Florida Technology MAGAZINE
2026 Legislative Issue

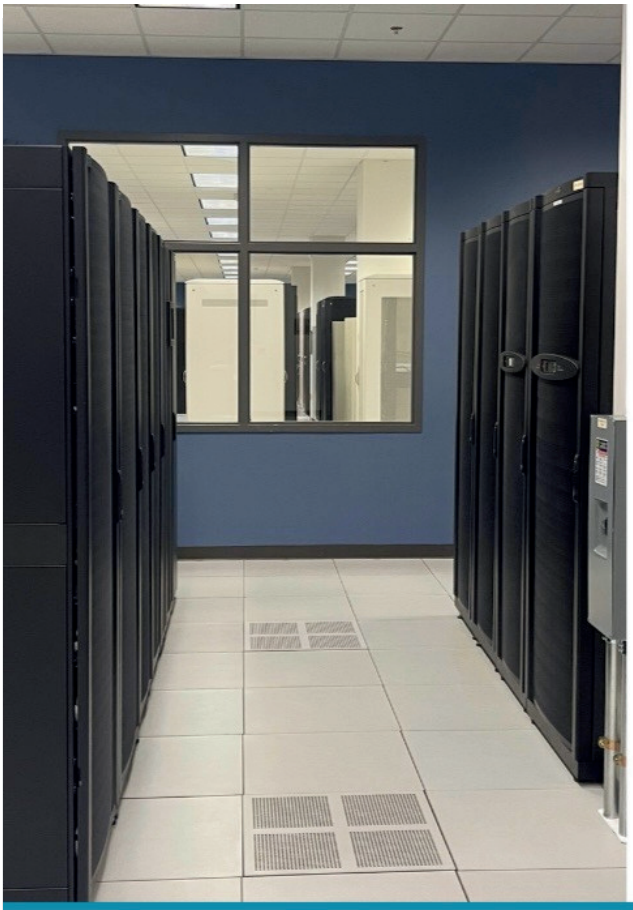


FLORIDA HOUSE DECLARES WAR

"We will fix the procurement and management of IT."

Representative Fiona McFarland

Chair House Information Technology Budget & Policy Subcommittee



NWRDC
FLORIDA'S CLOUD BROKER

NORTHWEST REGIONAL DATA CENTER

Powering Florida's Public Sector with Trusted, Secure, and Cost-Effective Technology Services

Navigating procurement should not stand in the way of progress. NWRDC offers a seamless, compliant, and streamlined path for Agencies to access the technology services they need-without delays, complex solicitations, or procurement hurdles.

WHY AGENCIES **CHOOSE NWRDC**

STATEWIDE MISSION & ACCOUNTABILITY

As a public, not-for-profit service organization, NWRDC is committed to supporting Florida's Agencies with transparent pricing, cost-recovery operations, and long-term partnership.

FASTER TIME-TO-SERVICE

With established agreements and standardized service catalog offerings, Agencies can onboard faster, predict costs, and reduce administrative burden.

COMPREHENSIVE TECHNOLOGY SERVICES

From cloud hosting (Azure, OCI, AWS, Google, private cloud) to managed storage, virtualization, cybersecurity services, data protection, networking, and more, NWRDC provides scalable and dependable solutions built for government.

COMPLIANCE YOU CAN TRUST

NWRDC meets Florida statutory data center requirements and supports Agency compliance needs across security, audit, and operational standards.

PROCUREMENT MADE SIMPLE. TECHNOLOGY MADE DEPENDABLE.

