

OIT ACCESS



OFFICE OF INFORMATION TECHNOLOGY

STREAMLINING IT IN ALABAMA STATE GOVERNMENT

IN THIS ISSUE

Network Security & Resilience	4
Alabama's Network Segmentation Project	
Digital Government Summit	8
2026 Event Details	
Agency Spotlight	10
Alabama Department of Corrections	
Alabama OpenAI Day	16
Highlighting Responsible Adoption Pathways	
Calera and Alabama's SLCGP	18
A Partnership in Cyber Readiness	
Service Spotlight	20
KnowBe4	



CONTENTS

Network Security & Resilience	4
Digital Government Summit.....	8
Agency Spotlight.....	10
Alabama OpenAI Day	18
Calera & Alabama's SLCGP	18
OIT Service Spotlight.....	20
Did You Know?.....	22
Out & About with OIT	26

Cover Photo: Stock photo of Oak Mountain State Park's colorful kayaks and canoes lined up and ready to rent for a fun day on Double Oak Lake in the summertime.



Photo: America 250 AL celebration and an F-35 fighter jet flyover. Official Office of the Governor photo taken by Billy Pope.

Welcome to *OIT Access*, the Office of Information Technology's quarterly newsletter. This publication is intended to be a resource for the numerous Alabama state agencies that rely on OIT and its services to help carry out their important missions and more effectively serve the citizens of our great state.

In addition to sharing the latest OIT news and announcements, each issue will help to keep readers informed about the wide range of information technology (IT) products and services available to agencies through OIT's Service Catalog. *OIT Access* also aims to be a platform for sharing news about several of the exciting IT projects, initiatives, and programs taking place at agencies across Alabama state government.

OIT is firmly committed to meeting the continuously evolving IT demands of the agencies we serve. If we are successful in this effort, it is the people of Alabama who are the true beneficiaries. OIT thanks you for your partnership in this vital work and we hope you enjoy this issue of *OIT Access*!

Leadership

Daniel Urquhart

Secretary
State Chief Information Officer

Willie Fields

Deputy Secretary

Chadwick Smith

Chief Information Security Officer

Aaron Wright

Chief Artificial Intelligence Officer

Mark Craymer

Executive Director of Shared Services

Brooke Covington

Executive Director of Finance

Keith Cousins

Executive Director of Business Execution

Our Mission

Lead the strategic IT management of Alabama executive branch digital assets by centralizing agency telecommunications, data, and cybersecurity services with comprehensive governance, cost-effective infrastructure, and enforcement of rigorous policy and standards that enable compatibility, security, and operational excellence.



Strengthening Alabama's Network Security and Resilience

OIT and Cisco Begin the Next Phase of the Network Segmentation Project



Strengthening the security, reliability, and resiliency of the State of Alabama's technology environment is one of OIT's most important responsibilities. As cyber threats become more frequent and difficult to contain, the State must continue taking practical steps to protect critical systems, safeguard sensitive information, and help ensure continuity of operations for the agencies and citizens that depend on them.

The Value of Network Segmentation

With that goal in mind, OIT has been advancing a multi-year Network Segmentation Project since 2024. Historically, the State has operated within a single, open network environment. While that approach supported broad connectivity, it also created a structural risk: a security incident affecting one system, environment, or agency could potentially spread and disrupt critical services elsewhere across the network.

Network segmentation is designed to reduce that risk by dividing the State network into smaller, more secure, and more manageable zones. In simple terms, this means creating clearer boundaries between important systems, applications, users, and network areas so that if an issue occurs in one part of the environment, it is easier to contain and less likely to affect unrelated services.

A Collaborative Approach

This effort is now moving into a new stage of direct, phased agency engagement, beginning with discovery and planning activities. OIT and Cisco, a trusted State partner with extensive networking and cybersecurity expertise, will work in close coordination with agency technology leaders to better understand each agency's systems, applications, connections, and service dependencies. That information will help guide an implementation approach that improves protection while minimizing operational impact.



Protecting State Agencies. Securing What Matters Most.

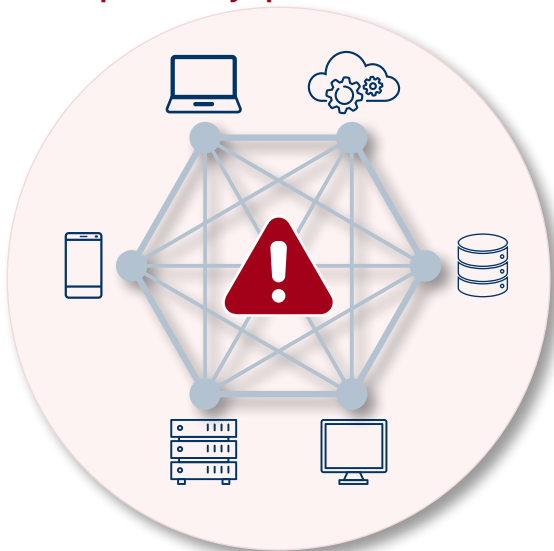
Cyber threats are increasing. An attack in one place can quickly disrupt critical agency services across the network.



Our Goal: Protect state agency services, reduce risk, and keep Alabama state government moving forward.

