Cybersecurity Audit Highlights Report

Client: Falcon Precision Systems, LLC
Industry: Small Defense Manufacturing & Engineering Contractor
Date: April 19, 2026
Prepared By: Oberheim Cybersecurity Consulting

Executive Summary

Oberheim Cybersecurity Consulting conducted a limited cybersecurity assessment of Falcon Precision Systems, a small defense-related business supporting government subcontract work. The assessment focused on endpoint security, user access, network protections, backup practices, and compliance with common defense-sector requirements.

The review identified several critical vulnerabilities that increase the risk of ransomware, unauthorized access, and loss of Controlled Unclassified Information (CUI). Multiple gaps were also noted against expected requirements under NIST SP 800-171 and CMMC Level 2.

Overall Risk Rating: High

Critical Findings

Severity	Finding	Business Impact
Critical	Multi-factor authentication (MFA) not enabled for email, VPN, or administrator accounts	High risk of account compromise and unauthorized access to CUI
Critical	Two engineering workstations and one file server missing security patches older than 120 days	Vulnerable to known exploits and ransomware attacks
High	Shared administrator account used by multiple employees	No accountability, weak password practices, and inability to track actions
High	Sensitive project files stored on a shared drive without access restrictions	Employees can access information unrelated to their role
High	Backups stored only on-site and connected to the network	Backups could be encrypted or destroyed during a ransomware incident

Medium	No formal incident response plan or tabletop exercise completed	Delayed response during a cyber event could increase downtime and losses

---

Compliance Gaps

The following gaps were identified against defense-related cybersecurity expectations:

Requirement Area	Gap Identified	Related Framework
Access Control	No MFA, excessive user permissions, shared admin account	NIST SP 800-171 3.1 / CMMC AC
Audit & Accountability	Limited log retention and no centralized monitoring	NIST SP 800-171 3.3 / CMMC AU
Configuration Management	Missing patch process and undocumented system baselines	NIST SP 800-171 3.4 / CMMC CM
Incident Response	No written incident response plan or annual testing	NIST SP 800-171 3.6 / CMMC IR
Media Protection	Portable USB drives allowed without encryption	NIST SP 800-171 3.8 / CMMC MP
System & Information Integrity	No vulnerability scanning or regular remediation process	NIST SP 800-171 3.14 / CMMC SI

Estimated Compliance Readiness: Approximately 55% aligned with NIST SP 800-171 / CMMC Level 2 expectations.

Prioritized Security Roadmap

Immediate Actions (0–30 Days)

1. Enable MFA for all email, VPN, cloud, and administrator accounts.
2. Patch all systems with critical and high-severity vulnerabilities.
3. Eliminate shared administrator accounts and assign named admin accounts.
4. Restrict access to project folders containing CUI.
5. Create an offline or cloud-isolated backup solution.

Near-Term Actions (30–90 Days)

1. Deploy endpoint detection and response (EDR) software to all workstations and servers.

2. Implement quarterly vulnerability scanning and patch reporting.
3. Develop a written incident response plan and conduct one tabletop exercise.
4. Configure centralized log collection for servers, firewalls, and Microsoft 365.
5. Encrypt all portable media and disable unauthorized USB devices.

Long-Term Actions (90–180 Days)

1. Complete a formal NIST SP 800-171 gap assessment.
2. Develop policies and procedures to support future CMMC Level 2 certification.
3. Segment the engineering network from the general office network.
4. Conduct annual security awareness training focused on phishing and CUI handling.
5. Establish ongoing monthly security reviews with executive leadership.

Conclusion

Falcon Precision Systems has several manageable but significant cybersecurity weaknesses that could impact operations, contract eligibility, and protection of defense-related information. By addressing the immediate high-risk items and following the recommended roadmap, the company can substantially reduce risk and improve readiness for future compliance requirements.

Prepared by:
Oberheim Cybersecurity Consulting