST COMPLIANCE

## 5NINES SERVICES

### PHASE ONE: THE CVA

During the Comprehensive Vulnerability Assessment (CVA), our team evaluates and addresses each of the 14 NIST control families utilizing powerful network scanning tools, our extensive IT experience and best practice guidelines for NIST 800-171 series documentation. A 5NINES technical cyber security specialist then assigns each family an easy-to-understand scoring metric that identifies at-risk areas needing improvement. This starting point is critical in identifying what steps need to be taken next.

### PHASE TWO: REMEDIATION

After completing the CVA, consult with a 5NINES technical security specialist to lay out a plan of action. This consulting service walks you or your IT department through mitigating vulnerabilities, fixing architecture, and adding highly-trusted CheckPoint hardware where needed. This one-time consulting work is project-based in order to improve your cyber security footprint.

### PHASE THREE: MANAGED SERVICES

We can manage your cyber security for you. Our 5NINES technical security specialists are highly trained in all things IT, including patch work, anti-virus, incident response and daily troubleshooting. We will also continue to evaluate your needs, place orders, and update, install and maintain your systems. We can do this all within your budget and on your timeline. With this service, you can leave your security to us so you can truly focus on running your business.

### PHASE FOUR: ONGOING ASSESSMENTS

5NINES offers ongoing scans to ensure that your business maintains practices in alignment with the most recent NIST security standards.

### NIST 800-171 CONTROL FAMILIES

Access Control	Awareness & Training
Audit & Accountability	Configuration Management
Identification & Authentication	Incident Response
Media Protection	Maintenance
Physical Protection	Personnel Security
Security Assessment	Risk Assessment
Systems & Comm. Protection	System & Info Integrity