CONTACT US TODAY

info@nwrdc.fsu.edu
https://www.nwrdc.fsu.edu/

Contents

2026 Legislative Edition

Florida Technology MAGAZINE

04

BUILDING SUSTAINABLE AI OPERATIONS IN GOVERNMENT: LESSONS FROM THE FIELD

By Paul Richards, World Wide Technology

7

DIGITAL PUBLIC SERVICE REDEFINED: CLOUD CRM AND AGENTIC AI AT WORK

By Nethaji Kapavarapu, Kyra Solutions

13

CHARTING A COURSE THROUGH AI'S MURKY WATERS

By Randy Phares, Akamai

16

MAKING GOVERNMENT WEBSITES WORK FOR EVERYONE: A 2026 ACCESSIBILITY ROADMAP

By Adrian Esquivel, TECKpert

20

FROM PRISON WALLS TO SILICON VALLEY CALLS: A STORY OF TECHNOLOGY AND TRANSFORMATION

By Perservere

22

MODERNIZATION STARTS WITH A CLEAR STRATEGY

By The Florida Technology Council

25

HACKING HUMANS: HOW TO DEFEND AGAINST YOUR BIGGEST CYBER RISK

By Proofpoint

30

MODERNIZE OR FALL BEHIND: FLORIDA'S CRITICAL TECH CROSSROADS

By David Clark, MyGovGuide

34

USING THE OPEN GROUP ENTERPRISE ARCHITECTURE FRAMEWORK TO ACCELERATE STATE DIGITAL TRANSFORMATION

By Dr. Darren Pulsipher and Hugues Morin, Intel Corporation

37

TRUSTED AI GOVERNANCE: FLORIDA'S PATH FORWARD A FRAMEWORK FOR STATE LEADERS TO BALANCE INNOVATION AND RESPONSIBILITY

By Leanne Lapp, IBM

39

PROTECTING TRUST AT THE SPEED OF RISK: WHY MODERNIZATION MATTERS

By Stephen Walsh and Chris Montgomery, Slalom

42

PROTECTING TRUST AT THE SPEED OF RISK: WHY MODERNIZATION MATTERS

By Ernie Sanders, Peraton

Florida Technology Magazine

PUBLISHER: Florida Technology Council
EDITOR: James Taylor
DIRECTOR OF MARKETING: Ava Lamberti

FLORIDA TECHNOLOGY MAGAZINE is a triannual publication provided as a joint venture between nonprofits, the Florida Technology Council and the Florida Technology Foundation.

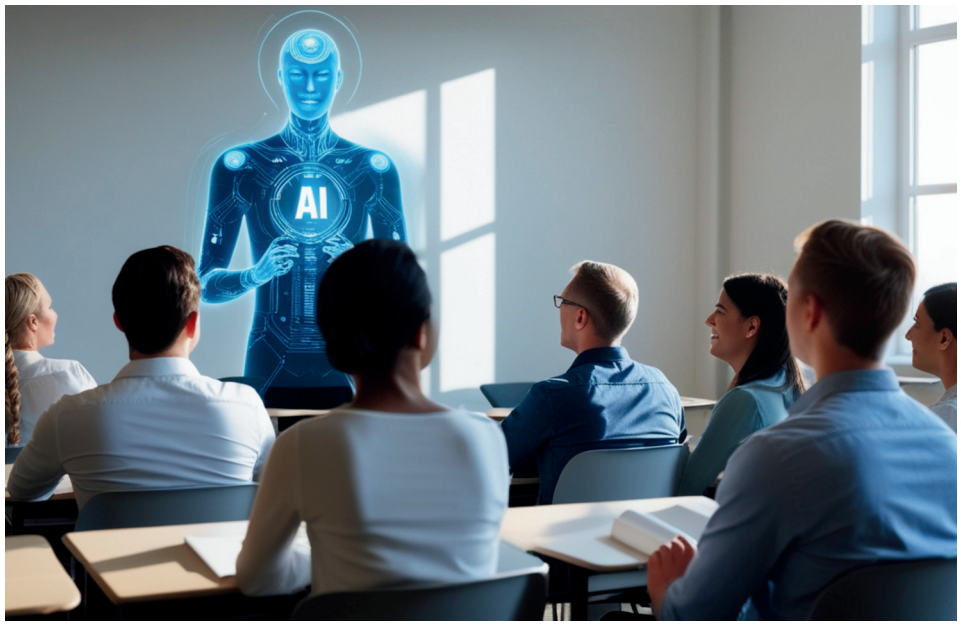
PRICE: FLORIDA TECHNOLOGY MAGAZINE is an educational resource provided at no cost for Florida legislative and agency leaders. It is available digitally and free of charge to all recipients. This magazine is not for sale and adheres to Florida's State gift ban statutes, ensuring compliance with all ethical standards.

EDITORIAL RESPONSIBILITY STATEMENT: Florida Technology Magazine publishes contributed content in good faith. All statements, facts, and representations are the sole responsibility of the contributing author. Florida Technology Magazine, the Florida Technology Council, and the Florida Technology Foundation assume no responsibility for errors, omissions, or inaccuracies, and disclaim liability for any actions taken in reliance on such content.

Building Sustainable AI Operations in Government: Lessons from the Field

*By **Paul Richards**, Client Services Executive, World Wide Technology*

The AI adoption wave is hitting state government with full force. Over the past two years, I've watched agencies across Florida begin their AI journeys - deploying chatbots, analytics tools, and automation systems at different paces and with varying levels of operational readiness.



Getting AI working? That's the "easy" part. Agencies can launch proofs-of-concept and demonstrate capabilities in months, not years.

The hard part is operating AI sustainably. Turning experiments into production infrastructure. Building operational discipline that lets you run AI systems reliably for years, through leadership transitions and budget cycles.

This is where I'm seeing a consistent pattern emerge among successful agencies.

The Two-Phase Approach: Prove Value, Then Scale

Ask any agency leader and they'll describe the same reality: budgets aren't growing, but citizen expectations are. When the legislature is actively discussing AI policy, when citizens demand digital-first service delivery, when peer agencies announce initiatives - you need momentum.

Successful agencies take a phased approach. First, they demonstrate AI value quickly to build organizational buy-in and secure resources for long-term investment. Then, they use that momentum to build the operational maturity that makes AI sustainable at scale.

