WRIGHTBRAINED
SECURITY

SAMPLE DELIVERABLE · SUPPLY CHAIN

Supplier Security Review

Prepared for Keystone Precision Machining (fictional). Six suppliers reviewed, September 2026. This is what a supplier review from us looks like.

This is a sample. Keystone Precision Machining and every supplier named here are fictional. The format, level of detail and plain-English style are what our clients receive. Two of the six supplier detail pages are shown.

1. Summary for leadership

The bottom line. Most of your suppliers have the basics in place. One does not, and it is the one that can reach every computer in your shop: your managed IT provider has no two-step login on its remote support tool. We recommend limiting that access until it is fixed, which they say will take two weeks.

Where your suppliers landed

Rating	What it means	Count
GO	Ready for the work	3
CONDITIONS	Workable, with a written plan	1
HOLD	Too many unknowns to decide	1
NO-GO	Not for this job, as things stand	1

Top three risks

BrightLine IT can reach every computer without a second login step. One stolen password to their remote tool would give an attacker your whole network.

Precision Gauge connects a laptop to your CMM and hasn't answered. We can't tell you whether that laptop is safe to plug in.

Apex holds your CUI drawings on three unmanaged computers. Fixable, but it needs a date.

Decisions we need from you

Approve turning off BrightLine's remote support tool except during scheduled, supervised sessions until MFA is enforced (target Oct 31).

Decide whether calibration visits continue while Precision Gauge is on Hold, or move to their offline process.

2. All suppliers at a glance

Supplier	Service	Touches	Rating	Key gaps	Next review
BrightLine IT Services	Managed IT provider	Systems access	NO-GO	No MFA on the remote support tool; alerts only reviewed in business hours	Oct 31, 2026
Precision Gauge Calibration	On-site calibration	Systems access	HOLD	No answers or evidence after two requests	Oct 15, 2026
Apex Anodizing & Finishing	Plating and finishing	Sensitive data (CUI drawings)	CONDITIONS	3 of 11 computers not centrally managed; no incident notice clause	Dec 15, 2026
CloudVault File Sharing	Cloud file sharing	Sensitive data (CUI)	GO	None	Sep 2027
Midstate Payroll	Payroll service	Sensitive data (employee records)	GO	None	Sep 2027
Northfield Heat Treat	Heat treating	Internal data (purchase orders)	GO	None that matter for what they touch	Sep 2027

3. How we reviewed

Ask, verify, rank, report. Each supplier answered a short questionnaire. We asked for evidence behind the answers that matter most for what they touch, rated them against the baseline the Department of Defense expects of its own contractors (managed computers, two-step logins, someone watching for attacks, proof, and a promise to tell you about incidents), and wrote this report.

4. Supplier details

BrightLine IT Services NO-GO

Service	Managed IT provider for all 42 workstations and 3 servers
What they touch	Systems access: remote support tool installed on every computer, admin rights
Business owner	Operations manager

Baseline item	Supplier said	Evidence we saw	Verified?
Managed computers	Yes	Patch compliance report, 98% current	Yes
MFA for email, remote, admin	Yes	Email: yes. Remote support tool: password only	No
Monitoring for attacks	Yes, 24/7	Alerts go to a shared inbox, reviewed business hours	No
Backups protected	Yes	Immutable copy confirmed in console screenshot	Yes
Incident notice	Informally	No contract clause	No
Proof	Self-assessment	Questionnaire only	Partly

What we found

The remote support tool, which can reach every computer, accepts a password alone. This is the single biggest risk in the review.

"24/7 monitoring" means alerts land in an inbox that is read during business hours. Ransomware crews prefer weekends.

Conditions to reach Go

Condition	Due	How we'll verify
Enforce MFA on the remote support tool for every technician	Oct 31	Policy screenshot and a live login demo
After-hours alert escalation to a named on-call person	Nov 30	Escalation procedure and a test alert
Add a 72-hour incident notice clause to the service agreement	Dec 31	Signed amendment

Apex Anodizing & Finishing CONDITIONS

Service	Plating and finishing on machined parts
What they touch	Sensitive data: CUI drawings sent by email for each job

Baseline item	Supplier said	Evidence we saw	Verified?
Managed computers	Partly	8 of 11 in device management	Partly
MFA for email, remote, admin	Yes	Conditional access policy screenshot	Yes
Monitoring for attacks	Yes	MSSP contract and monthly report	Yes
Incident notice	No	None in purchase terms	No

Conditions to reach Go

Condition	Due	How we'll verify
Enroll the last 3 computers in device management, or keep CUI off them	Nov 15	Updated compliance report

Condition	Due	How we'll verify
Add incident notice to purchase order terms	Dec 15	Updated PO terms

5. Recommended actions

#	Action	Owner	Due
1	Restrict BrightLine remote access to scheduled, supervised sessions until MFA is live	Operations manager	This week
2	Final evidence request to Precision Gauge; switch to offline calibration if no reply	Quality manager	Oct 15
3	Add incident notice and evidence-on-request language to standard PO terms	Purchasing	Dec 31

This review relied on supplier answers and the evidence they provided. It is not an audit or a test of supplier systems.

Want a second set of eyes?

We're assessors. We find the gaps, direct the fix, and check that it holds. **wrightbrainedsecurity.com/contact** · jil@wrightbrainedsecurity.com