Cybersecurity Maturity Assessment

Service Description

1. Description of Service: This document ("Service Description") describes the CyberSecurity MaturityAssessment ("CMA" 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: BlueVoyant we will assess the current state of your cybersecurity posture and maturity by comparing your current state against the Industry Standard framework (NIST, NCUA, FFIEC, NYDFS) and best practices. After evaluating your technology and interviewing your key staff, we will provide a report on your exposure points. Our report will include counsel on your unique challenges and will outline tailored improvements you should employ. These recommendations will help you to plan using your unique risk profile, budget, resources, policies, and compliance needs

3. Execution Phases: Execution phases ("Execution Phase") consists of **three phases**: **Understand**, **Evaluate**, and **Plan**. 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. <u>Understand Phase</u>: The objective of this phase is to confirm the overall approach and methodology before beginning a rapid assessment of the cybersecurity program. Two critical elements for an accurate, timely, and complete understanding of the current cybersecurity program across our considerations areas are the ability to gather information about the program from key stakeholders, and access to cybersecurity-related policies and procedures. Both critical dependencies will be addressed during the initiation of the project.

3.2. <u>Evaluate Phase</u>: The objective is to cultivate a shared understanding of currently implemented cybersecurity controls across the BlueVoyant assessment Framework. The team will utilize provided documentation and information gleaned from key stakeholder interviews to rapidly develop an understanding of your current cybersecurity state across each function, category, and sub-category. This approach will assign a maturity rating to each sub-category, which our observations detailed as justifications and recommendations for enhancing maturity based on observed best practices.

`

3.3. <u>Planning Phase</u>: In this final phase, we will group and prioritize individual recommendations by Function to enable business operations and buy down leading risks. These prioritized 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. Program Assessment: The team will deliver a PowerPoint document that will detail the team's evaluation process and scoring in all applicable functional areas.

4.2. Prioritized Program Enhancements: A PowerPoint document that outlines any recommended enhancements or improvements the team recommends.

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. It is also understood that based on the maturity of the organization that a full-length interview may not be required for each functional area.

5.2. Program Documentation: A foundational aspect of every Cybersecurity program is the processes and procedures that guide the program. The BlueVoyant team will need access to program documentation related to each of the functional areas. BlueVoyant 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.