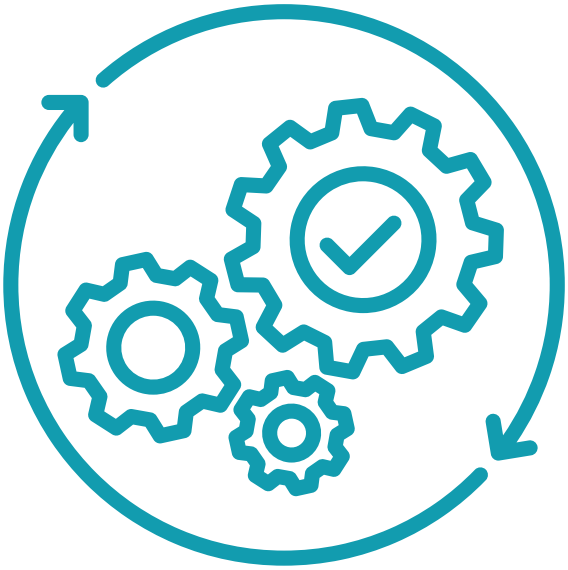
This is exactly what's happening at Florida Department of Corrections. They proved their chatbot concept rapidly, delivered visible wins, and built confidence across the organization. Now they're strategically building the foundation for sustainable operations.

Ken Kicia, CIO at Florida Department of Corrections, reflects on their evolution: "We prioritized speed to delivery over perfection and deprioritized some steps in the planning process. And while our first chatbot was functional, we lacked visibility into how it worked. Different people knew different pieces, but nobody had the complete picture of the architecture. We couldn't accurately track costs. We didn't have proper monitoring in place. And when something broke, like losing connectivity to our policy library, troubleshooting was a long and tedious process. We figured it out... eventually."

This is the reality of effective AI adoption in government - prove value fast to secure commitment, then build for scale.

It's how successful agencies operate: demonstrate capability, learn what's required, then architect for sustainability.

The agencies that succeed long-term are the ones that recognize when it's time to invest in operational foundations.



Key Pillars of Operational Sustainability

Working with agencies across Florida, I've identified key operational pillars that distinguish sustainable AI implementations from science projects.

Data Readiness

AI is only as good as the data it runs on. Before scaling any AI system, you need clean, structured, accessible data with proper governance frameworks in place. This means assessing data quality, establishing data pipelines, and ensuring integration across systems. Without solid data foundations, even the most sophisticated AI will fail.

Visibility

You need to understand your architecture end-to-end, track actual costs with monitoring data, and have real-time performance metrics that catch degradation before systems break. If you can't explain how your AI system works or what it costs to run, you're not operating it sustainably.

Platform Thinking

Smart agencies leverage enterprise platforms that integrate with existing technology investments. This reduces technical debt and creates secure, scalable environments for rapid AI development. At FDC, this approach is evolving their chatbot from simple policy search into a platform supporting voice interfaces, mobile apps, Teams integration, additional data sets, and enhanced analytics.

Predictable Scaling

Structured scaling frameworks that create predictable timelines and costs are essential. When new use cases emerge, you shouldn't start every conversation with "let me get back to you on scope." Agencies need approaches that assess readiness, plan scalable solutions, and deliver measurable value at each maturity stage.

Production-Grade Governance

Integrating governance and security from the start ensures AI systems are built to last. Scheduled maintenance, regular updates, budget forecasting, incident response procedures - this operational discipline separates infrastructure from science projects.

Why Chatbots Matter

Chatbots are emerging as an easier AI entry point. They're accessible, measurable, and deliver visible results quickly - perfect for the "prove value fast" phase.

Ken's experience validates this: "The benefits show up quickly. Reduced call volume, faster and higher quality responses, and staff capacity reclaimed for higher-value work. These aren't theoretical. They become visible within weeks of deployment."

The deeper insight: operational lessons learned with chatbots transfer directly to every other AI application. Agencies that master these pillars with chatbots are building muscle for everything that follows. The technical sophistication isn't solely in the AI model itself - it's also in the operational architecture that makes AI sustainable.

The Real Advantage

The competitive advantage in AI adoption isn't being first to deploy or having advanced algorithms. It's operational maturity - the ability to run AI

→

systems reliably, scale them predictably, and sustain them through budget cycles and leadership transitions.

Agencies with operational maturity deliver high quality services without adding headcount, have predictable costs, and build organizational AI literacy. And they do it on timelines that matter: months, not years.

Where This Goes Next

Florida agencies are navigating a crucial inflection point. As the legislature actively discusses AI policy, forward-thinking agencies aren't waiting for mandates - they're building operational maturity now.

Citizens expect digital-first service delivery. Budget constraints remain unforgiving. Agencies like FDC that prove value quickly, then invest strategically in operational foundations, are positioning themselves for long-term success.

This approach requires treating AI systems like critical infrastructure from day one of the scaling phase. It demands operational discipline that isn't glamorous but is essential for sustainability.

When agencies figure out this two-phase approach and share those lessons openly, others can accelerate their journeys. This is how technology adoption should work: peer learning, transparent sharing, and collaborative problem-solving.

The future of AI in government isn't only about futuristic capabilities. It's also about operational maturity applied to new technology.

