House Government, Labor, and Elections Committee

January 27, 2026

AGENDA

01 Introductions + Priorities

02 Maryland AI

03 Maryland Digital Service

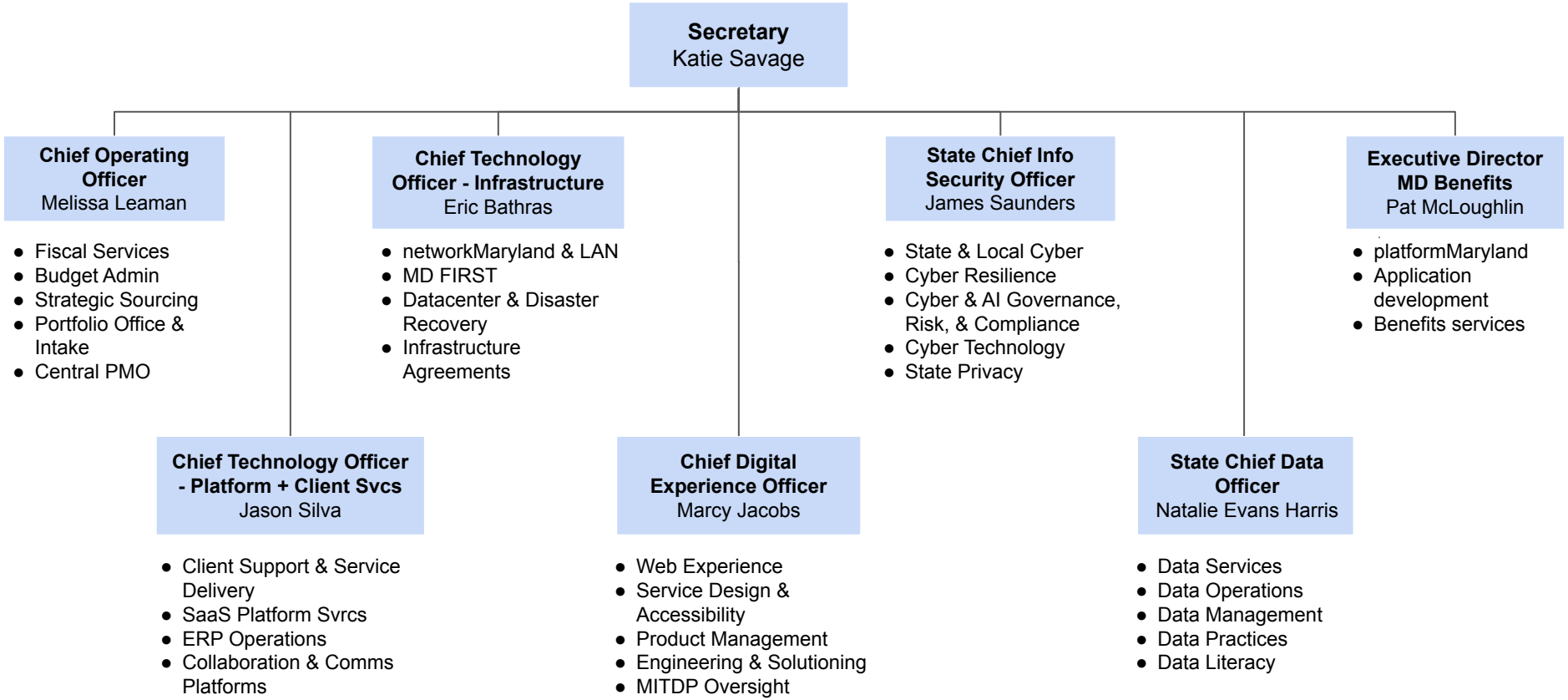
04 Office of Security Management

Introductions, Priorities, & Wins

Katie Savage
Secretary

Marcy Jacobs
Deputy Secretary
Chief Digital
Experience Officer

James Saunders
Chief Information
Security Officer


Secretary
Katie Savage
Chief Operating Officer
Melissa Leaman
Fiscal Services
Budget Admin
Strategic Sourcing
Portfolio Office & Intake
Central PMO
Chief Technology Officer - Infrastructure
Eric Bathras
networkMaryland & LAN
MD FIRST
Datacenter & Disaster Recovery
Infrastructure Agreements
State Chief Info Security Officer
James Saunders
State & Local Cyber
Cyber Resilience
Cyber & AI Governance, Risk, & Compliance
Cyber Technology
State Privacy
Executive Director MD Benefits
Pat McLoughlin
platformMaryland
Application development
Benefits services
Chief Technology Officer - Platform + Client Svcs
Jason Silva
Client Support & Service Delivery
SaaS Platform Svrcs
ERP Operations
Collaboration & Comms Platforms
Chief Digital Experience Officer
Marcy Jacobs
Web Experience
Service Design & Accessibility
Product Management
Engineering & Solutioning
MITDP Oversight
State Chief Data Officer
Natalie Evans Harris
Data Services
Data Operations
Data Management
Data Practices
Data Literacy

DoIT Priorities

1. **Building DoIT and agency capacity.**
2. **User centered service delivery.**
3. **Centralization to support agency missions.**

DoIT Accomplishments 2023-25

- **Department Wide Modernization:** DoIT completed a major organizational transformation, restructuring leadership, bringing the Chief Data and Privacy Officers into the department, and standing up new digital services, strategic sourcing, and compliance teams to modernize State IT operations.
- **Cybersecurity Expansion:** The Office of Security Management scaled from 5 to 22 full-time staff, launched the State's first bug bounty program ("Hack the State"), created an agency-embedded Information Security Officer program, and strengthened statewide cyber partnerships.
- **Modernized Benefits Delivery:** MD THINK transitioned from a project-based model to a product-driven approach, enabling the July 2025 launch of the mobile-first "One Application," now branded as Maryland Benefits, allowing residents to apply for multiple core benefits in a single application.