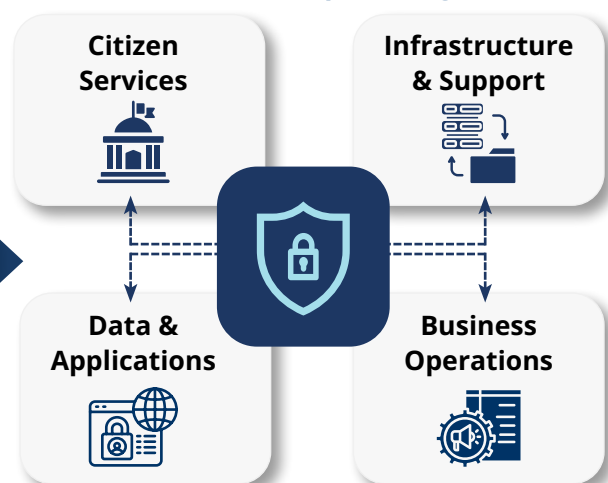
TODAY

Our network operates as one large, connected environment. A security issue in one area can **potentially spread to others.**



FUTURE

Create secure zones around important systems so problems stay contained and **services keep running.**



Each area is protected independently.
Problems stay isolated.

NETWORK SEGMENTATION BENEFITS FOR STATE AGENCIES



Protects What Matters

Better protects critical systems and sensitive information.



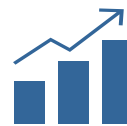
Reduces Impact of Incidents

Limits disruption so your team can respond faster and recover sooner.



Supports Statewide Security Goals

Aligns with OIT and State cybersecurity initiatives and requirements.



Creates a Strong Future Foundation

Establishes a secure platform that supports new services and growth.



Emphasizes Collaboration

Your team, OIT, and Cisco work together with minimal disruption to operations.



KEY TAKEAWAYS

- ✓ Support your technology team as they work with OIT and Cisco.
- ✓ Help OIT understand your environment so it can be protected the right way.
- ✓ No changes to your business processes are expected.



Your leadership helps us protect the services Alabama depends on.



Stronger protection. Less risk. Reliable services for Alabama.
That's the power of network segmentation.



What Agencies Can Expect

As agencies are scheduled for engagement, OIT will provide coordinated communications to each agency head and designated IT lead outlining the purpose of the effort, the discovery process, and the next steps for agency participation. The project is not expected to change agency business processes; its focus is strengthening protections around the systems and services Alabama depends on.

For agency business leaders, the purpose of this work is straightforward – strengthen protection without disrupting the mission. OIT is not asking agency leadership to manage the technical details of the project. Instead, agencies will be asked to support open communication between OIT, Cisco, and their technology teams so that operational priorities, business-critical services, and potential concerns are understood early in the process.

Agency technology teams will continue to serve as subject matter experts for their own environments. Cisco will provide technical guidance and engineering expertise, while OIT will coordinate the statewide approach to maintain consistency across the enterprise. Together, the teams will gather the information needed to identify key systems, map major dependencies, understand access requirements, and develop a practical roadmap for implementation.

The process is designed to be transparent and phased. Initial discovery will include an agency questionnaire, technical workshops, and review sessions to validate critical systems and operational needs. OIT and Cisco will then assess the information gathered, develop agency-specific recommendations, and work with the agency to plan deployment windows, milestones, and next steps. No production changes will occur without prior coordination, scheduling, validation, and approval with the agency.



Building a More Resilient Future

The expected benefits are significant. Network segmentation will help agencies better protect critical systems and sensitive information, reduce the potential impact of cyber incidents, improve resiliency and recovery by keeping issues more contained, support statewide cybersecurity goals and requirements, and build a stronger foundation for future modernization efforts.

Just as importantly, the project reflects a broader commitment to collaboration across Alabama state government. Cybersecurity is most effective when agencies, technical teams, and trusted partners work together with a shared understanding of both security needs and business priorities. Through this effort, OIT and Cisco will partner closely with agencies to strengthen Alabama's technology environment while supporting continuity of essential services.

As the Network Segmentation Project advances, OIT will continue communicating with agency leaders and technology teams to ensure planning remains coordinated, transparent, and aligned with each agency's mission. By taking this important step, Alabama is strengthening the network foundation that will support more secure, resilient State services for years to come.

Digital Government Summit

Make Plans to Attend the 2026 Alabama Digital Government Summit



Above Photo: Secretary Daniel Urquart welcomes attendees to the 2025 Alabama Digital Government Summit.

The 2026 Alabama Digital Government Summit is set to take place on Thursday, November 5, 2026, at the Renaissance Montgomery Hotel and Spa at the Convention Center.

In partnership with Government Technology (GovTech), OIT hosts this annual event, which unites state and local government leaders to explore new technologies, collaborate on real-world automation, and brainstorm modern solutions to ongoing challenges. The Alabama Digital Government Summit is designed to deliver valuable peer connections and actionable guidance for shaping strategy and moving public sector priorities forward.

This year's event will feature a variety of speakers discussing topics such as:

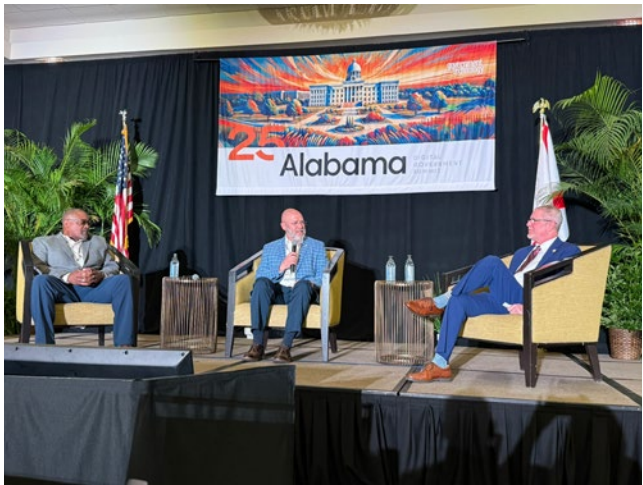
- Emerging technologies
- Data management and governance
- Cyber resilience
- AI and workforce readiness
- Alabama's State and Local Cybersecurity Grant Program (SLCGP)
- And more!



