

For managed security service providers, MDR and SOC providers, penetration testers, incident response firms, and security consultants. General IT managed service providers use CWCO-SUP-ITMSP. Complete with ACORD 125 and the carrier's technology E&O and cyber applications. Attach a sample master services agreement and statement of work, the service catalog, the applicant's own security controls summary, and five years of loss runs.

1 APPLICANT / BUSINESS INFORMATION

LEGAL BUSINESS NAME	DBA	FEIN	YEARS IN BUSINESS
BUSINESS ADDRESS	CITY / STATE / ZIP	WEBSITE	

Entity type:
☐ LLC ☐ Corporation ☐ Partnership ☐ Other

PRIMARY CONTACT / TITLE	PHONE	EMAIL

SECURITY CERTIFICATIONS HELD (SOC 2, ISO 27001, ETC.)	EMPLOYEES

2 OPERATIONS

Services offered (check all that apply):
☐ 24/7 SOC / MDR monitoring ☐ Managed firewall / EDR ☐ Penetration testing ☐ Incident response ☐ vCISO / compliance consulting
☐ Vulnerability scanning ☐ Security awareness training ☐ Reselling security software ☐ Backup and recovery

Clients:
 Active clients Endpoints monitored Largest client (% of revenue) Clients in health care or finance

Client industries (check all that apply):
☐ Health care ☐ Financial services ☐ Government ☐ Critical infrastructure ☐ Legal ☐ Retail ☐ Manufacturing

2-1 Does the applicant subcontract any monitoring or response work? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-2 Does the applicant have administrative access to clients' systems? ☐ Yes ☐ No
 IF YES, EXPLAIN

3 EXPOSURE & RISK QUESTIONS — DETECTION, RESPONSE & CLIENT CONTROLS

In 2025, Chubb's ACE sued an MDR provider to recover a ransomware payout, alleging it flagged the attack five days early but rated it only "moderate" and did not promptly warn the client. Missed alerts and controls a provider promised but did not run are the core claims against security firms.

3-1 Are alert severity levels and client notification times defined in writing for each client? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-2 Is every high or critical alert reviewed by a person within a set time? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-3 Are client notifications of alerts logged with time stamps? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-4 Does the applicant contain threats (isolate hosts, block accounts) without waiting for client approval? ☐ Yes ☐ No
 IF YES, EXPLAIN

3-5 Does each statement of work list which security controls the applicant is responsible for and which the client is? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-6 Are clients told in writing when they decline a recommended control such as MFA or backups? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-7 Does every penetration test have a signed authorization and scope letter? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-8 Does the applicant negotiate ransom payments for clients? ☐ Yes ☐ No
IF YES, EXPLAIN

4 EXPOSURE & RISK QUESTIONS — CONTRACTS & THE APPLICANT'S OWN SECURITY

A security provider with access to many clients is a single point of failure. Attacks through remote management tools have reached hundreds of downstream businesses at once.

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

4-2 Do agreements cap the applicant's liability? ☐ Yes ☐ No
IF NO, EXPLAIN

4-3 Do agreements require clients to carry their own cyber insurance? ☐ Yes ☐ No
IF NO, EXPLAIN

4-4 Do any agreements promise that clients will not be breached or guarantee detection? ☐ Yes ☐ No
IF YES, EXPLAIN

4-5 Is phishing-resistant MFA required for all access to client environments and management tools? ☐ Yes ☐ No
IF NO, EXPLAIN

4-6 Is access to remote management tools limited to approved users and devices? ☐ Yes ☐ No
IF NO, EXPLAIN

4-7 Is privileged access to client environments logged? ☐ Yes ☐ No
IF NO, EXPLAIN

4-8 Are the applicant's own backups kept offline or immutable? ☐ Yes ☐ No
IF NO, EXPLAIN

4-9 Are employees background-checked before getting client access? ☐ Yes ☐ No
IF NO, EXPLAIN

5 PAYROLL, SALES & REVENUE

ANNUAL REVENUE (\$)	MANAGED SERVICES REVENUE (\$)	INCIDENT RESPONSE / PEN TEST REVENUE (\$)	TOTAL ANNUAL PAYROLL (\$)

6 PRIOR INSURANCE & LOSS HISTORY

Attach currently valued loss runs for the last 5 years.

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

DATE OF CLAIM	CLIENT / DESCRIPTION	TOTAL INCURRED (\$)	OPEN / CLOSED

6-1 Has a client been breached or hit by ransomware while the applicant provided security services? ☐ Yes ☐ No
IF YES, EXPLAIN

6-2 Has a client or its insurer made a demand or claim against the applicant? ☐ Yes ☐ No
IF YES, EXPLAIN

6-3 Has the applicant itself had a security incident? ☐ Yes ☐ No
IF YES, EXPLAIN

6-4 Has any coverage been declined, cancelled, or non-renewed? ☐ Yes ☐ No
IF YES, EXPLAIN

6-5 Is the applicant aware of any incident or circumstance that could give rise to a claim?

☐ Yes ☐ No

IF YES, EXPLAIN

7 RISK MANAGEMENT & SAFETY

7-1 Are SOC procedures documented and reviewed after every major incident?

☐ Yes ☐ No

IF NO, EXPLAIN

7-2 Are contracts reviewed by counsel before signing?

☐ Yes ☐ No

IF NO, EXPLAIN

7-3 Does the applicant test its own incident response plan at least yearly?

☐ Yes ☐ No

IF NO, EXPLAIN

8 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, may be committing a fraudulent insurance act, which is a crime and may subject such person to criminal and civil penalties. State-specific fraud warnings appear on the insurer's application.

APPLICANT / AUTHORIZED SIGNATURE (TYPE FULL NAME)

TITLE

DATE

PRODUCER — CORY WASHINGTON & CO. LLC

PRODUCER SIGNATURE (TYPE FULL NAME)

DATE