SUPPLIER PERFORMANCE RISK SYSTEM (SPRS)
NIST SP 800-171 ASSESSMENT REPORT

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Distribution Statement: This document contains Controlled Unclassified Information (CUI) and is for official use only. Distribution is limited to authorized personnel with a need-to-know.

COVER PAGE

Company Name: CyberHygiene Consulting LLC

CAGE Code: [To be assigned]

Assessment Date: December 25, 2025

Report Version: 1.0

Assessment Scope: CyberHygiene Production Network (cyberinabox.net)

Assessment Standard: NIST SP 800-171 Revision 2

Prepared By: Daniel Shannon, System Administrator

Review Date: December 25, 2025

EXECUTIVE SUMMARY

Overall Assessment Results

The CyberHygiene Production Network has undergone a comprehensive self-assessment against all 110 security requirements specified in NIST SP 800-171 Revision 2. This assessment evaluated the implementation of security controls across 14 control families to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

Final SPRS Score: 105 / 110 points

Compliance Percentage: 97.6%

Weighted Score: 220.5 / 226 total possible points

Key Strengths

Robust Access Control Infrastructure

- FreeIPA-based identity management with Kerberos authentication
- Role-Based Access Control (RBAC) with least privilege enforcement
- Comprehensive password policies exceeding NIST requirements
- Account lockout after 5 failed attempts

Comprehensive Encryption Implementation

- FIPS 140-2 validated cryptography across all systems
- Full-disk LUKS encryption on all CUI-containing partitions
- TLS 1.2+ for all network communications
- Hardware encryption on Apple Silicon AI server (T2/M4 Secure Enclave)

Advanced Security Monitoring

- Wazuh SIEM with real-time threat detection
- Comprehensive audit logging (30+ day retention)
- AI-assisted security analysis and log review
- Integration with Suricata IDS/IPS on network perimeter

Secure Architecture

- Network segmentation capability via pfSense firewall
- SELinux mandatory access control in enforcing mode
- OpenSCAP CUI profile compliance (105/105 checks passed)

- Air-gapped AI infrastructure with no external dependencies

Configuration Management Excellence

- Documented baseline configurations
- Version-controlled system documentation
- Automated security updates via dnf-automatic
- Change control procedures with security impact analysis

Identified Gaps and Remediation

Three minor gaps were identified, totaling 5.5 points deficit:

1. IA-8: Multi-Factor Authentication for Non-Organizational Users (-3 points) - Target completion: Q1 2026 - Solution: YubiKey implementation
2. IR-3: Incident Response Testing (-0.5 points) - Target completion: Q2 2026 - Solution: Annual tabletop exercise
3. SI-8: Spam Protection (-2 points) - Target completion: Q1 2026 - Solution: Complete email system deployment

Upon completion of remediation activities, the system is projected to achieve 110/110 points (100% compliance).

System Overview

Component	Specification
Total Systems	5 (2 servers, 3 workstations)
Total CPU Cores	28 (mix of x86-64 and ARM64 architectures)
Total RAM	192 GB
Total Storage	~13 TB (fully encrypted)
Operating System	Rocky Linux 9.6 (RHEL derivative)

Key Capabilities:

- Centralized identity and access management (FreeIPA)
- Encrypted file sharing (Samba + LUKS)
- Security Information and Event Management (Wazuh)
- AI-assisted system administration (Ollama on Apple Silicon)
- Network security (pfSense + Suricata IDS/IPS)
- Automated compliance scanning (OpenSCAP)

DETAILED ASSESSMENT RESULTS

Control Family Scoring Summary

Control Family	Requirements	Possible Points	Achieved Points	%
Access Control (AC)	22	40	40	100%
Awareness and Training (AT)	3	7	7	100%
Audit and Accountability (AU)	9	19	19	100%
Configuration Management (CM)	9	19	19	100%
Identification and Authentication (IA)	11	21	18	85.7%
Incident Response (IR)	6	7	6.5	92.9%
Maintenance (MA)	6	10	10	100%
Media Protection (MP)	8	11	11	100%
Personnel Security (PS)	8	9	9	100%
Physical Protection (PE)	6	8	8	100%
Risk Assessment (RA)	3	7	7	100%
Security Assessment (CA)	3	7	7	100%
System and Communications Protection (SC)	9	39	39	100%
System and Information Integrity (SI)	7	22	20	90.9%
TOTAL	**110**	**226**	**220.5**	**97.6%**

PLAN OF ACTION AND MILESTONES (POA&M)

POA&M Summary

Total Identified Gaps: 3

Total Points Deficit: 5.5 points

Current SPRS Score: 105 / 110 points

Projected Score Upon Completion: 110 / 110 points (100%)

Item	Control	Description	Points Deficit	Target Date
1	IA-8	MFA for Non-Org Users	-3.0	2026-02-28
2	IR-3	Incident Response Testing	-0.5	2026-06-30
3	SI-8	Spam Protection	-2.0	2026-03-31

CERTIFICATION STATEMENT

I certify that this assessment was conducted in accordance with NIST SP 800-171A assessment procedures and accurately reflects the security posture of the CyberHygiene Production Network as of December 25, 2025. All findings are based on documented evidence, system configuration reviews, and operational testing.

The information in this assessment is accurate and complete to the best of my knowledge.

Signature: _____

Name: Daniel Shannon

Title: System Administrator / Security Officer

Date: December 25, 2025

DOCUMENT CONTROL

Document Title: SPRS NIST SP 800-171 Assessment Report

Version: 1.0

Date: December 25, 2025

Classification: CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Review Schedule: Annual (next review: December 2026)

Version	Date	Author	Description
1.0	2025-12-25	D. Shannon	Initial SPRS assessment report

END OF DOCUMENT