SAMPLE BREAKDOWN - Based on real federal solicitation structures

NOTE: This sample demonstrates our analysis capabilities. We run this same process on your exact RFP.

Cybersecurity Operations
CMMC Compliance Support

Based on real federal solicitation structure - DoD Cybersecurity / Small Business

NAICS CODE	541519 - Other Computer Related Services
SET-ASIDE TYPE	Total Small Business Set-Aside (FAR 19.5)
CONTRACT TYPE	Firm Fixed Price
ESTIMATED VALUE	~$4.2M over 3-year base + 2 option years
TYPICAL SCOPE	SOC Operations + CMMC Level 2/3 Implementation
TYPICAL PAGE LIMIT	40 pages technical + management volumes

What this is

A complete breakdown of a DoD CMMC cybersecurity RFP - the compliance items most teams miss until it is too late to fix them.

What we did

We mapped every CMMC and DFARS 7012 requirement, structured all proposal volumes, and identified what separates winning DoD cyber bids.

What it means for you

CMMC proposals that miss compliance items are rejected before scoring. This tells you exactly what those items are before you submit.

WHAT'S IN THIS DOCUMENT

SECTION 1 - COMPLIANCE CHECKLIST

Review every item before proposal submission. Items marked with a checkbox are required compliance actions.

Registration & Eligibility

- [ ] SAM.gov registration active with CAGE code, NAICS 541519 listed as primary
- [ ] Size standard confirmed: 541519 = $30M average annual receipts for small business
- [ ] No active exclusions, debarments, or suspensions in SAM.gov
- [ ] DUNS/UEI active and matching SAM.gov registration

CMMC & Compliance Certifications

- [ ] CMMC Level 2 or 3 certification in place (or active C3PAO assessment underway with letter of engagement)
- [ ] SPRS score documented in SAM.gov (NIST SP 800-171 self-assessment score)
- [ ] System Security Plan (SSP) current and complete for all CUI-handling systems
- [ ] Plan of Action & Milestones (POA&M) current for any open NIST 800-171 control gaps
- [ ] CUI handling procedures documented and staff trained within the last 12 months
- [ ] DFARS 252.204-7012 Safeguarding clause compliance demonstrated with prior contracts

Technical Capabilities

- [ ] Security Operations Center (SOC) capability documented - 24/7 or defined coverage hours with escalation
- [ ] SIEM platform in use - name the specific platform (Splunk, Microsoft Sentinel, QRadar, etc.)
- [ ] Endpoint Detection & Response (EDR) deployed on all systems handling CUI
- [ ] Vulnerability scanning capability: frequency, tools, and remediation SLA documentation
- [ ] Incident response plan current, tested via tabletop or live exercise within 12 months
- [ ] DoD 8570/8140 certifications confirmed for all proposed security personnel

Personnel & Clearances

- [ ] Proposed ISSM holds active DoD IAM Level II or III certification (CISSP, CISM, or equivalent)
- [ ] SOC Lead holds active DoD IAM Level I-II certification (Security+, CySA+, or equivalent)
- [ ] Clearance status: Secret clearance for personnel accessing classified systems
- [ ] All personnel with CUI access have completed annual cybersecurity awareness training
- [ ] Background investigations current for all personnel on-site at DoD/DISA facilities

SECTION 2 - PROPOSAL OUTLINE & SECTION GUIDANCE

Each section below includes page allocations, what evaluators are looking for, and specific must-include elements.

VOLUME 1 - TECHNICAL APPROACH - PAGE LIMIT: 40 pages

1.0 Executive Summary - Mission Understanding [2 pages]

Evaluator Guidance:

DISA's mission is to provide, operate, and assure command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure. Your executive summary should demonstrate you understand the stakes - a security failure in a DISA-supported system can have national security implications. Lead with your CMMC status and SOC maturity, not generic cybersecurity language.