DoIT Accomplishments 2023-25

- **Digital Service & Accessibility Reform:** DoIT established the Maryland Digital Service to reduce technical debt, introduce in-house design and engineering expertise, and implement the State's first comprehensive digital accessibility policy.
- **AI Readiness:** Following the Governor's AI Executive Order, DoIT laid the groundwork for responsible AI adoption by issuing interim GenAI guidance, completing the State's first AI inventory, providing workforce training, and launching an AI Enablement team.
- **Broadband & Infrastructure Leadership:** On January 7, 2025, Governor Wes Moore established the State's Digital Infrastructure Group to better coordinate statewide digital infrastructure planning and investment under DoIT's leadership. This work supports a fiber first strategy that expands capacity, reduces duplication, and helps close the digital divide.

Maryland AI

We've built a strong foundation that has moved us from 0 to 1

Policy: Through the AI executive order, SB818, and internal AI guidance artifacts, we are shaping policy to enable progress and prevent setbacks.

Strategy: The 2025 AI strategy and study roadmap coordinates agencies and defines clear approaches to enable AI statewide, and clarify opportunities and risks in a dozen critical domains.

Data: Programs establishing authoritative data sources, strong data governance, data classification standards, and open data improvements are setting AI initiatives up for success.

Experimentation/Adoption: The State AI Inventory's almost 150 agency-submitted use cases; deployment in crucial areas; broadly vetted tooling; along with experiments and pilots show practical adoption.

Governance: AI policies are operationalized through DoIT intake, with ever-improving capabilities to unlock new use cases and ensure we first do no harm. Governance cards and AI Inventory center continuous monitoring.

Literacy: InnovateUS courses provide foundational and some role-specific AI learning to equip state staff with essential skills.

Community & org infrastructure: AI Community of Practice, AI Subcabinet, working teams at agencies; and national engagement build a growing, connected ecosystem for state AI leadership.

