AIS Network CMMC Scoping Questionnaire: Helping You Prepare for Compliance in 2025

General Business Information

- What is your organization's primary line of business, and how does it interact with the Department of Defense (DoD)?
- What is your company's size (number of employees, locations, etc.)?
- What types of sensitive data (*e.g.*, Controlled Unclassified Information - CUI, Federal Contract Information - FCI) does your organization handle?
- What contracts or projects require CMMC compliance, and what CMMC level is required for those contracts?

CMMC-Specific Needs

- What CMMC maturity level do you need to achieve (Level 1 through Level 3)?
- What is the deadline for CMMC certification, based on contract requirements?
- Are you seeking guidance for achieving full CMMC compliance or just a gap analysis?

Current Cybersecurity Posture

- Do you have an existing cybersecurity program or framework in place (*e.g.,* NIST 800-171, ISO 27001)?
- Have you conducted any cybersecurity assessments (self-assessments, third-party audits)? If so, can you share the results?
- What cybersecurity tools, technologies, or solutions are you currently using (*e.g.*, firewalls, antivirus, SIEM, encryption)?
- Do you currently have policies and procedures in place for data security, access control, incident response, and risk management?

Infrastructure and IT Systems

- What type of IT infrastructure is in place (cloud-based, on-premises, hybrid)?
- How many endpoints, servers, and network devices need to be included in the CMMC scope?
- Do you utilize any third-party service providers (e.g., cloud services, managed IT providers), and if so, what role do they play in your IT environment?
- Are there any special technologies or systems (e.g., Industrial Control Systems) that require tailored security measures?

Data Flow and Management

- Can you describe how CUI or FCI is transmitted, stored, and processed within your organization?
- How is access to sensitive data controlled and monitored?
- Do you have any mechanisms in place to track and audit data flows involving CUI or FCI?

P.O. Box 2082, Ashland, VA 23005 • Phone 888.579.AISN (2476)
919 E. Main St., Suite 1000, Richmond, VA 23219 • Phone 847.202.1400 • Fax 847.202.4460
www.aisn.net

Human Resources and Training

- What level of cybersecurity awareness and training do employees currently receive?
- How are privileged users (*e.g.,* IT administrators) trained and managed with respect to security practices?
- Is there a designated cybersecurity officer or security team responsible for compliance?

Incident Response and Risk Management

- Do you have an incident response plan in place? If so, has it been tested or used recently?
- Have you experienced any security incidents or data breaches in the past? If so, how were they handled?
- How do you assess and manage cybersecurity risks?

Compliance and Governance

- Are you subject to any other regulatory requirements or frameworks (*e.g.,* HIPAA, GDPR, DFARS)?
- How do you document and manage compliance efforts? Are they centrally tracked or distributed among teams?
- Do you have any third-party or internal audit programs in place to ensure ongoing compliance?

Budget and Timeline

- What is your budget for achieving CMMC compliance?
- Are there specific timeframes or project milestones that must be met (*e.g.,* pre-audit, gap analysis, remediation)?
- Are you looking for a phased approach to CMMC compliance, or do you plan to achieve compliance all at once?

Expectations and Deliverables

- What are your expectations for this project? Are you looking for specific deliverables such as policies, tools, or training programs?
- Do you have a preference for internal staff training, process improvement, or simply the completion of technical remediation efforts?
- Will you need ongoing support after CMMC certification, such as continuous monitoring, compliance maintenance, or periodic assessments?

Party Dependencies

- Are there any key vendors or partners who will be involved in the CMMC compliance process?
- How do you currently manage third-party risk, especially when it comes to handling sensitive data?