# Cybersecurity Maturity Model Pre-Certification

Service Description

1. Description of Service: This document ("Service Description") describes the CyberSecurity Maturity Model Certification ("CMMC" or "Service") offered by BlueVoyant to its customers ("Customer", "Client", or "you") pursuant to a service order explicitly authorizing the purchase and sale of the Service. For the avoidance of doubt, the terms of BlueVoyant Master Services Agreement ("MSA") available at https://www.bluevoyant.com/bvmssterms shall govern in the absence of a master services agreement signed by BlueVoyant superseding those terms.

2. Service Overview: The CMMC framework for assuring the security of suppliers to the DoD was finalized in January 2020. While CMMC is new, the BlueVoyant Proactive Services team has extensive experience providing similar assessments including NIST 800-171 assessments and our proprietary Cybersecurity Maturity Assessment (CMA). Our team now provides proactive CMMC pre-assessments to include a detailed comparison of the current state of your cybersecurity posture and maturity against the CMMC framework controls associated with the maturity level you wish to achieve. While the final stages of certifying assessors have not been completed by the DoD, Clients that can show that required controls are in place will be able to fast track through the final step of the assessment, saving time and ensuring that there are no gaps in eligibility for future contract opportunities.

3. Execution Phases: Execution phases ("Execution Phase") consists of three phases: **Preparation, Evaluation,** and **Reporting**. The execution phases begin once the signed Service Order is received and ends with the acceptance of the associated deliverables. The execution phase is dependent on a number of factors, such as the number of stakeholder interviews, the complexity of the Client's network, Client requirements, and the ability of Client to provide BlueVoyant with the requested information within a mutually agreed-upon timeframe.

    3.1. Preparation Phase: The BlueVoyant team begins the preparation process by working with you to determine the appropriate maturity level for your organization. Once there is agreement on the level that will be pursued, our team will confirm with key stakeholders the required access to information, personnel, policies, procedures, and technology in order to perform the evaluation. Our team will then walk the client through the methods that will be used for the evaluation process and review expected outcomes.

3.2. Evaluation Phase: The team will use information and access to systems provided by the Client to assess the organization's security posture against the desired level of maturity within the CMMC framework. During this phase we may need to interview key staff members and will do so as efficiently as possible, being mindful of their time. The primary focus during this phase will be to assess your technology and processes against the required controls and begin to create a report on your exposure points specifically related to those controls.

`

3.3. Reporting Phase: In this final phase, we will finalize a report that will include a checklist of all of the required controls that are in place and a list of controls that have not been achieved. For each missing control, we use our extensive experience with security maturity assessments to provide suggested methods for achieving compliance that takes into account your unique risk profile, budget, resources, and policies. These recommendations will help you understand the right capabilities and organizational adjustments to invest in, rather than blindly raising individual maturity levels.

4. Deliverables

4.1. CMMC Pre-Certification Evaluation Report: The team will deliver a full report against the required controls with clear guidance provided on alternative methods that may be taken to achieve compliance with each control.

4.2. Roadmap to Certification: At the completion of the assessment we will provide a PowerPoint document that outlines all recommended remediation steps along with an expected timeline and recommended prioritization of steps to take in order to fast track and streamline your path to full compliance.

5. Client Responsibilities

5.1. Stakeholder Commitment: An essential key to success during a CMA is the commitment from the key stakeholders and their staff members. It is necessary to set aside time for the BlueVoyant team to conduct interviews with team members. We typically set aside 30-min to an hour for each of the evaluation areas understanding that one staff member may cover multiple areas.

5.2. Program Documentation: Timely access to existing cybersecurity policies and information regarding processes and procedures is critical to the effective and efficient completion of our evaluation process. The BlueVoyant team will need access to program documentation related to each of the functional areas and will provide ShareFile access for documents to be uploaded and reviewed.

5.3. Program Roadmap and Project Charter: As part of the Planning phase the BlueVoyant team will need access to any current or draft program roadmaps or project charters. BlueVoyant will provide ShareFile access for documents to be uploaded and reviewed.