Or as Ken puts it:
"Do more with less. That's just good management."

About the Author

Paul Richards *is a Client Services Executive at World Wide Technology, partnering with Florida state agencies on AI adoption and technology modernization.*





Digital Public Service Redefined: Cloud CRM and Agentic AI at Work

By ***Nethaji Kapavarapu****, Technology Leader in Public-Sector Digital Transformation at Kyra Solutions*

Modernization in government is no longer a distant goal; it is a pressing need today. Citizens now expect fast, transparent, and personalized digital services, while agencies face rising demands for security, compliance, accessibility, and accountability. Meeting these expectations requires more than putting forms online; it demands a new model that integrates people, processes, and technology. Drawing from my experience architecting statewide digital platforms across public-sector agencies, I have seen how Cloud CRM and Agentic AI redefine service delivery at scale.

Cloud CRM and Artificial Intelligence, specifically Agentic AI, are transforming government operations by enabling scalable, secure, and cost-efficient services. AI agents automate approvals, send proactive alerts, answer FAQs, and provide real-time updates, reducing call volumes and turning days of work into hours. Cloud CRM portals let citizens apply for benefits, renew licenses, and track requests online, allowing staff to focus on cases that require human judgment.

This article highlights how Florida can modernize public services through Cloud CRM and Agentic AI while keeping citizens at the center. In Florida, several agencies have begun implementing Cloud CRM solutions across education, health, financial programs, and public engagement. At the same time, other states, including Rhode Island, Colorado, Georgia, Ohio, New Mexico, New Jersey, and Illinois, have already adopted these platforms to modernize licensing, permitting, inspections, grants, and long-term care, achieving significant gains in efficiency, transparency, and cost savings.

Cloud CRM and Agentic AI: The New Backbone of Public Services

Cloud CRM solutions centralize constituent data, unify workflows,

and streamline administrative processes. With standards-driven architectures, they enable agencies to uphold federal and state compliance mandates while delivering accessible, user-centered digital services. The results are impressive:

- **50-70% faster deployment of new programs and service delivery portals**, enabling agencies to launch digital services in a couple of months instead of a year and deliver improvements to citizens much sooner.
- **Up to 60% automation of routine approvals, verifications, and escalations**, reducing delays, minimizing manual workload, and ensuring cases move forward even during peak demand.
- **25-40% increase in staff productivity and case throughput,** as employees shift from repetitive tasks to higher-value work, resulting in faster responses and reduced backlogs across programs.

Cloud platforms accelerate modernization by replacing agency-specific systems with shared components like login, case management, and payment modules that can be reused statewide. This speeds up deployment, improves consistency, and consolidates legacy workflows into a single CRM system, reducing redundancy and enabling cross-agency collaboration.

Standardization strengthens secure data migration, interoperability, and partner integration, allowing legacy upgrades while preserving historical data and delivering a unified citizen experience.



Modernization also relies on people. Public servants need intuitive tools, and residents need accessible services. Streamlined workflows reduce handoffs, remove redundancies, clarify accountability, and move applications through a single automated process—improving transparency and reducing delays.

The Role of Agencies and Technology Partners in Ensuring Secure Modernization

Security and trust remain the foundation of every digital modernization effort in government. As guardians of citizen data, state agencies must meet rising expectations for privacy, compliance, and resilience while delivering services that feel as seamless as the best digital experiences in the private sector. In my role as a leading expert in Cloud CRM and AI-driven system design I architect statewide digital platforms that modernize public services and enhance government operations. I see firsthand how this balance is achieved when agencies and technology partners collaborate around secure, scalable Cloud CRM and Experience Cloud platforms, which are built on FedRAMP-secure platforms, support accessibility, configurable permissions, role-based access, multi-factor authentication, and detailed audit trails.

Across Florida and other states, leaders are preparing their digital ecosystems for an era shaped by artificial intelligence, predictive analytics, and data-driven decision-making. Cloud CRM environments can quickly incorporate capabilities such as automated eligibility guidance, workload forecasting, and proactive resident notifications. These flexible platforms reduce technical debt and avoid costly rebuilds, helping agencies adapt to natural disasters, regulatory changes, and increasing service demands.

Modernization in government is not just a technology upgrade; **it is an organizational shift led by the public workforce itself.** When technology, redesigned workflows, and human-centered practices align, agencies move beyond transactional service delivery toward greater efficiency, responsiveness, and citizen empowerment. Employees become more engaged as streamlined processes and better tools improve their work, while residents gain faster access to services. This alignment breaks down silos and creates a more collaborative, agile, people-centered government ready for modern demands.

