CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)
LEVEL 1 READINESS ASSESSMENT QUESTIONNAIRE

PILIERO MAZZA

This CMMC Level 1 readiness questionnaire is designed to start the process for determining the cybersecurity requirements that may be applicable to your company and to get a general sense of your current cybersecurity practices compared to the requirements for CMMC Level 1. If you are not sure of the answer to a particular question, or if you believe further explanation is necessary to give a complete understanding of your response, please provide supplemental responses in the space designated for supplemental responses starting on page 5.

Section 1 – Background Information

Your Name	
Company Name	

	Yes	No
1. Do you have prime contracts with the U.S. Department of Defense "DoD")?	☐	☐
2. Do you have subcontracts under DoD prime contracts?	☐	☐

3. Do any of your prime contracts or subcontracts contain any of the following FAR/DFARS clauses?	Yes	No
52.204-21, Basic Safeguarding of Covered Contractor Information Systems	☐	☐
252.204-7008, Compliance with Safeguarding Covered Defense Information Controls	☐	☐
252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	☐	☐
252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting	☐	☐
252.239-7009, Representation of Use of Cloud Computing	☐	☐
252.239-7010, Cloud Computing Services	☐	☐

	Yes	No
4. Do you operate an information technology ("IT") system on behalf of the U.S. Government? If you answer no, we assume this means your IT system is for your company. Please explain further as needed in the supplemental section.	☐	☐
5. Do you use cloud computing to provide IT services in the performance of federal contracts?	☐	☐

	Yes	No
6. Do you use your own internal cloud solution to host and/or process data? If you use a cloud service provider, please answer no and provide a supplemental response to provide an explanation including the name of the provider you use.	☐	☐
7. Do you have controlled technical information or other information described or labeled as "Controlled Unclassified Information" or "CUI" in your internal IT system? If you are not sure, provide a supplemental response to explain.	☐	☐
8. Do you have a system security plan or other written guide addressing your internal security practices and procedures for your IT system?	☐	☐
9. Have you registered in DIBNET (https://dibnet.dod.mil)?	☐	☐
10. Do you have policies and procedures addressing cybersecurity in your employee handbook?	☐	☐

Section 2 – CMMC Level 1 Practices

	Yes	No
11. Do you limit access to your IT system by authorized users, processes acting on behalf of authorized users, or devices (including other information systems)?	☐	☐
Examples of limited access include giving a username and password to every employee who uses a company computer. Another example is password protecting your company Wi-Fi to keep unauthorized devices from accessing your network.		

	Yes	No
12. Do you limit IT system access to the types of transactions and functions that authorized users are permitted to execute?	☐	☐
For example, are only certain people in your company able to access certain parts of your network, such as only your HR or finance department personnel have access to the portion of your network that houses payroll, personnel, and other employee or financial information?		

	Yes	No
13. Do you verify and control/limit connections to and use of external information systems?	☐	☐
For example, do you prevent employees from using their personal devices to access your network and any federal contract information ("FCI") that may be on your network? Is your network only accessible on work devices? Do you allow only authorized employees to connect to outside systems, particularly for the purposes of installing software that can potentially be run by outside users or systems?		

	Yes	No
14. Is controlled information posted or processed on publicly accessible information systems?	☐	☐

For example, do you review all the marketing you release on your website (and in general) to make sure you have not included any FCI?

	Yes	No
15. Do you identify information system users, processes acting on behalf of users, or devices?	☐	☐
For example, do you require employees to enter their username and password to access your systems, and associate the "level of access" allowed for each employee with their username and password? In other words, when Joe from the shipping department logs in, is he only able to access the part of your network necessary for his job functions, or can he access anything in the network he wants?		

	Yes	No
16. Do you authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems?	☐	☐
For example, you do not use "default" usernames and passwords (e.g., username: "admin" password: "password"), nor a username and password that are the same. Instead, you use unique usernames and hard-to-guess passwords.		

	Yes	No
17. Do you sanitize or destroy information system media containing FCI before disposal or release for reuse?	☐	☐
For example, you happen to come across some old CDs that contain FCI. You shred the CDs instead of simply throwing them in the trash.		

	Yes	No
18. Do you limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals?	☐	☐
For example, you have a server that stores FCI in your office. You keep that server in a locked area that the general public cannot access.		

	Yes	No
19. Do you escort visitors and monitor visitor activity?	☐	☐
For example, company personnel are trained for if the see a visitor wandering your hallways, the visitor would be escorted back to the reception area to get a visitor badge and the incident would be reported to the relevant security personnel in your company.		

	Yes	No
20. Do you maintain audit logs of physical access?	☐	☐
For example, visitors and/or employees are required to sign in and out at your reception desk.		

	Yes	No
21. Do you control and manage physical access devices?	☐	☐
"Physical access devices" are any devices serving the function of a lock or key (key cards, fobs, combination locks, card readers). So, for example, when an individual stops working for your company for any reason, you immediately retrieve all of their "physical access devices."		

	Yes	No
22. Do you monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems?	☐	☐
For example, you purchase a router with a built-in, configurable firewall. You route all internet connections in your company through that router. You configure the firewall to block sites that are known to spread malware.		

	Yes	No
23. Do you implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks?	☐	☐
For example, you have multiple servers. You want to allow the public to download certain information from your website. You ensure that the downloadable information is hosted on a different server than your servers that host FCI.		

	Yes	No
24. Do you identify, report, and correct information and information system flaws in a timely manner?	☐	☐
For example, you enable all security updates for all operating systems and applications you use.		

	Yes	No
25. Do you provide protection from malicious code at appropriate locations within organizational information systems?	☐	☐
For example, you purchase and install anti-malware software on all company computers.		

	Yes	No
26. Do you update malicious code protection mechanisms when new releases are available?	☐	☐
For example, you enable automatic updates for your anti-malware software.		

	Yes	No
27. Do you perform periodic scans of your information system and real-time scans of files from external sources as files are downloaded, opened, or executed?	☐	☐
For example, you enable your anti-malware software's periodic system-wide scans.		

Section 3 – Supplemental Responses

Question #____:
Question #____:
Question #____:
Question #____:
Question #____:
Question #____:
Question #____:
Question #____: