



Department of
Administrative
Services

Ohio Cybersecurity and Fraud Advisory Board

September 2026

DRAFT

Background

Established in Ohio Revised Code (ORC) 126.41 in 2025, the Ohio Cybersecurity and Fraud Advisory Board (Board) was created to examine and develop recommendations regarding best practices, operational experiences, and future efforts to improve cybersecurity and fraud prevention across State of Ohio IT systems and shared services. Membership consists of senior cybersecurity and technology leaders across state government, including representatives from the Governor's Office, the Secretary of State's Office, the Treasurer of State's Office, the Auditor of State's Office, and the Attorney General's Office and the State Chief Information Security Officer from the Department of Administrative Services (DAS).

This report addresses cybersecurity and fraud prevention with respect to the information technology systems and shared services used across state agencies, including fraud against state programs, payments, and identities that is committed through those systems.

Report Scope

ORC 126.41 sets the scope of the Board's work. As stated in law, with respect to the state's cybersecurity and fraud prevention measures, this report is not to examine:

- Open vulnerabilities
- Security protocols
- Legal issues

This report strictly considers the subset of cyberfraud in which fraud is committed using digital systems, networks, or the internet with respect to the information technology systems and shared services used across state agencies.

Executive Summary

Governor Mike DeWine has issued many Executive Orders since 2019 that have enabled the modernization of Ohio's cybersecurity and digital-service landscape. The state has delivered sustained, measurable advancements in protecting both government systems and the Ohioans who rely on them. Ohio has established the Ohio Comprehensive Cybersecurity Plan, strengthened identity-centric protections through the InnovateOhio Platform, expanded whole-of-state cybersecurity support to local governments, and significantly matured statewide assessment, training, and incident response capabilities. The Department of Administrative Services (DAS) Office of Information Security and Privacy (OISP) has also modernized core security infrastructure, established statewide security standards, and was recently recognized by the National Association of State Chief Information Officer's (NASCIO) with a Cybersecurity Award for the State of Ohio's Agentic Security Operations Center (SOC), highlighting Ohio's leadership in forward-leaning, AI-assisted operational security.

Ohio's fraud-prevention posture has similarly strengthened. State agencies have prevented and recovered hundreds of millions of dollars across human services, taxation, and workers' compensation programs, while the InnovateOhio Platform now manages over eight million OHID identities and operates the also NASCIO-recognized OHID Fraud Detection and Reporting (FDR) system. Ohio has launched Positive Pay in partnership with the Treasurer and the Office of Budget and Management (OBM), modernized vendor-risk controls, and integrated cross-agency identity validation capabilities. These achievements demonstrate maturing enterprise discipline, deeper collaboration across agencies, and a growing ability to identify and prevent sophisticated fraud attempts.

Building on this strong foundation, the Cybersecurity and Fraud Advisory Board recommends several key next steps to continue Ohio's upward trajectory. In cybersecurity, Ohio should accelerate adoption of continuous identity-risk management, advance readiness for post-quantum cryptography, and expand whole-of-state support for local government resilience. In fraud prevention, Ohio should increase cross-program detection capabilities for online government services, adopt OHID Business-Entity Verification statewide, and develop a centralized enterprise fraud detection engine capable of real-time anomaly identification across multiple agency programs. Together, these forward-looking actions chart a clear roadmap for continued statewide improvement strengthening security, safeguarding public trust, and ensuring Ohio remains a national leader in cybersecurity and fraud prevention.

Cybersecurity

Current State Observations

The Ohio Comprehensive Cybersecurity Plan (OCCP) is a two-year strategic roadmap outlining Ohio's whole-of-state framework, managed by CyberOhio and the OCCP Executive and Planning committees. The plan outlines goals in several areas including State and Local Cybersecurity Grant Program (SLCGP) administration, supporting local governments, and strengthening cybersecurity practices across state agencies and across critical infrastructure entities.