All state and local IT professionals will receive complimentary registration to the 2026 Summit. Complimentary guest parking will also be available in the Renaissance parking deck. Please be sure to bring your parking voucher to the conference registration table upon check-in to have your parking ticket validated upon arrival.

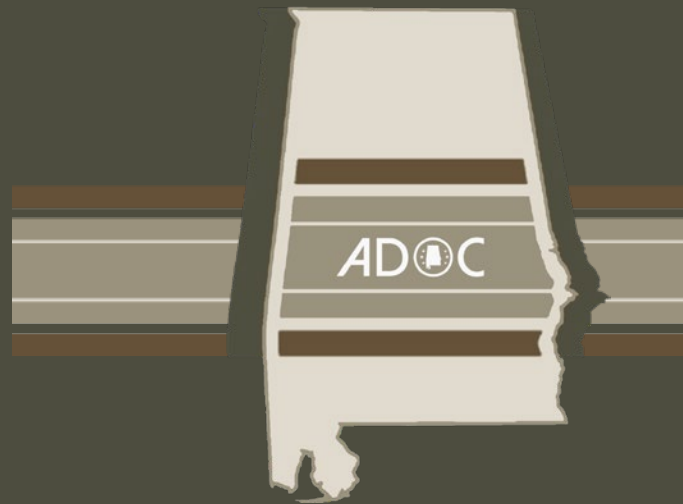
To learn more about the 2026 Alabama Digital Government Summit and to register, please visit GovTech’s event page at events.govtech.com/Alabama-Digital-Government-Summit.

We look forward to welcoming you on November 5th for a day of collaboration, partnership, insight, and solutions. See you there!



Agency Spotlight

Alabama Department of Corrections



The Alabama Department of Corrections (ADOC) is modernizing the technology that supports facility operations, administrative services, and leadership decision-making. The goal is straightforward: give employees reliable tools, reduce unnecessary manual work, protect sensitive information, and make trusted data available when it is needed.

By improving our administrative systems and making better use of information, we are strengthening facility security while becoming a more efficient and resilient organization.

John Demas, Chief Information Officer — Alabama Department of Corrections

This work is not centered on one application or one office. It is a coordinated, department-wide effort spanning statewide infrastructure, health services, security and law enforcement, financial and workforce systems, transportation, supply and inventory, education and rehabilitation, administrative and community services, cybersecurity, data integration, reporting, and business continuity across Alabama. These functions carry distinct legal, operational, security, privacy, and reporting requirements, yet their systems and processes are increasingly interdependent. Together, they are helping ADOC build a more secure, efficient, resilient, and connected correctional environment.

Strengthening Infrastructure and Operational Resilience

Technology has become essential to the daily operation of a correctional system. ADOC supports health services, law enforcement, finance, transportation, logistics, education, administration, and community services in a complex 24-hour environment. Personnel depend on reliable systems and communications to perform critical duties, manage resources, meet reporting obligations, and respond to operational needs. A modern application is only useful when employees can reach it consistently and trust its availability.

ADOC is working with the Alabama Office of Information Technology (OIT) and other state partners to strengthen the infrastructure behind these services. This includes improving network connectivity, system availability, equipment management, monitoring, access controls, and continuity planning. The work also includes identifying aging technology, standardizing equipment where practical, and improving coordination between central-office and facility personnel.



Correctional facilities present unique technological challenges. Systems must operate reliably across geographically dispersed, secure facilities, support employees around the clock, and accommodate clinical, security, transportation, inventory, education, and program workflows. Maintenance and upgrade windows are limited, and changes cannot unnecessarily disrupt facility operations. ADOC therefore evaluates not only what technology is installed, but how it is integrated, deployed, supported, secured, maintained, and recovered.

Reliable connectivity is especially important as ADOC adopts more cloud-based applications and statewide platforms. Infrastructure planning and application modernization must move together because network capacity, workstation readiness, user access, security controls, technical support, and recovery requirements span multiple platforms and locations. These interdependencies have to be considered before a new system can deliver its intended value.

Operational resilience is another key focus. Equipment failures, connectivity interruptions, cybersecurity incidents, and other unexpected events can make mission-critical systems temporarily unavailable. Business continuity and disaster-recovery planning help ADOC identify critical services, assign responsibilities, document recovery procedures, and establish practical alternatives. These preparations support facility safety and help the department continue essential administrative and operational functions during disruptions.

Modernizing Administrative Operations

A statewide correctional agency manages interdependent financial, procurement, personnel, payroll, timekeeping, transportation, supply, inventory, health services, education, program, and reporting requirements across facilities, central offices, community operations, and shared state services. Activity in one area can affect staffing, security, purchasing, budgeting, service delivery, and compliance elsewhere. When these functions depend on disconnected systems, spreadsheets, paper workflows, or repeated manual entry, employees spend valuable time reconciling information and correcting inconsistencies. Modernization is intended to reduce that burden while strengthening accountability and visibility.



ADOC's implementation of the Correctional Information System (CORIS) of Alabama (CORAL) is an opportunity to improve how administrative and financial information is recorded, processed, reviewed, and reported. Created by Abilis Solutions, CORIS is an enterprise-wide platform dedicated to helping correctional agencies manage inmate data, facility operations, and community supervision. The objective is not simply to replace one application with another. It is to review existing procedures, remove unnecessary steps, standardize processes, and improve the quality of information available to managers.