Centralized efforts to direct the power of AI to solve Statewide problems

- ➔ **Set direction:** Establish statewide AI strategy, governance, and policy through the AI Roadmap
- ➔ **Coordinate & adapt:** Use the AI Subcabinet to align efforts and adjust strategy over time
- ➔ **Focus on impact:** Target shared, high-value use cases (plain language, transcription, document management)
- ➔ **Build once, scale many:** Buy or build solutions that can be reused across agencies
- ➔ **Make data AI-ready:** Set standards for data quality, labeling, accuracy, and fairness
- ➔ **Power it all:** Scale secure AI infrastructure through Platform Maryland

Universal tools to increase the pace of AI-driven innovation by empowering and encouraging agencies to experiment

- ➔ **Platforms & tools:** Shared platforms, sandboxes, and applications to apply AI to agency workflows
- ➔ **Training & skills:** AI, data literacy, and privacy training in partnership with DBM and DOL
- ➔ **Community & alignment:** Forums for strategy and knowledge-sharing, including the AI Community of Practice
- ➔ **Procurement pathways:** Buy secure, private, cost-effective, future-ready AI systems with DGS
- ➔ **Ecosystem access:** Connections to academia, nonprofits, industry, and government for talent, licenses, and pilots
- ➔ **Hands-on delivery:** Solutioning and deployment support through Maryland Digital Service

Examples of “AI-Shaped Problems”

Example capabilities

- **Translation:** Improve accessibility in any language, focusing on top MD languages.
- **Document Processing:** Automate data extraction from forms and documents.
- **Coding Assistance:** Boost coder productivity, speed software delivery, modernize legacy code, enable rapid prototypes.
- **Digital Twins:** Real-time virtual models for simulation, analysis, and prediction.

Example areas of application

- **Call Centers:** Assist staff with faster, accurate responses; surface info to constituents; reduce backlogs.
- **Permitting & Licensing:** Shorten turnaround, improve experience, ensure complete applications.
- **Benefits Delivery:** Support case workers with high caseloads and complex regulations.

Maryland Digital Service

Maryland Digital Service (MDDS)

Mission: The mission of DoIT's Maryland Digital Service (MDDS) is to increase trust in Maryland's government through improved access to digital services and benefits. MDDS supports state agencies in delivering on their missions by building well-designed, human-centered digital experiences that improve efficiency and outcomes while reducing the cost of serving Maryland residents.

2025 Accomplishments: This year, MDDS has been focused on scale - reflected in team growth, procurement vehicle expansion, deployed teams to support agency projects, and delivery of critical foundational efforts.

Scaling MDDS Capabilities and Delivering Services

- **Team growth:** MDDS more than doubled from 22 to 49 staff (+122%) between 2024 - 2025.
- **Expanded** User experience, product management, and engineering capacity to better support agencies.
- **Awarded** ADEPT contract vehicle to 8 local firms to rapidly scale digital service delivery.
- **Validated** Drupal as a secure, scalable CMS; launched new Maryland.gov and modernized COMAR.
- **Implemented** statewide analytics (Google Analytics, Microsoft Clarity & CX measurement).
- **Completed** AI pilot with MDE and Percepta enabling self-service document access for site selection.
    - **Projected impact:** ~300 staff hours saved per month and ~50% reduction in PIA requests.

MITDP Background & Reform

- DoIT is responsible for oversight of all technology projects over $5M across the State, called “MITDPs”
- These projects have historically underperformed
- DoIT is implementing significant reforms to reduce risk that projects do not deliver, shifting the projects from project management or system implementation to **service delivery**
- Implemented ‘interventions’ - both discovery projects and deployed teams
- Publishing a MITDP Dashboard this month to increase visibility and transparency

Maryland's Goals in Investing in Permitting

1. Make it easier for Marylanders to get a job in their desired field
2. Make it easier to start, manage, and grow a business in Maryland
3. Make it easier to develop and build property in Maryland