Must Include:

- Your CMMC certification level and date (or C3PAO engagement status)
- SOC maturity level and years of federal cybersecurity experience
- Your top 2-3 differentiators specific to DISA's environment
- Statement of understanding of DISA's mission and this contract's role

1.1 Cyber Operations - SOC Architecture & Detection/Response [10 pages]

Evaluator Guidance:

DISA evaluators will be technical. Generic SOC descriptions will not score well. Be specific about your SIEM platform, detection rules, alert triage process, and response playbooks. The key differentiator is demonstrating that your SOC can detect and respond to advanced persistent threats (APTs), not just commodity malware. If you have experience with specific threat actor TTPs relevant to DoD (nation-state actors targeting defense contractors), reference it.

Must Include:

- SOC architecture diagram with tool stack named (SIEM, SOAR, EDR, TIP, UEBA)
- Detection coverage: MITRE ATT&CK framework mapping of your detection rules
- Alert triage process: L1/L2/L3 analyst roles, escalation criteria, response times
- Playbooks for top 10 incident types relevant to DISA environment
- Threat intelligence integration: feeds, sources, enrichment process
- Metrics: MTTD (mean time to detect), MTTR (mean time to respond) from prior contracts
- Staffing model: analyst FTEs, shifts, geographic distribution, backup coverage

1.2 CMMC Level 2/3 Implementation - Gap Assessment & Roadmap [8 pages]

Evaluator Guidance:

Most small businesses competing for DoD cyber contracts are still struggling with CMMC compliance themselves. If you have already achieved CMMC Level 2 or 3 certification, you are in a small group of credible competitors. Lead with your own certification, then explain how you will help the Government and its contractor ecosystem achieve compliance. Show your gap assessment methodology - the structured process you use to evaluate a client against all 110 NIST 800-171 practices (or 130 for Level 3 CMMC).

Must Include:

- Your own CMMC certification level and assessment date
- Gap assessment methodology: how you evaluate all 110/130 practices
- Tooling: what platform you use for SSP development and POA&M tracking
- Remediation prioritization approach: how you sequence fixes to maximize SPRS score improvement
- Timeline estimates: typical duration from gap assessment to C3PAO assessment readiness
- Common failure modes you have seen and how you address them

1.3 NIST 800-171 / 800-53 Controls - Implementation & Continuous Monitoring [6 pages]

Evaluator Guidance:

Continuous monitoring is the difference between passing a CMMC assessment and maintaining compliance over the contract period. DISA will want to see a mature continuous monitoring program - not just 'we scan quarterly.' Show your ConMon methodology including the monitoring cadence for each control family, your process for detecting and responding to control deviations, and how you track and report compliance posture to the Government.

Must Include:

- Control family coverage: which 800-171 families are highest risk and how you prioritize them
- Continuous monitoring cadence: daily automated scans, monthly reviews, annual assessments
- Control deviation response: how you detect a control has failed and your remediation SLA
- Compliance reporting: dashboard or report format you provide to Government stakeholders
- POA&M management: how you track open items, update completion dates, and close findings

1.4 Incident Response & Recovery [6 pages]

Evaluator Guidance:

DFARS 252.204-7012 requires reporting cyber incidents to DoD within 72 hours (and preserving images for 90 days). Your incident response plan must explicitly address this requirement. DISA will want to see that you have a mature IR capability that goes beyond detecting incidents - you must have demonstrated ability to contain, eradicate, recover, and report within the required timeframes.

Must Include:

- Incident classification: severity levels and corresponding response time commitments
- DFARS 7012 reporting procedure: who reports, to what system (DIBNet), within what timeframe
- Containment procedures: network isolation, account lockdown, evidence preservation
- Evidence collection and chain of custody for potential law enforcement involvement
- Recovery procedures: system restoration, verification, return to operations
- Post-incident review: lessons learned process and after-action report format
- Reference a real incident (de-identified) demonstrating your IR capability

1.5 Supply Chain Risk Management (SCRM) [4 pages]

Evaluator Guidance:

DISA and DoD broadly are deeply concerned about supply chain risk after high-profile incidents (SolarWinds, Kaseya, etc.). Show that you have a mature software and hardware supply chain vetting process - not just a list of approved vendors, but an active process for evaluating new suppliers, monitoring for compromise indicators, and responding to supply chain incidents.