More consistent processes can reduce duplicate work, strengthen internal controls, improve reporting, and provide leadership with more timely information about expenditures, obligations, and available resources. Successful implementation also requires practical readiness: accurate data, clearly defined business processes, appropriate security roles, effective testing, and support for employees as they learn the new system.

ADOC is taking a similar approach to workforce-management modernization. The department receives and manages information from multiple scheduling, timekeeping, payroll, and State-supported systems, each with distinct data, business rules, and operational dependencies. The transition to the Ultimate Kronos Group (UKG)'s eSTART software platform creates an opportunity to improve how employee time, leave, schedules, and payroll-related information are managed.

For an organization operating correctional facilities 24 hours a day, seven days a week, workforce information is operationally critical. Leaders need a clear view of staffing levels, scheduled hours, actual hours worked, leave usage, overtime, and potential coverage gaps. Modern tools can provide this information more consistently, but only when data exchanges are accurate, calculations are validated, responsibilities are clear, and business processes are understood by everyone involved.

Employee readiness is just as important as technical readiness. A well-designed system can still fall short when users do not understand the process behind it or lack confidence in the information it produces. Training, documentation, communication, and post-implementation support are therefore essential parts of ADOC's modernization strategy. Employees need to know not only how to complete a task, but also why the process is changing and how their work affects other areas of the department.

Building a Connected, Data-Driven Department

A major challenge in a large, geographically distributed organization is making sure systems and business processes work together. ADOC manages information across security and law enforcement, health services, transportation, finance, workforce, supply and inventory, education, rehabilitation, community services, and statewide platforms. Historically, much of that information has been delivered through separate exports, reports, spreadsheets, or manual processes. Each system may perform its own function, but the department gains far greater value when information can be shared, validated, and used consistently.

ADOC is working toward a connected technology environment in which data is treated as a department-wide resource rather than information belonging to a single system or office. That requires common definitions, improved data quality, clear ownership, reliable interfaces, documented responsibilities, and reporting processes that decision-makers can trust.

For example, workforce data affects more than scheduling. It also influences payroll, budgeting, overtime, transportation coverage, security posts, health services staffing, education and program delivery, and compliance reporting. Financial data supports procurement, contracts, inventory, fleet operations, budget development, program oversight, and executive decision-making. When systems are disconnected, employees must manually reconcile information, increasing errors, delaying reporting, and obscuring the authoritative source.

Data governance provides the structure needed to address those issues. In practical terms, it establishes how information is defined, collected, protected, maintained, shared, and retained. It also identifies who is responsible for resolving discrepancies and approving changes. Without that structure, different offices may use the same term to mean different things, maintain competing versions of a report, or rely on information that has not been fully validated.

The department is also working to ensure that new systems do not create new data silos. Modern platforms must be evaluated not only on their individual features, but also on how they interact with ADOC's broader technology environment, shared state services, and business processes. This approach supports operational intelligence, financial and workforce planning, health services, transportation and logistics, inventory control, education and rehabilitation, community services, mandated reporting, and safety reporting.

Improving Reporting and Executive Decision-Making

Modernization is most valuable when it helps employees and leaders make better decisions and demonstrate compliance. ADOC is improving the availability, consistency, traceability, and usefulness of information for managers, executive leadership, and authorized state and federal partners. This includes establishing trusted data sources and reducing the time required to prepare recurring operational, financial, programmatic, and mandated reports.

In a fragmented environment, one report may require information from several systems. Employees may have to download files, combine spreadsheets, correct formatting, and manually verify totals before the report can be used. The result may be accurate, but the process is slow, difficult to repeat, and vulnerable to inconsistencies.

ADOC's goal is more standardized and sustainable reporting. Wherever practical, information should come from validated sources, be calculated using documented rules, retain an auditable history, and be presented in a format appropriate for the decision or requirement being addressed. Better reporting can help leadership identify operational trends, understand resource demands, evaluate project and program progress, recognize emerging risks, meet state and federal reporting obligations, and determine where additional attention is needed. The objective is not to produce more reports. It is to provide the right information to the right people at the right time.

Cybersecurity as an Operational Responsibility

As ADOC becomes more dependent on connected systems across distributed locations, cybersecurity must remain central to every technology initiative. Correctional systems contain sensitive health, operational, law-enforcement, personnel, financial, education, community-services, and security-related information. Protecting that information requires more than purchasing security products. It requires clear policies, employee awareness, access management, system monitoring, vulnerability management, incident-response planning, and coordination with state cybersecurity partners.

Identity and access management is one practical example. Employees should receive the access necessary to perform their duties, but permissions must also reflect job responsibilities and appropriate separation of duties. Access should be reviewed when employees change positions, assume new responsibilities, or leave the department. These controls help protect sensitive information and reduce the risk of unauthorized activity.

Employees also remain an important part of ADOC's defense against phishing, credential theft, malicious files, and other common threats. Technology teams can implement safeguards, but strong security depends on informed users who recognize suspicious activity and follow established procedures. Cybersecurity is therefore not a separate technical function; it is an operational responsibility that supports facility safety, information integrity, workforce continuity, and public trust.

Modernization Through Partnership

None of these initiatives can be completed by one office working alone. Many span several functional areas and must be coordinated while daily operations continue. ADOC's modernization depends on collaboration

among correctional leadership; facility, health services, security, transportation, logistics, finance, human resources, procurement, inventory, education, program, and community services personnel; information technology staff; state agencies; vendors; and other partners.