Independent cybersecurity assessments over the past three years show consistent progress in executive branch agencies reaching a 'repeatable' tier of maturity in industry-recognized frameworks. Significant state investments include cutting-edge workforce and citizen-facing application defenses, deploying free phishing simulations, network security services, 24/7 monitoring, and security operations center services across all 88 County Boards of Elections via the Secretary of State's Cyber Defense Team, and administering federal SLCGP funds towards municipal .gov domain migrations and software modernizations. Operational resources like the Ohio Cyber Integration Center, the Ohio Cyber Reserve, and the Ohio Persistent Cyber Improvement Program actively assist local governments and critical infrastructure operators. However, user identity has become the state's new security perimeter, and emerging technologies like artificial intelligence and quantum computing introduce urgent vulnerabilities.

To address these risks and improve the state's resiliency to cyber disruption, the Board recommends:

1. Maintain a Strong and Adaptive Continuous Identity Risk Management

Balancing ease of access and cybersecurity is a moving target. In 2019, Governor Mike DeWine established the InnovateOhio Platform (IOP) to foster the growth of customer-centric digital interactions between agencies, Ohioans, businesses, and visitors. One area of focus for IOP is the establishment and maintenance of a common, secure digital identity for the state workforce and Ohioans. IOP also promotes secure data and analytics sharing across state programs and agencies to better serve the public. To further evolve identity management, the state should adopt a continuous identity risk management framework. One that dynamically evaluates user, device, and machine trust throughout the entire session rather than just at initial login. Key steps to advance to this maturity level include:

- 1.1 Continue existing efforts to require multifactor authentication (MFA) on all human based accounts, strengthening identity-proofing¹, centralized governance, and adaptive access

¹ The process by which a Credential Service Provider (CSP) collects, verifies, and validates identity information about an applicant to ensure that the claimed identity exists in the real world and that the person presenting the claim is indeed that specific individual before issuing credentials.

- controls while prioritizing phishing-resistant MFA², privileged-access management, and just-in-time privilege elevation³ for all high-risk roles.
- 1.2 Apply the same discipline to accounts used by software, automated systems, and AI tools as to human-based accounts. Enable the secure adoption of agentic AI⁴ by implementing safeguards that ensure agents can only act within approved boundaries.
 - 1.3 Continue aligning identity platforms and domain structures across state agencies to establish identity as a shared security foundation.
 - 1.4 Requiring mandatory integration of OHID Business-Entity ID verification across state suppliers, grantees, authorized providers, business licensing, tax filers, and related state-business platforms to counter nationwide surges in business identity theft and synthetic entity creation.

2. Accelerate Post-Quantum Cryptography Preparedness and Cryptographic Agility

Quantum computing is an emerging technology that represents a fundamental shift in how information can be processed. Simply stated, quantum computing allows systems to evaluate and solve complex problems dramatically faster than conventional computers. As the technology matures, these capabilities will threaten current encryption methods that secure sensitive data, online transactions, and digital communications. Adversaries have already begun capturing encrypted information with the expectation that future quantum computers will be able to break the encryption algorithms protecting it, a tactic known as “harvest now, decrypt later.” Once attackers gain access to quantum-capable systems, any organization still relying on traditional public-key encryption could face serious risks, including impersonation of trusted services, tampering with digital systems, and exposure of confidential information.

The DAS Office of Information Security and Privacy (OISP) established a multi-agency Post-Quantum Cryptography (PQC) Task Force in 2025, which delivered recommendations in the Spring of 2026. The task force determined the state is steadily progressing towards crypto-agility⁵ and quantum-safe readiness. Several workstreams are already in motion including vendor due diligence, inventorying cryptographic assets statewide, updating policies and standards to include PQC requirements, and multiagency training efforts. The state’s focus is on building cryptographic agility by using modular techniques to easily rotate algorithms. This approach protects the

² Phishing-resistant MFA uses cryptographic keys tied to the application one is authenticating to, making credential theft structurally impossible, whereas traditional MFA relies on shared codes or prompts that attackers can intercept or trick users into giving away

³ An identity management strategy where elevated or administrative rights are granted strictly on a temporary basis for a specific approved task, then automatically revoked immediately upon task completion to minimize standing privileges.