Must Include:

- Vendor vetting process for all software and hardware in the solution stack
- Prohibited technology list compliance (Section 889, FAR 52.204-25)
- Software bill of materials (SBOM) capability and process
- Monitoring for supply chain compromise indicators (CVE tracking, vendor security advisories)
- Incident response for supply chain compromise: how you respond to a compromised vendor

VOLUME 2 - MANAGEMENT & PAST PERFORMANCE - PAGE LIMIT: No stated limit (typical: 25 pages)

2.0 Program Management Approach [5 pages]

Evaluator Guidance:

DISA wants predictable, low-drama contract management. Show a governance structure with clear accountability, a risk management process, and a mechanism for rapidly communicating security incidents or compliance issues to the CO and ACOR.

Must Include:

- Org chart with named key personnel and their reporting relationships
- Communication plan: status reporting cadence, escalation paths, emergency contact protocol
- Risk management methodology: how you identify, track, and mitigate contract risks
- Quality assurance: how you measure your own performance against KPIs

2.1 Key Personnel [6 pages + resumes as attachments]

Evaluator Guidance:

ISSM qualifications are scrutinized closely on DISA contracts. Your ISSM must hold a DoD 8570 IAM Level II or III certification and ideally have prior DISA or DCSA coordination experience. The SOC Lead needs demonstrated experience managing analysts in a 24/7 operational environment. Name people who will actually work the contract.

Must Include:

- ISSM: DoD 8570 IAM Level II/III cert, active Secret clearance, prior federal cyber experience
- SOC Lead: 5+ years SOC management, relevant tool certifications, federal environment experience
- Compliance Manager: CMMC experience, NIST 800-171 implementation track record
- Availability commitment for each key person

2.2 Past Performance [5 pages]

Evaluator Guidance:

Two DoD cybersecurity contracts with verifiable CPARS ratings will significantly differentiate you. References should demonstrate SOC operations at comparable scale, CMMC/NIST 800-171 implementation experience, and incident response for DoD or cleared defense contractor environments.

Must Include:

- 2+ DoD or cleared defense contractor cybersecurity references
- CPARS ratings or equivalent performance documentation
- Specific metrics: incidents detected/responded to, CMMC clients certified, SPRS score improvements
- Reference contact information with active phone and email

SECTION 3 - KEY WIN THEMES & TACTICAL GUIDANCE

These are the 5 most important differentiators for this contract type. Each theme includes tactical guidance on how to execute it in your proposal.

WIN THEME 1: CMMC Readiness Is Your Most Powerful Differentiator

Most small GovCon IT firms are still unprepared for CMMC Level 2. If you have an active C3PAO assessment or prior Level 2 certification, lead with it on every page.

Tactical Guidance:

The CMMC ecosystem is still maturing. As of 2026, a significant percentage of small businesses competing for DoD IT contracts have not yet achieved a formal CMMC certification - they are still operating under self-attestation. If you have a third-party CMMC Level 2 assessment in progress or completed, you are in a small minority of the competitive field.

This is not just a compliance checkbox - it is a business development asset. In your executive summary, state your CMMC status in the first paragraph. In your technical approach, explain what you learned from your own C3PAO assessment and how that experience helps you guide clients through the same process.

If you are still working toward CMMC certification, be transparent about your timeline and current SPRS score. Evaluators can check your SPRS score in SAM.gov. If your score is low, explain the gap and your remediation plan. If it is high (90+), mention it.

Do not claim CMMC compliance you do not have. DISA will verify, and misrepresentation in a federal proposal is a serious issue.

WIN THEME 2: Dedicated 24/7 SOC vs. Best-Effort Coverage

Many small businesses propose a SOC but deliver 9-5 coverage with on-call. If your team can demonstrate true 24/7 continuous monitoring with <15 minute detection-to-alert SLA, quantify it.

Tactical Guidance:

The difference between a real SOC and a marketing claim is shift coverage. A true 24/7 SOC has analysts on keyboard at 2am on a Sunday morning who can respond to an alert, not an on-call engineer who gets paged and logs in 45 minutes later.

For DISA, the key metric is MTTD and MTTR from your SIEM console. If your SIEM data shows a 3-year average of 8-minute MTTD and 23-minute MTTR on your previous federal SOC contract, put that number in your proposal. Evaluators are comparing you to competitors who will write 'we detect threats quickly' - you are the one with data.