OIT is an important partner in this work, providing statewide leadership, technical standards, cybersecurity support, procurement assistance, infrastructure services, and coordination for initiatives that extend beyond a single agency. ADOC also works with partners such as the Alabama Law Enforcement Agency (ALEA), the Alabama Department of Finance's State Business Systems (SBS), Ingram State Technical College (ISTC), and the Alabama Bureau of Pardons and Paroles (ABPP) when technology, data, or statewide processes across agencies.

ADOC's role is to make sure statewide solutions meet the practical needs of a large, shift-based correctional environment. A system may function technically but still require changes to support secure facilities, health services, transportation, inventory accountability, education and program operations, community services, law enforcement, financial controls, or department policies. That is why subject-matter experts and end users are involved throughout planning, testing, training, implementation, and post-implementation review.

Modernization also requires accountability from vendors and project partners. Responsibilities, deliverables, data requirements, testing expectations, and implementation milestones must be clearly defined. When problems arise, they must be documented, assigned, and resolved promptly so that every participant remains focused on delivering a functional outcome for the Department.

Looking Ahead

Technology is not the primary mission of ADOC, but it is the connective foundation for the department's highly complex responsibilities. Reliable systems support facility security and law enforcement, continuity of health services, transportation and logistics, supply and inventory control, financial accountability, education and rehabilitation, administrative and community services, and the data needed to meet state and federal mandates. Strong cybersecurity protects these critical operations and the sensitive information they depend upon.

ADOC will continue working with OIT and its other partners to improve system integration across these operational areas, strengthen reporting, reduce unnecessary manual processes, modernize aging infrastructure, enhance continuity planning, and ensure employees have the training and support needed to use new systems effectively. Going live is an important milestone, but it is not the end of modernization. Systems must be monitored, processes reviewed, user feedback considered, and improvements continued as operational needs, statutory requirements, and reporting obligations evolve.

The department's direction is clear: connect and modernize the full breadth of correctional operations to build a safer, more accountable, and more resilient correctional system for Alabama.





Alabama OpenAI Day

Highlighting Practical Pathways for Responsible AI Adoption

Artificial intelligence (AI) continues to move from emerging concept to everyday operational tool, and Alabama state agencies are taking thoughtful steps to understand how this technology can be used responsibly, securely, and effectively. On Wednesday, July 22, OIT partnered with OpenAI to host Alabama OpenAI Day, a focused event designed to help agency leaders explore practical ways AI can support State operations and improve service delivery.

Preparing Practical Agency Use Cases

In the weeks leading up to Alabama OpenAI Day, OpenAI worked directly with a small group of state agencies that were already actively using ChatGPT licenses. These pre-event engagements gave participating agency teams an opportunity to identify meaningful business challenges, shape those ideas into practical AI use cases, and prepare demonstrations that could be shared with a broader audience.

Rather than focusing on theoretical possibilities, the agencies explored how ChatGPT could be applied to real workflows within state government. This work helped participating teams think through the value of their ideas, consider how AI could assist staff in their daily responsibilities, and determine how their use cases could be responsibly replicated within Alabama's shared technology environment.

By grounding the discussion in agency-driven examples, OpenAI worked with these teams to showcase the potential benefits of AI usage across the executive branch. The use cases that were developed demonstrated not only what AI tools can do, but also how agencies can begin moving from early interest to secure, mission-focused implementation.

Hands-On Support for Power Users

Alabama OpenAI Day began with a dedicated Power User Working Session, where participating agency teams received hands-on guidance from OpenAI experts. Building on the pre-event engagements, the session gave teams additional time to strengthen their demonstrations, ask practical questions, and consider how their workflows could be improved before presenting them to the larger audience.

This format helped power users move beyond general AI awareness and focus on specific opportunities within their agencies. It also reinforced the importance of prompt development, thoughtful workflow design, and responsible use as agencies continue learning how AI can support their missions.



Agency Demonstrations and Adoption Insights

Later that afternoon, agency participants from across the executive branch gathered in the Gordon Persons Auditorium for a session featuring the agency project demonstrations developed in advance of the event, as well as OpenAI insights on AI adoption from peer states and relevant federal agencies. The session wrapped up with an executive discussion of priority applications and next steps for Alabama.

A key emphasis throughout Alabama OpenAI Day was responsible adoption. As agencies explore how AI can support their missions, OIT continues to stress the importance of using approved tools, maintaining appropriate enterprise controls, protecting sensitive data, and ensuring that promising ideas can be implemented safely within the State's technology environment. Alabama OpenAI Day provided agencies with a valuable forum to discuss those considerations while also seeing how AI can be applied to realistic government workflows.

Learning Across Agencies

The event also encouraged cross-agency learning. By hearing from peer agencies and discussing common challenges, participants were able to identify areas where AI may help streamline internal processes, support decision-making, or improve service delivery. These conversations are especially important as Alabama continues building a coordinated approach to AI that balances innovation with accountability.

Moving Forward with Purpose

Alabama OpenAI Day was another positive step in Alabama's broader AI journey. It reinforced that successful AI adoption is not simply about deploying new tools; it requires collaboration among agencies' executive leadership, IT professionals, legal teams, business leads, and frontline staff who understand agency operations. It also requires a commitment to governance, training, and continuous evaluation so that agencies can use AI in ways that are both beneficial and responsible.

As agencies continue developing AI use cases, OIT will remain focused on helping the State move forward with purpose. By creating opportunities for hands-on learning, responsible experimentation, and informed discussion, Alabama is positioning itself to embrace new technology while protecting the data, systems, and public trust that are essential to state government.