⁴ Agentic AI refers to artificial intelligence systems that can make decisions, plan tasks, use tools, and take actions on their own with very little help from people, so they can achieve complex goals.

⁵ The ability of an information system, application, or protocol to rapidly change or switch cryptographic algorithms, key lengths, and parameters without requiring fundamental changes to the underlying infrastructure or application logic.

confidentiality of state data against future threats without requiring applications to be completely rewritten. The federal government's standards body has set 2030 as the year after which today's encryption should no longer be used for new systems, and 2035 as the year it must be retired entirely.

The Board recommends building upon these efforts by:

- 2.1 Continuing efforts to mandate a completed statewide cryptographic asset inventory.
- 2.2 Accelerating adoption of National Institute of Standards and Technology (NIST)-standardized quantum-safe algorithms and integrating crypto-agility into the software development lifecycle to enable rapid algorithm rotation as standards evolve while prioritizing remote access systems, networks, critical authentication systems, and applications providing public-facing services or containing confidential information with retention schedules extending past 2030 in order to mitigate harvest now/decrypt later risks.
- 2.3 Requiring technology vendors, as part of state contracts and renewals, to show their plan and timeline for moving to quantum-safe encryption.

3. Expand Whole-of-State Efforts and Local Government Support

State agencies and local governments work together to support Ohio's communities. Local government entities across the United States face a world of threat actors many of whom are well organized and funded. Whole-of-State Cybersecurity is a recent strategy many US States and Territories are taking that aligns state agencies, local governments, educational institutions, and critical infrastructure under a shared defense framework to protect digital infrastructure and public data. It is not a one-size-fits-all solution, and Ohio has established itself as a model example with several whole-of-state efforts taking shape over the last several years with a combination of state funding and federal grant funds.

The Ohio Cyber Integration Center, a joint effort between Ohio Homeland Security and The Adjutant General's department was established in 2024 to provide a central resource to promote information sharing and coordinate incident response efforts across the state. The Ohio Persistent Cyber Improvement Program, a SLCGP federal funded initiative led by the University of Cincinnati, provides free cybersecurity training to over 30,000 local government employees. In 2019, the Ohio Cyber Reserve was established as a volunteer cyber force under command of The Adjutant General and has grown to over 200 members dedicated to incident response, cybersecurity education and outreach, and performing cybersecurity assessments for local government entities and critical infrastructure operators throughout the state. These capabilities, the coordination efforts of CyberOhio, and the partnerships with existing state agency cyber resources have established a mechanism to support the whole-of-state approach to cybersecurity maturity, information sharing, and preparation and response to cyber incident disruption.

To continue Ohio's whole-of-state strategy, the Board recommends:

- 3.1 Scaling and expanding operations to ensure state-level cybersecurity resources, incident response capabilities, and maturity assessments continue to be freely available to local political subdivisions.
- 3.2 Supporting Regional Security Operations Center⁶ models that pool threat intelligence, cybersecurity and technology tools and services, and specialized security operations staff to simultaneously protect local government entity networks while offering clear technical career progression.

Fraud Prevention

Current State Observations

Ohio's fraud prevention capabilities feature strong multi-agency wins, including the launch of Positive Pay by the Ohio Treasurer and the Ohio Office of Budget and Management in November 2025. This fraud prevention system verifies supplier check details against issuer records to detect alterations, counterfeits, and unauthorized transactions in near real-time. Additionally, in state Fiscal Year 2023, over \$59M in fraudulent tax disbursements were prevented by the Ohio Department of Taxation, \$17 million across income and business taxes. During the same timeframe, the Ohio Bureau of Workers' Compensation recovered more than \$700,000 and prevented another \$73 million, along with over \$180M recovered or prevented across unemployment benefits and Supplemental Nutrition Assistance Programs by the Department of Job and Family Services. Additionally, DAS IOP manages over eight million OHID user identities and operates the NASCIO-awarded OHID Fraud Detection and Reporting system. Vendor contract language was also updated to mandate contractor fingerprinting, background checks, and other insider threat safeguards for critical suppliers. Furthermore, the Auditor of State has provided guidance that local government entities should guard against fraudulent financial transfers by increasing verification steps with payees including in-person validation. Despite these efforts, agencies are vulnerable to synthetic identity fraud and complex business process manipulation.