For small businesses, a fully staffed 24/7 SOC may require partnerships or co-managed SOC arrangements. If you use a co-managed model, be transparent about it - explain the workflow, the hand-off procedures, and how you maintain accountability for incidents that occur during co-managed hours.

The specific metric that appears most frequently in DISA cybersecurity RFPs: <15 minutes from initial SIEM alert to analyst triage decision. If you can demonstrate this from historical data, it is a direct evaluation discriminator.

WIN THEME 3: DFARS 7012 Implementation Track Record

Prior experience implementing and auditing DFARS 252.204-7012 for subcontractors in a prime/sub relationship is rare and explicitly valued.

Tactical Guidance:

DFARS 252.204-7012 requires that any contractor handling Covered Defense Information (CDI) or operating on DoD networks must implement the NIST SP 800-171 security requirements and report cyber incidents to DoD within 72 hours. This obligation flows down to all subcontractors.

The challenge for most prime contractors: they sign DFARS 7012 compliance commitments on behalf of their supply chain, but they have no visibility into whether their subs are actually compliant. If you have built and executed a program for vetting and monitoring subcontractor DFARS 7012 compliance - reviewing their SSPs, tracking their SPRS scores, conducting spot assessments - that is a rare capability.

Describe your process in the technical proposal: how you onboard a new subcontractor, what documentation you require (SSP,

POA&M, incident response plan), how you track their ongoing compliance, and what you do when a sub is found to be non-compliant.

If you have a case study - even de-identified - of identifying a non-compliant subcontractor and remediating the gap, that is a compelling past performance narrative.

WIN THEME 4: Named ISSM With Verifiable Credentials

A named ISSM with active Secret/TS clearance, DoD 8570 IAM Level II/III certification, and prior DISA/DCSA coordination experience can single-handedly elevate your technical score.

Tactical Guidance:

DISA proposals are evaluated by technical personnel who know what good ISSM credentials look like. A generic 'we will provide a qualified ISSM' response will score poorly. A named individual with a CISSP, an active TS/SCI clearance, 8 years of federal cybersecurity experience, and two prior DISA A&A packages to their name is a proposal differentiator.

Beyond credentials, prior DISA coordination experience is specifically valuable because DISA has unique processes (eMASS for ATO documentation, specific STIG requirements, DISA STIGs vs. CIS benchmarks, ACAS for vulnerability scanning) that take time to learn. Someone who has navigated a DISA ATO before can credibly promise a smoother compliance process.

If your ISSM has a relationship with a specific DISA FSIO or cyber team from prior engagements, that institutional knowledge has real value - mention it (without promising inappropriate influence).

For this proposal, the ISSM should be named in Section 2.1 with a full resume as an attachment. Do not just describe the role requirements - name the person and tie their specific experience to the specific challenges of this contract.

WIN THEME 5: Story-Based Incident Response Evidence

Reference a real incident (de-identified) where your team detected, contained, and reported a cyber incident. Narrative-based past performance beats template IR plans.

Tactical Guidance:

Every proposal will include an incident response plan formatted around the NIST IR lifecycle (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned). What separates winning proposals is evidence that you have actually executed this process under pressure, not just that you have documented it.

Include a de-identified incident narrative in your past performance section. Structure it around the key facts that matter to DISA evaluators: what was the initial indicator of compromise, how long between first indicator and analyst triage (MTTD), what containment action was taken and how quickly, whether the incident met the DFARS 7012 72-hour reporting threshold and how you handled that reporting, and what was the business impact (or lack thereof) due to your response.

A specific example: 'In Q3 2024, our SOC detected anomalous outbound traffic on a client's CUI enclave at 02:47 on a Saturday morning. Analyst triage was completed within 11 minutes. The affected endpoint was isolated within 18 minutes of initial detection. DFARS 7012 reporting was initiated to DIBNet within 6 hours. Post-incident forensics confirmed no CUI exfiltration had occurred. The client received a passing CMMC assessment 60 days later.'

That narrative is more convincing than any IR plan template.