Through continued collaboration with agencies and technology partners, OIT will help ensure AI adoption in Alabama remains practical, secure, and focused on improving the way state government serves its citizens.

Calera and Alabama's SLCGP

A Partnership in Cyber Readiness



Cybersecurity can be difficult for local governments to explain, fund, and sustain. Unlike a road, facility, or other visible public investment, successful cybersecurity improvements are rarely noticed by residents. Yet for Alabama's cities, counties, schools, utilities, and other public-sector entities, strong cybersecurity is essential to keeping public services running.

That message was central to Alabama's inaugural Public Sector Cybersecurity Summit, which took place on Thursday, June 4, 2026, in Montgomery. Hosted by the Alabama Office of Information Technology (OIT) and Government Technology, the event provided an important

opportunity to promote Alabama's State and Local Cybersecurity Grant Program (SLCGP) and encourage eligible entities to apply for available support.

A featured session highlighted a success story from the City of Calera. Craig Whittinghill of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security and James Fuller, Chief Information Officer for the City of Calera, discussed how Alabama's SLCGP is helping local governments strengthen cybersecurity in a way that is approachable, collaborative, and responsive to local needs.

Like many growing municipalities, Calera supports a broad range of public services with a lean technology team and an IT environment that must remain available, reliable, and secure. Fuller emphasized that cybersecurity investments may not always be visible to the public, but they are critical to protecting systems that residents, employees, and local leaders depend on every day.

Through Alabama's SLCGP, Calera found a practical way to build on its cybersecurity priorities. The city worked with cybersecurity professionals from the McCrary Institute to evaluate needs, identify opportunities for improvement, and determine which services would provide meaningful value. Rather than navigating the process alone, Calera had access to knowledgeable partners who understand the realities of local government IT.

That partnership-driven approach is a defining feature of Alabama's SLCGP. OIT serves as the State Administrative Agency for the grant program and works with the McCrary Institute to provide

cybersecurity guidance and service delivery. Through this model, eligible entities can assess their cybersecurity posture, identify gaps, and connect with resources designed to improve resilience.

For Calera, the experience was both practical and validating. Fuller described the process as straightforward and responsive, noting that it helped the city prioritize improvements while reinforcing that its team was asking the right questions and moving in the right direction.

The session also addressed a common concern among local governments: whether participating in a state-supported cybersecurity program means giving up control of local systems. Fuller made clear that this was not his experience. Instead, he described Alabama's SLCGP as a collaborative program that respects local decision-making while providing access to expertise, tools, and support that many local governments could not easily obtain on their own.

Fuller emphasized that the goal of Alabama's SLCGP is not to take over local networks. Rather, it is to help eligible entities make informed cybersecurity decisions, improve their posture, and strengthen public services across Alabama.

Alabama's SLCGP offers eligible cybersecurity services and resources such as assessments, security awareness and phishing training, endpoint protection, vulnerability scanning, multi-factor authentication, enhanced logging, boundary protection, network monitoring, password management, business continuity support, cybersecurity planning, incident response exercises, and related services.

The program also supports participating entities through the Alabama Cybersecurity Intelligence Center (ACIC), a centralized cybersecurity hub developed through OIT's partnership with the McCrary Institute. ACIC is designed to enhance threat intelligence, information sharing, monitoring, vulnerability analysis, and incident response coordination for eligible entities that participate in the program.

Calera's experience demonstrates why this work matters. Local governments are responsible for essential services, sensitive information, public safety functions, financial systems, and citizen-facing operations. Even modest improvements in visibility, authentication, monitoring, training, and planning can strengthen an entity's ability to prevent, detect, respond to, and recover from cyber threats.

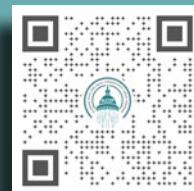


Fuller's advice to other eligible Alabama entities was simple: apply. Entities do not have to solve every cybersecurity challenge before participating. The program is designed to help them understand where they are, determine where they need to go, and identify practical next steps.

Eligible Alabama entities are encouraged to learn more and apply at slcgp.alabama.gov. Services and resources are available while funding remains available and are subject to program approval.

Just sign up for the program. It really is the easiest grant you'll ever apply for.

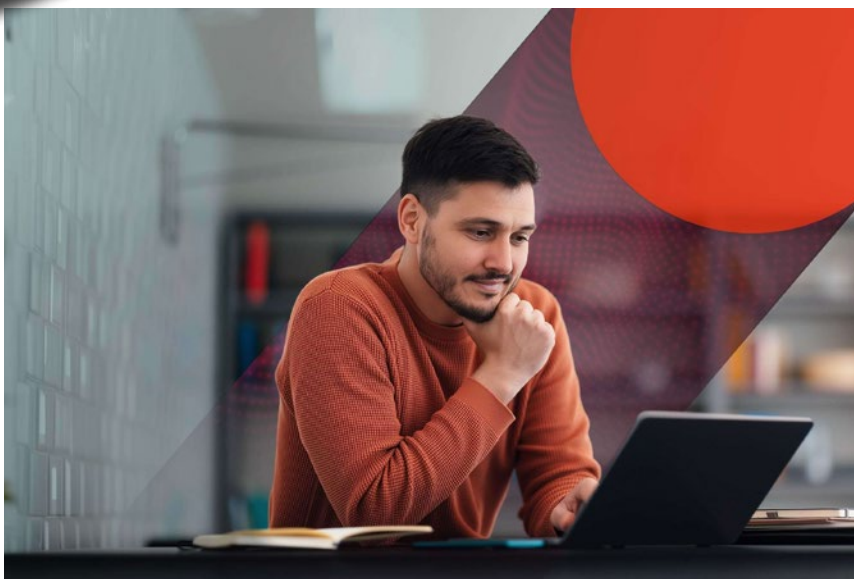
~ James Fuller, Chief Information Officer, City of Calera



**SCAN &
APPLY
TODAY!**

OIT Service Spotlight

knowbe4



Security awareness training is essential to strengthening Alabama's cybersecurity posture. While technical safeguards are critical, people remain among the State's strongest lines of defense against phishing, credential theft, social engineering, and other common cyber threats.

