Covers managed service providers, managed security providers, IT consultants, and network and help-desk services. Also complete CWCO-SUP-CYBER for the applicant's own security controls. Complete with ACORD 125. Attach a standard master services agreement.

1 APPLICANT / BUSINESS INFORMATION

LEGAL BUSINESS NAME	DBA	FEIN	YEARS IN BUSINESS

BUSINESS ADDRESS	CITY / STATE / ZIP	WEBSITE

Entity type:
☐ Sole proprietor ☐ Partnership ☐ LLC ☐ Corporation

PRIMARY CONTACT / TITLE	PHONE	EMAIL

2 OPERATIONS

SERVICE	% OF REVENUE

Services: managed IT (monitoring and help desk); managed security (SOC, MDR); cloud and hosting; backup and disaster recovery; network installation; software resale and licensing; projects and migrations; consulting; other.

MANAGED CLIENTS	ENDPOINTS MANAGED	LARGEST CLIENT (% OF REVENUE)	TECHNICIANS

Client industries served (check all that apply):
☐ Healthcare ☐ Financial services ☐ Government ☐ Legal ☐ Critical infrastructure ☐ Retail / e-commerce

2-1 Does the applicant resell or manage clients' security tools (firewalls, EDR, email security)? ☐ Yes ☐ No
IF YES, EXPLAIN

2-2 Does the applicant host client data or applications on its own servers? ☐ Yes ☐ No
IF YES, EXPLAIN

2-3 Does the applicant subcontract work to other IT providers or offshore staff? ☐ Yes ☐ No
IF YES, EXPLAIN

3 EXPOSURE & RISK QUESTIONS — REMOTE ACCESS, RMM TOOLS & CLIENT COMPROMISE

In the 2021 Kaseya attack, ransomware spread through a remote-management tool to about 50-60 MSPs and up to 1,500 of their clients at once. In 2025 another group used an MSP's remote-management platform to steal and encrypt client data.

3-1 Is phishing-resistant multi-factor authentication required for every technician login to RMM, PSA, and client systems? ☐ Yes ☐ No
IF YES, EXPLAIN

3-2 Are RMM and remote-access tools patched within 72 hours of critical security updates? ☐ Yes ☐ No
IF YES, EXPLAIN

3-3 Does each technician have individual, least-privilege access, with no shared admin accounts? ☐ Yes ☐ No
IF YES, EXPLAIN

3-4 Are client environments segmented so one client's compromise can't spread to others through the applicant's tools? ☐ Yes ☐ No
IF YES, EXPLAIN

3-5 Is EDR deployed on all of the applicant's own endpoints and servers? ☐ Yes ☐ No
IF YES, EXPLAIN

3-6 Is the applicant's own environment monitored 24/7 by a SOC or MDR service? ☐ Yes ☐ No
IF YES, EXPLAIN

3-7 Are client backups kept immutable or offline, separate from the RMM platform? ☐ Yes ☐ No
IF YES, EXPLAIN

3-8 Are technician accounts disabled the same day an employee leaves? ☐ Yes ☐ No
IF YES, EXPLAIN

3-9 Has a client suffered a breach, ransomware, or data loss that the client attributed to the applicant? ☐ Yes ☐ No
IF YES, EXPLAIN

4 EXPOSURE & RISK QUESTIONS — CONTRACTS, SERVICE LEVELS & PROJECTS

4-1 Does every managed client sign a master services agreement? ☐ Yes ☐ No
IF YES, EXPLAIN

4-2 Does the agreement cap the applicant's liability (e.g., to fees paid)? ☐ Yes ☐ No
IF YES, EXPLAIN

4-3 Does the agreement exclude consequential damages such as lost profits? ☐ Yes ☐ No
IF YES, EXPLAIN

4-4 Does the agreement state which security services are and aren't included? ☐ Yes ☐ No
IF YES, EXPLAIN

4-5 Are clients who decline recommended security controls asked to sign a written waiver? ☐ Yes ☐ No
IF YES, EXPLAIN

4-6 Are projects and migrations tested with a rollback plan before cutover? ☐ Yes ☐ No
IF YES, EXPLAIN

4-7 Has a client claimed a missed service level, failed project, or outage caused by the applicant? ☐ Yes ☐ No
IF YES, EXPLAIN

5 EXPOSURE & RISK QUESTIONS — SUBCONTRACTORS, DATA & STAFF

5-1 If yes to 2-3, do subcontractors carry technology E&O and cyber coverage? ☐ Yes ☐ No
IF YES, EXPLAIN

5-2 Are criminal background checks done on all technicians with client access? ☐ Yes ☐ No
IF YES, EXPLAIN

5-3 Does the applicant sign business associate agreements with healthcare clients? ☐ Yes ☐ No
IF YES, EXPLAIN

6 PAYROLL, SALES & REVENUE

TOTAL ANNUAL PAYROLL ($)	PROJECTED ANNUAL GROSS REVENUE ($)	RECURRING MANAGED-SERVICES REVENUE ($)

7 PRIOR INSURANCE & LOSS HISTORY

Attach currently valued loss runs for the last 5 years.

TECH E&O / CYBER CARRIER / LIMITS	RETROACTIVE DATE	GL CARRIER / LIMITS

7-1 Has any carrier declined, cancelled, or non-renewed coverage in the last 5 years? ☐ Yes ☐ No

IF YES, EXPLAIN

DATE OF LOSS	DESCRIPTION	TOTAL INCURRED ($)	OPEN / CLOSED

7-2 Is the applicant aware of any incident, complaint, or circumstance not yet resulting in a claim that could reasonably give rise to one? ☐ Yes ☐ No

IF YES, EXPLAIN

8 RISK MANAGEMENT

8-1 Is there a written incident response plan covering an attack that affects multiple clients? ☐ Yes ☐ No

IF YES, EXPLAIN

8-2 Is the applicant's security program assessed yearly by a third party (e.g., SOC 2)? ☐ Yes ☐ No

IF YES, EXPLAIN

9 SIGNATURE & FRAUD WARNING

The undersigned declares that the statements and answers given in this supplemental are true, complete and correct to the best of their knowledge, and that no material fact has been withheld or misstated. The applicant agrees that this supplemental, together with all ACORD applications and attachments, forms the basis of any submission to insurers and may be relied upon by them. Signing this supplemental does not bind coverage. This supplemental is an intake document prepared by Cory Washington & Co. LLC to support carrier submission; it does not itself provide coverage.

FRAUD NOTICE: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information, or conceals for the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties. (State-specific fraud warnings apply; see state amendatory notice.)

APPLICANT / AUTHORIZED SIGNATURE (TYPE FULL NAME)	TITLE	DATE

PRODUCER — CORY WASHINGTON & CO. LLC	PRODUCER SIGNATURE (TYPE FULL NAME)	DATE