Florida: A Statewide Model for Cloud CRM + Agentic AI

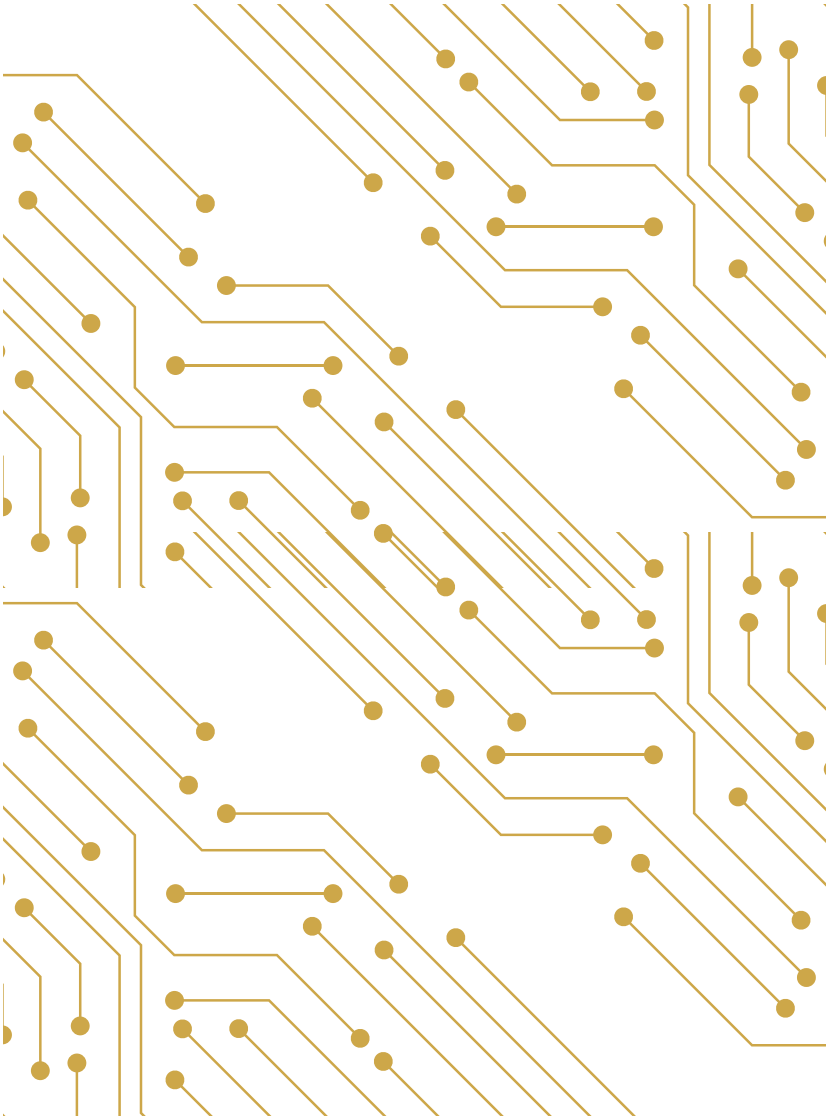
Florida is advancing major Cloud CRM and Agentic AI-enabled modernization efforts, delivering statewide programs that modernize citizen-facing services in the health, education, environmental and financial sectors.

For example, the Florida Prepaid College Board modernized its customer, donor, scholarship, and gifting experiences through unified Cloud CRM platforms supported by intelligent AI assistants. These systems now handle millions of citizen interactions, over $1 billion in annual transactions, and assets exceeding $15 billion, while providing personalized, real-time guidance to families, students, and donors.

In the health sector, the **FRAME program** automated medical education reimbursement workflows, enabling fast, transparent distribution of millions in funding.

The Office of Medical Marijuana Use (OMMU) increased inspection capacity by 40% through unified licensing, compliance, and field-inspection tools powered by Agentic AI–driven workflows.

Florida's Department of Education transformed its School Choice program with an online portal supporting application intake, e-signatures, parent communications, and real-time case visibility, serving over 2 million students and improving transparency for families and educators.

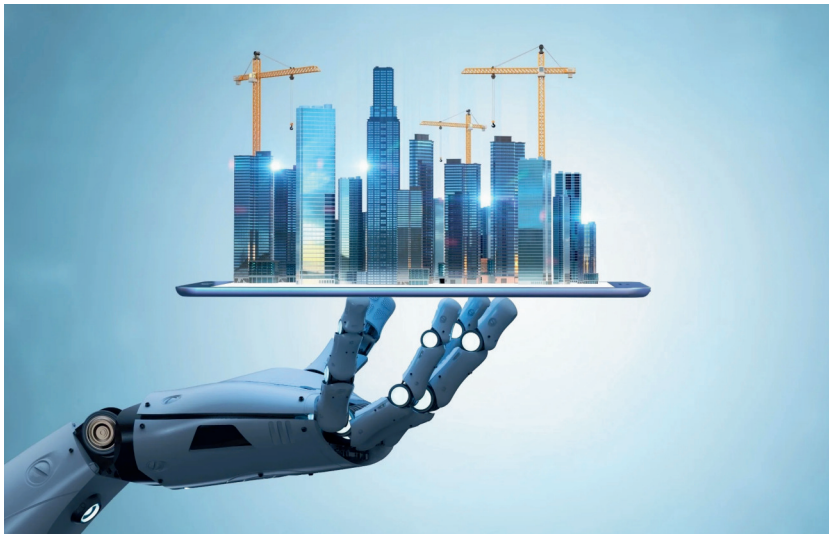


Modernization Success Across the United States

Across the United States, government agencies are modernizing with Cloud CRM platforms, delivering measurable improvements in efficiency, compliance, and citizen transparency.