To address these risks and improve resiliency to fraud and abuse of state resources, the Board recommends:

4. Adopting Statewide Fraud Prevention Principles:

- (1) Monitoring fraud builds public trust beyond dollar returns;
- (2) Prevention investments should be proportionate to risk and potential losses, recognizing deterrent and public-trust value beyond direct dollar returns.;
- (3) Public administrative burdens must be minimized;
- (4) Investments by one agency can yield cross-agency benefits; and

⁶ A centralized security operations facility designed to aggregate security monitoring, threat intelligence sharing, log analysis, and incident response across multiple public sector entities (such as local municipalities, school districts, and county agencies) within a defined geographic region to pool resources and lower operational costs.

(5) Detection must connect to investigation, referral, prosecution, and recovery so that identified fraud is acted on, not only blocked.

5. Formalize and Extend Current Operational Programs and Analytics Data Sharing Within Legal Limits That Identify and Prevent Fraudulent Activity Across State Systems and Services.

In 2026, Ohio established a statewide data sharing compact, a framework that enabled state agencies to share information while addressing privacy, security, and emerging threats in a consistent way. This compact simplifies and streamlines the state's ability for authorizing cross-agency data sharing. Additionally, the OHID state online identity service, with its eight million OHID user identities and Fraud Detection and Reporting System, can serve as a foundation to build out a centralized statewide fraud detection engine.

Leveraging this new data sharing framework, the Board recommends the state:

- 5.1 Require every agency under the Governor's authority to participate, and invite the statewide elected offices, the General Assembly, the courts, and public colleges and universities to join by agreement in the Ohio Statewide Data Sharing Compact (grounded in ORC 125.32 and supported by the DAS Office of Data and Efficiency).
- 5.2 Establish an automated and centralized state fraud detection engine leveraging advanced analytics with high-value datasets such as payments, supplier records, identity attributes, eligibility data, and licensing records to assess and prevent fraudulent activities in real-time and allow for referral for prosecution.
- 5.3 Continue efforts to enforce statewide data governance, including data quality, timeliness, and baseline sharing requirements to improve cross-agency fraud visibility.

6. Continue to Build Trust in Fraud Prevention Services by Implementing Strong Privacy Protections

Critical to the state's operations is public trust in the services it provides. Efforts to reduce cyberfraud help to establish that trust when done responsibly. The Board recommends that efforts to implement privacy protections extend to all recommendations made in this report, specifically:

- 6.1 Limit the use of fraud prevention data to fraud prevention programs. Do not allow sharing of anti-fraud data with state agencies and other entities for purposes other than fraud prevention unless authorized by law.
- 6.2 Enforce data minimization, collecting only the identity data necessary to identify fraud risk and retaining it only as long as required for the assessment, any appeal, and any resulting investigation or prosecution, under approved records-retention schedules.
- 6.3 Require human review before taking actions identified in an automated process that will result in an adverse effect relating to a public right, benefit, finding, or determination such as a denial of a license, permit, or public benefit.

- 6.4 Ensure formal processes exist for individuals to review, challenge, and correct inaccurate data and to appeal determinations based on false positives. Notify individuals of their review and appeal rights.
- 6.5 Limit access to anti-fraud data and systems to those working in anti-fraud and cybersecurity work by implementing role-based access controls ⁷ and automated monitoring and recording of access to fraud prevention data.

State Workforce Capacity and Risk Reduction

Current State Observations

Specialized skill shortages persist in areas like artificial intelligence risk monitoring, cloud security engineering, investigative analytics, and cyberfraud prevention. While programs like the state's IT Apprenticeship Program create valuable entry points, systemic investments and partnerships are necessary to expand technical capabilities across both state and regional public entities.

