	Georgia Technology Authority	
Title:	**Cybersecurity Capability Maturity Model Standard**	
PSG Number:	SS-20-001	
Issue Date:	TBD	**Effective Date:** TBD
Synopsis:	Establish an enterprise cybersecurity maturity model.	

PURPOSE

An Enterprise Cybersecurity Maturity Model provides a structure for the State of Georgia (Executive Agencies) to baseline current capabilities in cybersecurity while establishing a foundation for consistent evaluation. By implementing a cybersecurity maturity model, state agencies will not only have a framework for measuring the maturity of their cybersecurity program, but also a guidance on how to reach the next level as the agency maturity impacts cybersecurity premiums.

SCOPE and AUTHORITY

Information Technology Policies, Standards and Guidelines (PM-04-001) [or add: Enterprise Information Security Charter (PS-08-005)]

The Governor's Executive Order of March 2008 and O.C.G.A. 50-25-4(8), (13) & 50-25-7.10

STANDARD

The Georgia Cybersecurity Capability Maturity Model is a tool that agencies shall use to develop, assess and refine the State's Cybersecurity Program. The maturity model will be used annually to evaluate, rate and score each agency's maturity level as it relates to the Center for Internet Security (CIS) 20 Critical Security Controls. Agency Cyber Risk Scores will be determined by the State Technology Annual Report Register (STARR) Cybersecurity questionnaire which shall be annually completed by each Agency. This approach allows for the prioritization and consideration of control effectiveness as

demonstrated by the CIS Controls, in business and IT areas across the State. The information received within each agency's STARR submission has a direct financial impact on the State as an enterprise through cybersecurity insurance premiums and deductibles. Agency's that fail to complete the required STARR questionnaire may experience higher premiums as it will be assumed that the agency operates at a maturity level 0.

MATURITY LEVEL DETAILS

A maturity level is a well-defined evolutionary plateau toward achieving a mature cyber capability process. Each maturity level provides a layer in the foundation for continuous process improvement.

Maturity levels consist of a predefined set of process areas. The maturity levels are measured by the achievement of the specific and generic goals (CIS 20 Critical Controls) that apply to each predefined set of process areas. The following sections describe the characteristics of each maturity level in detail.

Maturity Level 1 (Initial): Processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment. Success in these organizations depend on the competence and heroics of the people in the organization and not on the use of proven processes.

Maturity Level 2 (Repeatable): At maturity level 2, an organization has achieved all the specific and generic goals of the maturity level 2 process areas. In other words, the projects of the organization have ensured that requirements are managed and that processes are planned, performed, measured, and controlled.

Maturity Level 3 (Defined): At maturity level 3, an organization has achieved all the specific and generic goals of the process areas assigned

to maturity levels 2 and 3. At maturity level 3, processes are well characterized and understood, and are described in standards, procedures, tools, and methods.

Maturity Level 4 (Quantitatively Managed): At maturity level 4, an organization has achieved all the **specific goals** of the process areas assigned to maturity levels 2, 3, and 4 and the **generic goals** assigned to maturity levels 2 and 3.

Maturity Level 5 (Optimizing): At maturity level 5, an organization has achieved all the **specific goals** of the process areas assigned to maturity levels 2, 3, 4, and 5 and the **generic goals** assigned to maturity levels 2 and 3.

Cyber Insurance Risk Tiers: Cyber Insurance Risk Tiers are risk scores based on each agency's maturity. The scores ranging from 1.0 - 5.0, directly impacts the cyber insurance billing model for each agency. All agencies shall achieve Level II (Risk Score 3.0) by June 2022.

Maturity Levels	Cyber Insurance Tiers
Level V- CIS Controls 1-20 (optimized	Risk Score: 1.0
Level IV- CIS Controls 1-19 (Managed)	Risk Score: 1.5
Level III- CIS Controls 1-19 (Defined)	Risk Score: 2.0
Level II- CIS Controls 1-6, 10, 17 (Repeatable)	Risk Score: 3.0*
Level I- CIS Controls 1-6, 10, 17 (Initial/Informal)	Risk Score: 4.0
Level 0- No processes	Risk Score: 5.0

* June 2022 Goal for all agencies.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES
Independent Security Assessments (SS-08-042)