- **Rhode Island:** The Department of Environmental Management consolidated 36 license types and digitized agriculture and water permits, serving 35,000 residents, processing over 4,000 applications, and improving response efficiency by 85%.
- **Colorado:** Title V air quality permitting and compliance workflows were digitized on a FedRAMP-secure Cloud CRM platform, strengthening data accuracy and regulatory oversight.
- **Georgia:** The Medical Cannabis Commission implemented a unified system for licensing, COA oversight, inspections, and seed-to-sale tracking, supported by mobile tools and real-time dashboards.
- **Ohio:** The Department of Health replaced legacy tools with centralized CRM for long-term care licensing, automating licensure, scheduling, invoicing, and data exchange.
- **New Mexico:** This modernization effort delivered some of the strongest outcomes nationwide, including a 40% reduction in payment reconciliation time for the Medical Board, more than 143,000 applications processed by the Boards and Commissions Division, millions saved by the Alcohol Division through an OTP-based portal that eliminated the need for 60,000+ external user licenses, and a 70% reduction in processing time for the Cannabis Control Division while supporting more than 3,000 license holders.
- **New Jersey:** Advanced cannabis regulation through automated workflows, mobile inspections, METRIC integration, and improved licensee visibility.
- **Illinois:** Modernized cannabis oversight with digitized licensing, integrated compliance tracking, and real-time inspection tools that strengthen regulatory transparency.

Together, these statewide transformations demonstrate how Cloud CRM and Agentic AI implementations are creating a scalable and repeatable modernization blueprint across the nation—delivering faster processing, significant cost savings, stronger compliance, and more transparent citizen experiences.



Cost-Savings Perspective — Why Multi-State Trends Matter

Across states, Cloud CRM and Agentic AI cut costs by eliminating unnecessary licenses, reducing manual labor, and retiring expensive legacy systems. For example, New Mexico saved millions by automating reconciliation and processing, reducing the time required for these tasks. Workforce efficiency also improves as routine jobs are managed through automated approvals, routing, analytics, and mobile inspections.

Citizens see significant improvements, with self-service portals and real-time updates that decrease in-person visits and administrative workload. Shared CRM components and continuously advancing AI capabilities also enable agencies to launch new programs more quickly and at much lower costs than traditional IT projects, making modernization both transformative and economically sustainable.

Steps Agencies Can Take Today with Cloud, CRM, and AI

Modernization is a long-term journey, but agencies can start experiencing benefits right now by capitalizing on Cloud platforms, CRM tools such as Salesforce or Microsoft Dynamics 365, and Agentic AI in real-world applications:

- **Transfer Citizen Services to the Cloud –** Shift high-demand services like benefits claims, license renewals, and permits to cloud-based portals. This provides secure access anywhere, minimizes paper-based processes, and enhances scalability during peak demand.
- **Apply CRM for a Single View of Citizens –** Integrate citizen records into advanced CRM technologies such as Salesforce or Dynamics 365 to do away with silos. One view of engagement enables agencies to respond quickly, cut duplication, and provide more tailored service.
- **Streamline Approvals with Automation –** Integrate CRM workflows with AI-driven automation to automate repetitive verifications, eligibility checks, and routing. This speeds up processing and frees employees to handle intricate cases that require human judgment.
- **Empower Proactive Communication –** Leverage CRM notifications and AI-powered alerts to keep citizens notified of application status, deadlines, or impending eligibility changes and minimize frustration and enhance trust.
- **Modernize Data Migration and Interoperability –** Move legacy data safely into cloud-based CRM systems and establish interoperability standards. AI solutions can help cleanse and map data, ensuring consistency across systems.
- **Enhance Security and Transparency –** Cloud platforms and CRM systems today offer natively built-in encryption, audit trails, and monitoring. Agencies can further leverage AI to identify anomalies, prevent fraud, and publish performance data through public dashboards.

A Forward-Looking Model for Modern Governance

Florida's modernization reflects a significant shift in how government serves residents. Progress happens when technology, people, and redesigned processes work together. Cloud CRM and Agentic AI provide the digital foundation, but public employees who rethink workflows and support citizens turn these tools into real value.

By adopting innovations that improve collaboration, transparency, accountability, and resilience, Florida is increasing efficiency and trust. The state is creating an inclusive and secure digital environment where services are intuitive, responsive, and citizen-centered. This approach shows that modernization is about improving how government works and delivers impact.

About Kyra Solutions

Kyra Solutions has over 25 years of delivering modernizing technology to the public sector across multiple regulatory and service domains. Its client-focused approach and deep domain knowledge help state agencies improve compliance, speed service delivery, and enhance operational efficiency.