To continue improving the training experience for learners and administrators, the State of Alabama is moving to KnowBe4 as its enterprise learning management system (LMS) for security awareness training. KnowBe4 was selected because of its robust

security training content, phishing campaign management capabilities, and flexible administrative tools that can support a wide range of state agencies, affiliated organizations, and public entities.

With the contracts for the State's current security awareness LMS — ThreatAdvice and Inspired eLearning — expiring, this move also provides an opportunity to consolidate from multiple platforms to a single enterprise solution with expanded capabilities and a more consistent user experience. Organizations are encouraged to begin moving to KnowBe4 now to avoid potential training disruptions, as users will no longer have access to the current LMS platforms or associated training content once these contracts expire (ThreatAdvice: September 30th / Inspired eLearning: December 21st).

Security awareness training is available to state agencies, both within and outside of the Alabama Shared Tenant, as part of their Information Security Services fee. Moving to the KnowBe4 platform will not result in any immediate changes to that fee. OIT will also work with affiliated public entities not subject to this fee to help coordinate next steps for use of the platform where applicable.



KnowBe4 offers an expanded library of training content covering cybersecurity, remote work, artificial intelligence, and regulatory topics such as HIPAA, PII, PHI, and FERPA. In addition to OIT-recommended annual courses, organizations can assign targeted training for policy acknowledgements, regulatory tracking, or other specific needs.

The platform also provides dashboards and reporting for manager-level and executive-level visibility, agency branding for training materials, and phishing campaign tools to administer, track, and report campaign progress. Each organization that uses KnowBe4 will have its own environment and can manage its own courses, groups, phishing campaigns, and reporting, with OIT Governance, Risk, and Compliance staff available to assist administrators as needed.

By moving to KnowBe4, Alabama is taking an important step toward a more unified, efficient, and engaging approach to security awareness training. This enterprise platform will help organizations educate learners, reinforce secure habits, and better prepare users across Alabama government to recognize and respond to today's evolving cyber threats.

For questions or to begin moving your agency's learners to KnowBe4, reach out to the OIT Service Desk at service.desk@oit.alabama.gov or (334) 242-2222 and open a ticket titled "KNBE-Onboarding and Access."

Did You Know?



AI in Action: Microsoft Copilot Enablement

Beginning in July, OIT launched a limited Microsoft Copilot enablement effort to better understand how generative AI can support day-to-day work across state government. Working with a small group of agencies and their designated pilot participants, this early phase is intended to test practical use cases in Microsoft 365, gather feedback from agency users, and identify the guidance and support agencies will need before broader adoption.

Through overview sessions, hands-on immersion activities, and feedback opportunities, participants are exploring how Copilot may assist with tasks such as summarizing information, drafting content, preparing meeting notes, and improving productivity.

The goal is not simply to introduce a new tool, but to learn where Copilot can provide real value for users and how OIT can help agencies use it responsibly and effectively. OIT will continue emphasizing responsible use, good data hygiene, appropriate permissions, and verification of AI-generated outputs as this enablement effort moves forward.



October is Cybersecurity Awareness Month

October is National Cybersecurity Awareness Month and OIT wants you to be prepared.

OIT echoes this year's message from the Cybersecurity and Infrastructure Security Agency (CISA), specifically reminding everyone who manages critical infrastructure to practice the 3 Rs of Cybersecurity: Reduce (vulnerabilities), Replace (end-of-support devices), and Recover (quickly to sustain operations). Check out OIT's LinkedIn page at [linkedin.com/company/alabama-office-of-information-technology/](https://www.linkedin.com/company/alabama-office-of-information-technology/) all month long for more information about how you can do your part in ensuring our state's infrastructure and networks are strong and secure.



Copper Service Contract Expiration

The State's copper service contract will expire on April 15, 2027, marking an important step in OIT's ongoing effort to move agencies away from aging copper-based services and toward more modern, supportable solutions. Copper facilities and the infrastructure that supports them are increasingly difficult and costly to maintain as providers continue retiring legacy service.

This transition is important for improving long-term reliability, reducing risk, and helping agencies avoid potential service impacts tied to outdated technology. If your agency has not yet transitioned off copper-based services, please reach out to the OIT Service Desk as soon as possible for assistance in developing a transition plan.

Copper-based service will cease to be available as of April 2027.



Cleaning Up Stale Accounts and Devices

OIT has begun a structured review of State user accounts and devices that may be stale, duplicated, or no longer in use across Active Directory and Microsoft Entra ID. This effort is designed to improve security, reporting accuracy, licensing visibility, and overall directory health while minimizing agency impact.

An enterprise-wide informational meeting took place on July 15 to introduce the effort and discuss how agencies can help validate reports, identify exclusions, and provide feedback on the access review process. Because personnel and administrative teams may be best positioned to confirm whether certain user accounts, shared mailboxes, or business-related resources are still needed, agencies are encouraged to involve those teams as part of the review process.