Key Objectives for MDE Portal

- Long turnaround times are a major complaint, and lagging indicator of many underlying issues.
  - Paper checks can take 2-3 weeks to process and are prone to reconciliation issues
  - Current permit forms and processes could be simplified and streamlined
  - **OKR: reduce decision time by 25%**
- Secondary goals:
  - Make it easier to find correct permit
  - Enable applicants to track permit status without contacting MDE

Prioritization: Time-to-Value

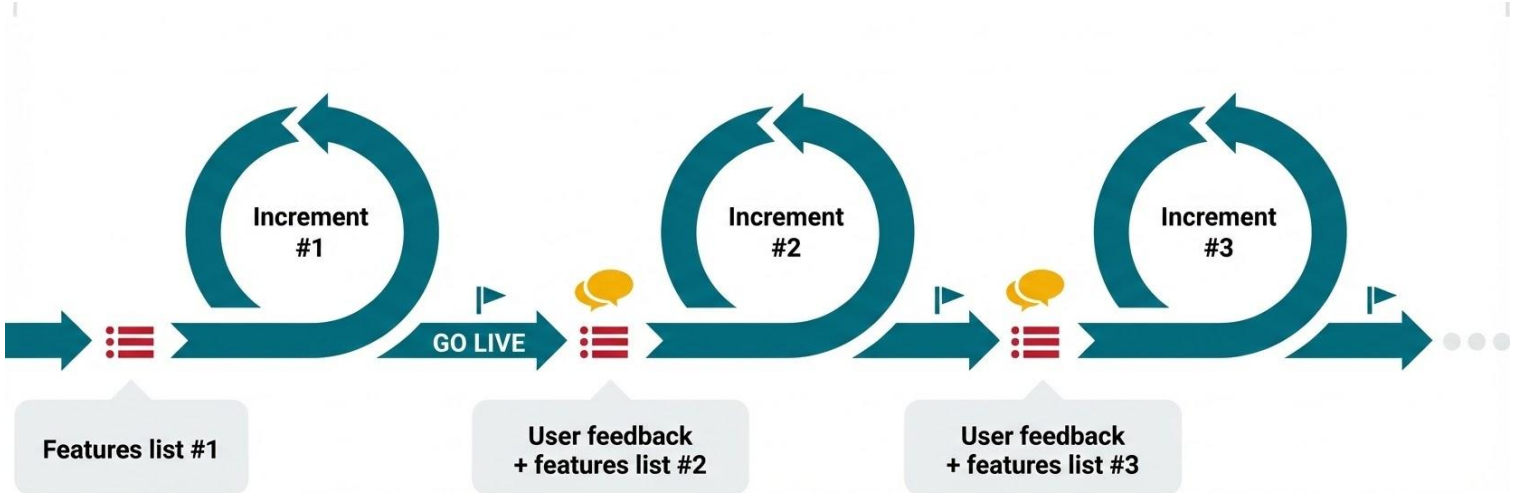
Our Product Roadmap prioritizes **Time-to-Value**. By focusing on the top **20%** of permits, we aim to capture **80%** of the application volume.

The original Project Plan treated development of all permits equally. This is risky because:

1. **ROI Mismatch:** We would spend thousands of dollars developing a permit used only once a year.
2. **Inflexibility:** Permits can have different characteristics, e.g. complexity or heavy manual review. The best way to support one category may be different than another. Worse, if we plan to treat all permits in the same way, but discover an error near the end of the project, we may have to re-do hundreds of permits.

Recommendation: We should prioritize based on *Volume Coverage*, not *Permit Count*. We target supporting 80% of MDEs volume by our project milestone date, rather than committing to a maximized number of permits.

Product Approach Focuses on Speed to Value



- Reduce risk by making smaller “bets”
- Iterative, shorter cycles to learn quickly
- Focus on continually adding value to users

Office of Security Management (OSM)

The **Office of Security Management (OSM)** is a legislatively established organization[1], led by the State CISO, focused on the cybersecurity & privacy of the State of Maryland.