About the Author

Nethaji Kapavarapu *is an experienced technology leader and innovator with nearly two decades of industry experience, including 11 years dedicated to public sector modernization. He specializes in enterprise architecture, Cloud, CRM, and AI-driven solutions that deliver citizen-centered services while advancing innovation, compliance, and public trust.*

accenture



For three decades, we've supported Florida's mission across state government, universities, and community partners with secure, compliant delivery and reliable outcomes for residents.

Our Florida-focused teams pair local know-how with national scale—bringing expertise from offices in **Tallahassee, Tampa, Orlando, and Miami**. We modernize essential services, strengthen cybersecurity, and improve customer experiences statewide.

Learn more about Accenture in Public Service



Charting a Course Through AI's Murky Waters

*By **Randy Phares**, Sr. Major Account Executive, Akamai*

The United States does not yet have a single, comprehensive AI law. Instead, a patchwork of federal executive actions and plans (notably America's AI Action Plan and related Executive Orders most recently the executive order signed by President Trump on December 11, 2025), the National Institute of Standards and Technology (NIST) AI Risk Management Framework, and sectoral statutes like the Gramm-Leach-Bliley Act (GLBA) and Artificial Intelligence (AI) at HHS from the Department of Health and Human Services collectively shape AI governance.

At the U.S. state level, there was some momentum with the passing of Colorado's AI Act (Senate Bill 24-205), which was designed to focus on consumer protection against "algorithmic discrimination" from "high-risk" AI systems like housing, employment, and healthcare, and is expected to become law in mid-2026. Importantly, there is no categorical restriction on the use of AI or machine learning for cybersecurity purposes. Instead, the focus is on ensuring that systems are trustworthy, secure, and do not introduce undue risk — principles that align with best practices in security operations.

Now the new Trump order, titled "Eliminating State Law Obstruction of National AI Policy," seeks to establish a minimally burdensome national standard rather than 50 different state regulatory regimes. States would face significant limitations on their ability to regulate AI going forward. Tech policy researchers say the Trump administration cannot restrict state regulation in this way without Congress passing a law, and legal challenges are expected.

While the question of whether a federal authority can block state laws on artificial intelligence is a complex and evolving constitutional issue, Florida has an opportunity to be a national model for shaping state and influencing federal frameworks in AI security governance. Florida lawmakers already plan to sponsor a specific "AI Bill of Rights" to tackle issues like deepfakes, algorithmic bias, consumer protection, data privacy, and transparency with number of proposals:

- Banning local governments from contracting with Chinese-created AI tools
- Preventing AI companies from selling consumer data
- Fortifying anti-deep fake protections
- Allowing parents to access their child's conversations with these chatbots
- Requiring attorneys to certify whether they used AI to write legal briefs
- Prohibiting utility companies from charging Floridians to subsidize data centers
- Allowing local governments to refuse AI data centers
- Preventing AI data centers being constructed construction in agricultural areas

Policymakers can take steps to protect the public from the new technology with a "State AI and Bot Framework" incorporating the same strict "never trust, always verify" policy as human users, requiring continuous authentication, least-privilege access, and real-time monitoring to prevent exploiting gaps in systems, which often struggle with bot-driven attacks mimicking human behavior at scale.

- Establish effective and constant coordination between legal compliance teams and cybersecurity teams to find balanced approaches.
- Implement a tiered assessment program that distinguishes among AI used for citizen-facing decision-making or broad-based "answer anything" type systems (e.g., chatbots), AI used exclusively for threat detection and security-based decision-making, and employee use of AI platforms for content creation or citizen engagement.
  - Require model transparency documentation (e.g., data-lineage maps, validation, and testing reports, etc.) that satisfy specific the specific AI Act and NIST documentation requirements while still protecting proprietary detection logic. From a compliance perspective, "It ain't compliant if you can't prove it!"
  - Adopt privacy-preserving telemetry, such as hashing, tokenization, or differential privacy, whenever possible so security models can ingest high-fidelity signals without processing PII, which can reduce exposure.
  - Establish a continuous monitoring and improvement loop. Align performance monitoring with regulatory mandates for post deployment monitoring, ensuring that drift and false-positive spikes are promptly addressed and documented.
  - Enhanced scrutiny of technology companies with relationships enabling the development of powerful AI by Chinese companies, and their management of AI web traffic, including that from Chinese bots.
  - Mandatory disclosure and approval process for any state systems integrating foreign AI services.

Implementing technological framework in an AI environment involving several key practices:

- Strong Identity Verification: Every entity, human or machine, must be rigorously authenticated and authorized at every access attempt.
- Principle of Least Privilege (PoLP): This foundational security principle ensures that all entities have only the minimum access rights necessary to perform their specific tasks.
- Microsegmentation: GenAI attacks are fast and adaptable, meaning perimeter defenses will likely fail. Dividing the network into small, isolated segments to control lateral movement and enforce granular policies across applications and physical operational technology devices.
- Continuous Monitoring for Applications and API's: All digital traffic and AI behavior are monitored for anomalies in real time, allowing for rapid detection and response to potential threats.
- Firewall for AI: Real-time input/output security for compliance, privacy, and safe generative AI interactions. This security layer protects users interacting with AI from threats like prompt injection, data leaks, and misuse by inspecting both user inputs (prompts) and AI outputs in real-time, using AI to identify malicious patterns, filter sensitive data, enforce policies, and block harmful content before it reaches the user or the model.