During the initial reporting period, agencies are asked to review OIT-provided reports and identify any devices, accounts, service accounts, shared resources, or operational systems that remain active, business critical, or tied to special use cases before future action is taken.

An additional benefit of this effort is that it will support managed patching and vulnerability remediation by improving inventory accuracy and helping agencies address unsupported software, maintenance windows, exceptions, and devices that need attention. Agencies should continue reviewing reports and coordinating with OIT on questions or required exclusions.

Did You Know?



Maintaining Momentum on Digital Accessibility

As OIT has shared in previous issues of OIT Access, the Department of Justice's compliance deadline for website and digital content accessibility requirements under Title II of the Americans with Disabilities Act has been extended to April 26, 2027.

While the extension has provided additional time, agencies should continue reviewing and remediating public-facing websites, online services, documents, forms, applications, and other digital content to meet WCAG 2.1 Level AA standards.

Accessibility should also be built into normal publishing workflows so new content is accessible when released. OIT will continue supporting agencies with guidance, tools, and agency-specific consultation as the new deadline approaches.



Microsoft Retiring SMS and Voice Authentication

Microsoft has announced that it will retire SMS (i.e., text message) and voice authentication methods on February 1, 2027. Several agencies have users who rely on a text message or phone call for multifactor authentication (MFA), so this change will be impactful and may require action by your agency's IT team.

Agencies should continue identifying users who rely on SMS or voice authentication, as well as devices or business processes that may require remediation or an exception path. Users already using passkeys, Windows Hello for Business, FIDO2 security keys, Microsoft Authenticator, or another approved method should see little to no impact.

Early review and action will help agencies avoid authentication and access disruptions once Microsoft retires SMS and voice authentication methods in early 2027.



New Emerging Tech Pages on OIT Website

OIT has launched a new Emerging Tech section on the OIT website to provide a central location for information related to emerging technologies and responsible innovation. The section includes details about the Technology Quality Assurance Board, AI Community of Practice, training resources, past events, information from the GenAI Task Force's completed work, and other helpful materials.

These pages also help consolidate information about emerging technologies and Alabama's ongoing work to evaluate, adopt, and implement innovative solutions. Agencies are encouraged to bookmark oit.alabama.gov/emerging-tech and check back regularly for updates as statewide efforts in this space continue to evolve.



Mainframe Migration and Data Cleanup

OIT is working with agencies that still maintain data, applications, or services on the State mainframe to plan for migration and data cleanup before the end of 2026. While this effort directly affects agencies with remaining mainframe usage, it is an important modernization milestone for the State as a whole.

OIT is negotiating a single-year renewal with Kyndryl for 2027, which is expected to be the final year of State mainframe service. Agencies that will require mainframe service into 2027 should anticipate significant price increases during the final year and are encouraged to review what still resides on the mainframe, determine whether data or services can be migrated, archived, or removed, and identify any support that may be needed to complete cleanup or transition activities. Doing so will help reduce unnecessary costs, limit risk, and support a more modern, sustainable technology environment.

Agencies with questions or remaining mainframe needs should contact the OIT Service Desk as soon as possible to begin coordination.

Out & About with OIT



Above — State & Local Government AI Summit: In August, Chief Artificial Intelligence Officer Aaron Wright represented the State of Alabama at the 2026 State & Local Government AI Summit in Huntington Beach, California.



Above — ALGMIS Summer Conference: OIT Director of Grants Management, Brian Forster, and members of Auburn University's McCrary Institute attended the Alabama Government Management Information Sciences' (GMIS) summer conference to promote Alabama's State and Local Cybersecurity Grant Program (SLCGP) and encourage eligible local government entities to apply for funding.



Above — OIT Service Pins: On August 20th, OIT celebrated several deserving team members by presenting them with longevity service pins in recognition of their years of dedicated service to the State of Alabama. Pictured (L to R): Jelene Franklin, Larry Prestwood, Nic Thomas, Ben Bernhart, Daniel Urquhart, Kiya Stephens, Marilyn Frazier, Samantha Brown, Linda Hood, and Michael Bowen.



Above — College Colors Day: OIT staff participated in the Governor's Proclamation of College Colors Day promoting higher education on September 4th.





Above — Alabama League of Municipalities Meeting: OIT was invited to speak at the Alabama League of Municipalities' annual Standing Committee Meeting on September 3rd. Chief Information Security Officer Chad Smith presented to the Committee on Public Safety and encouraged city leaders to consider cybersecurity every bit as critical as other essential municipal services like police and fire.



Above and Left — State Combined Campaign 2026 Kick-Off Brunch: SCC Key Workers from OIT attended the 2026 State Combined Campaign Kickoff. Each year the campaign provides the opportunity for Alabama public employees to support numerous worthy causes

around our region and state. Samantha Brown (L) and Kenyatta Fishoe (R) won door prizes donated to the SCC by Heart Gallery Alabama and the Children's Center of Montgomery.



Above — Patriot Day: On September 11th, OIT employees gathered for a moment of silence to reflect on the 25th anniversary of the 9/11 terrorist attacks on our nation, to remember those who lost their lives, and to honor the brave first responders who rushed toward danger. #NeverForget



Left — End of Summer Luau: Members of the OIT Client Support team marked the end of summer with a fun, lighthearted luau on September 2nd.



Streamlining IT in Alabama State Government

GET IN TOUCH

Address

64 North Union Street,
Montgomery, AL 36130

Contact

Main Phone: (334) 242-3800
Service Desk: (334) 242-2222

Email | Website

Service.Desk@oit.alabama.gov
OIT.ALABAMA.GOV

