Modernizing Maryland's Security Standards: From Legacy Manual to Policy Suite

Background and Summary:

The transition from the legacy Maryland IT Security Manual v1.2 to the Maryland Cybersecurity & Privacy Policy Suite represents a fundamental shift in the State's cybersecurity posture. This multi-tiered governance framework replaces the previous manual with an agile, Zero Trust Architecture (ZTA) that prioritizes data-centric security and continuous verification.

The Suite is organized into a clear hierarchy to ensure policy remains constant while technical standards evolve with the threat landscape:

- **100-Series (Governance):** High-level mandates that establish "who" is in charge and "what" the overarching goals are.
- **200-Series (Functional):** Policies aligned with the NIST Cybersecurity Framework (CSF) 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.
- **300-Series (Standards):** Granular, technical requirements geared toward IT staff (e.g., specific password lengths, encryption protocols).
- **400-Series (Procedures and Guidelines):** Step-by-step actions required to implement policies and standards. These provide practical, detailed instructions on the specific mechanisms used to enforce security requirements across the enterprise.
- **Emergency Directives Mandatory:** Short-term instructions issued to address immediate cybersecurity threats or urgent vulnerabilities. These directives require prompt action to protect State systems and assets during a specific, time-sensitive emergency.
- **Binding Operational Directives:** Mandatory, long-term instructions designed to safeguard Maryland information systems. These establish uniform practices to mitigate operational risk and remain in effect for all identified State units until officially modified or revoked.

Benefits of the New Policy Suite

The transition to the Maryland Cybersecurity & Privacy Policy Suite introduces several critical improvements to the State's security posture as outlined below:

- **Primary Philosophy:** The State is shifting from a perimeter-based, "trust but verify" approach to a Zero Trust Architecture that assumes the network is already compromised. This "never trust, always verify" mindset moves defense to the asset and user level, significantly limiting the lateral movement of attackers.

- **Framework Alignment:** The new suite modernizes controls by aligning with NIST CSF 2.0 (Functions) and NIST 800-53 Rev 5 (Standards), replacing the legacy alignment with NIST 800-53 Rev 4. This update incorporates privacy-centric engineering and Supply Chain Risk Management (C-SCRM).
- **Document Structure:** The previous monolithic 200+ page manual has been replaced with a Modular Hierarchy. This tiered structure enables the State to perform rapid updates to specific technical standards without requiring full revisions to the entire governance framework.

Stakeholder Engagement

- The development of the Policy Suite was a cross-functional effort involving several key oversight and operational bodies.
- Primary stakeholders included the Maryland Cybersecurity Coordinating Council (MCCC) GRC Working Group, the Maryland Local Cybersecurity Collaborative (MLCC), as well as additional agency CISOs, security teams, and operational Subject Matter Experts.
- Internal DoIT participation was also significant, incorporating perspectives from Information Security Officers, and Data, Infrastructure, and Communications teams.

Targeted Training Improvements

The new Awareness & Training Standard (MD-STD-302-AT-01) replaces annual "check-the-box" exercises with a more sophisticated approach:

- **Role-Based Training:** Mandated specialized training for "privileged users" (admins) and senior executives.
- **15-Day Onboarding:** New employees must complete security training within 15 days of hire, prior to gaining full access to sensitive data.
- **Continuous Learning:** Monthly, bite-sized modules addressing modern threats like AI-driven deepfakes and social engineering.

Key Technical Improvements in the Maryland Cybersecurity & Privacy Policy Suite

- **Authentication:** Standardizes a minimum length of 15 characters and eliminates periodic resets unless compromise is suspected. Following NIST 800-63B, these passphrases are more resistant to brute-force attacks and prevent the use of weak, pattern-based passwords.
- **Incident Response Velocity:** Mandates a one (1) hour notification window to the MD-SOC from the moment of discovery. This high-velocity reporting ensures the Core Cyber Response Team (CCRT) can contain threats before they escalate.

- **Data Classification & Integrity:** Integrates the "High-Water Mark" principle to automatically categorize system security based on the highest data level handled (including a 4th "Restricted" level). This ensures systems touching data like Federal Tax Information (FTI) inherit the most rigorous controls.
- **Proactive Vulnerability Management:** Establishes a formal reporting portal for ethical researchers and mandates rigorous scanning—weekly for standard systems and continuous for High-Value Systems—while enforcing a 15-day remediation window for Critical vulnerabilities.