- Statewide Cybersecurity & Privacy Strategy, Standards, and Policy
- Providing Centralized Cybersecurity Technology & Services
- Leading Statewide Cybersecurity Incident Response & Preparedness
- Reporting “State of Cybersecurity Preparedness” at least annually

1: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gsf&section=3.5-2A-04&enactments=True&archived=False

OSM Structure and Services

State Chief Privacy Officer (SCPO)	State & Local Cybersecurity (SLC)	State Cybersecurity Technology (CT)	State Cybersecurity Governance, Risk, & Compliance (GRC)	State Cyber Resilience (CR)
Oversees the Statewide Privacy Program to ensure the protection of citizen data.	Serves as the primary cybersecurity liaisons for state and local government entities.	Leads the architecture, engineering, and management of cybersecurity platforms.	Bolsters statewide cybersecurity and AI risk management through strategic oversight.	Executes whole-of-state cyber defense and proactive resilience services.
• **Implementing** Privacy Impact Assessment (PIA) processes. • **Developing** statewide privacy policies and standards. • **Managing** privacy-related incidents and responses. • **Ensuring** adherence to Fair Information Practice Principles (FIPPs).	• **Managing** the State and Local Information Security Officers (ISOs). • **Executing** statewide cybersecurity preparedness assessments. • **Leading** cybersecurity and privacy awareness training programs. • **Partnering** with critical infrastructure providers.	• **Managing** the lifecycle of centralized cybersecurity technologies. • **Designing** and assessing Zero Trust security architectures. • **Evaluating** readiness for Post-Quantum Cryptography.	• **Establishing** statewide cybersecurity, privacy, and AI governance policies. • **Managing** third-party and supply chain cybersecurity risks. • **Standardizing** guidelines for statewide security compliance.	• **Operating** the Maryland Security Operations Center (MD-SOC). • **Facilitating** the Maryland Information Sharing and Analysis Center (MD-ISAC). • **Administering** the Statewide Vulnerability Disclosure Program (VDP).

2025 OSM Accomplishments

1. **Launched the Vulnerability Disclosure Program (VDP)**, which enables responsible vulnerability reporting to state and local governments.
2. **Published the Maryland-ISAC Binding Operational Directive**, which allows state vendors and critical infrastructure partners to enroll.
3. **Partnered with state and local government cybersecurity policy experts** to advise Maryland's forthcoming Cybersecurity and Privacy Policies and standards.
4. **Improved the State's cyber defensives** by deploying AI-enabled email protection and began protecting critical websites behind a leading web application firewall.
5. **Deployed the State Information Security Officer (ISO) program**, assigning OSM liaisons to each organization under OSM's purview. Primary focus is reviewing 2022-2023 cyber preparedness maturity assessment findings and driving centralized cybersecurity service adoptions.
6. **Matured the Local ISO Program**, performing cybersecurity maturity assessments and supporting State and Local Cybersecurity Grant Program (SLCGP) applications.

OSM CY2026 Key Focus Areas

Governance

- **Governance Modernization:** Publishing updated, comprehensive statewide cybersecurity, AI, and privacy policies, standards, and guidelines.
- **Launch 2026-2027 Cyber Preparedness Maturity Assessments:** Resume assessing agencies' cybersecurity practices to identify areas of improvement.

Cybersecurity Defense

- **Cyber Centralization:** Continue driving cybersecurity centralization to achieve consistent visibility and response capabilities.
- **Infusing Zero Trust and Post-Quantum Cryptography readiness:** Identify, plan, and implement modern architectures and technologies to defend against emerging cyber threats.

Outreach and Partnership

- **Critical Infrastructure:** Expand the Maryland Information Sharing and Analysis Center (MD-ISAC) to include private utilities and Maryland's CI providers.
- **Deepened Partnerships:** Continue growing as a partner across the State, Local, and industry.

Questions/Discussion