Separately, in recent years Ohio has significantly advanced its insider threat prevention posture. The state implemented contractor fingerprinting and background check requirements, strengthened identity validation during onboarding, and expanded training through the annual Securing Ohio statewide awareness program that now includes an Insider Threat module. Additionally, DAS OISP published formal cybersecurity guidance, providing agencies with concrete procedures for vetting, hiring, contractor oversight, monitoring user activity, and reporting suspicious behavior to mitigate Insider Threat risks.

7. Increase Protection Against Insider Threats

In 2025 DAS OISP established a statewide Insider Threat Prevention Task Force to investigate the current state of maturity in mitigating and detecting Insider Threats among the state workforce and make recommendations to further address these risks. Insider threats are a risk, whether intentional or negligent, to the security and privacy of state data. Many steps have been taken due to the recommendations of the Task Force, but to continue to address these risks the Board recommends the state:

- 7.1 Establish a statewide Insider Risk Management program to centralize insider risk detection, behavioral analytics, anomaly investigation, and governance. This program would provide structured workflows, standardized reporting, and coordinated response mechanisms.
- 7.2 Enhance organizational capacity to manage contract workers. This capacity ensures there is a management role and responsibility within agencies to manage onboarding, offboarding, access, and other worker activities.

⁷ An access control model where system access permissions are granted to users based strictly on defined organizational roles or job functions.

- 7.3 Continue to expand the Securing Ohio training with role-based modules for privileged users, managers, procurement teams, and third-party oversight roles. This would include incorporating scenario-based exercises that replicate insider data exfiltration, sabotage, misuse of privileged accounts, and contractor access violations.

8. Expand State Workforce Staff with Specialized Capabilities in Technology Systems and Cyberfraud Prevention and Investigation.

The Ohio Digital Academy was launched to build a skilled workforce ready to meet the advancing technology and cybersecurity needs of Ohio’s public and private-sector employers. Since then, the program has evolved into the IT Apprenticeship program that is designed to address recruitment and retention challenges in the IT field, close skill gaps through structured training and experience, and provide employees with a defined and supported career path leading to full-performance IT classifications with the State of Ohio. The state also partners with career-technical centers to employ high school seniors and graduates in IT career fields. The state has established a career path for these students to eventually be hired as IT Apprentices and ultimately full-time IT professionals. To further this success, the Board recommends:

- 8.1 Establishing fraud analytics training programs to grow skillsets within the current state workforce and to maintain skills into the future.
- 8.2 Scaling technical apprenticeships and specialized academies by expanding recruitment for the IT Apprenticeship Program and building formal higher-education partnerships to maintain a continuous, skilled talent pipeline in high-demand cyber and analytics fields.

Conclusion

The Cybersecurity and Fraud Advisory Board submits this report on [Report Delivery Date], reflecting the Board's commitment to strengthening Ohio's digital resilience and safeguarding state data. Over the past several years, Ohio has built a modern cybersecurity and fraud-prevention foundation anchored in enterprise governance, statewide collaboration, and disciplined program execution. These efforts now position the State not only to sustain its progress but to advance into the next phase of maturity with confidence and clarity.

The recommendations outlined in this report are intended to guide Ohio's continued evolution: enhancing identity-centric protections, preparing for quantum-era cryptographic threats, extending statewide support to government entities, maturing fraud-detection capabilities, and deepening enterprise data sharing and governance. Together, these actions form a forward-looking path that reinforces the State's commitment to secure, reliable, and trusted digital services for all Ohioans.

The Board looks forward to the ongoing collaboration between State leadership, agencies, and partners as Ohio continues to strengthen its cyber readiness and fraud prevention capabilities.

Cybersecurity and Fraud Advisory Board Representatives:

- Chair and Interim State Chief Information Security Officer, Matt Hemker
- CyberOhio Administrator and appointee of Governor Mike DeWine, Lexie Meade
- Chief Information Security Officer, Ohio Attorney General, Joe Cossin
- Deputy Chief Information Officer, Auditor of State, Ron Rollo
- Chief Information Security Officer, Secretary of State, Jason DeBord
- Chief Risk Officer, Treasurer of State, Joe Bell