> **The time to act with legislative focus is now—before policy gaps become security catastrophes.**

Florida legislators face a critical window to establish leadership in securing AI and bot-driven environments before preventable breaches and unintended outcomes occur. Creating a Florida AI and Bot Framework provides a comprehensive, forward-looking approach that acknowledges the reality of automated entities as both tools and potential threat vectors. By moving beyond hoping AI will be secure by default to actively knowing it is contained by stringent, dynamically enforced guardrails, Florida can protect its digital infrastructure, citizen data, and democratic institutions while still leveraging the benefits of AI innovation.



About the Author

Randy Phares *is an ISC2 Cyber Certified Sr. Major Account Executive supporting the State of Florida at Akamai Technologies. Akamai's core mission is to "power and protect life online", making digital experiences fast, reliable, and secure for billions of users daily by solving complex internet challenges in cloud computing, cybersecurity, and content delivery.*

Making Government Websites Work for Everyone: A 2026 Accessibility Roadmap



By ***Adrian Esquivel****, CEO, TECKpert*

For many Floridians, a government website is the front door to public services. It is where a family signs up for benefits, a small business renews a license, or a resident checks storm information during a fast-moving emergency. When a site is difficult to navigate with a keyboard, a screen reader, or captions, people do not just get frustrated. They get blocked from services.

Accessibility is also moving from best practice to a clear requirement. In April 2024, the US Department of Justice issued a final rule under Title II of the Americans with Disabilities Act that sets WCAG 2.1 Level AA as the technical standard for state and local government web content and mobile apps. For agencies serving 50,000 or more people, the compliance date is April 24, 2026. Smaller entities generally have until April 26, 2027.

The takeaway for leadership is straightforward: accessibility is not a single audit or a one-time remediation project. It is an operating discipline that touches procurement, design, content, development, and ongoing support. Agencies can reduce risk quickly by standardizing design patterns, focusing on the highest impact user journeys, and adding practical checks to the way they publish and release changes.

Use USWDS to Standardize Design and Reduce Risk

One of the most effective accelerators available to government teams is the US Web Design System, commonly called USWDS. USWDS provides accessible components, patterns, and implementation guidance that help teams start closer to compliance before they add custom features. It also reduces one of the biggest cost drivers in government web programs: every site being built as a custom experience with inconsistent navigation, forms, and content templates.

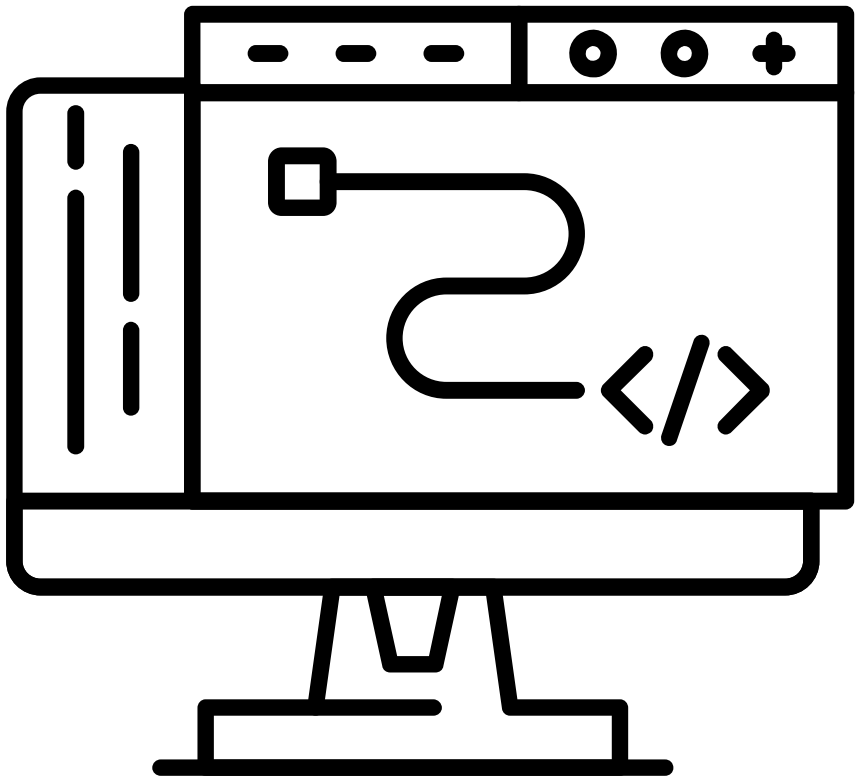
When agencies adopt a shared design system, they do not just make one site better. They create repeatable components for forms, alerts, navigation, and common templates that can be reused across programs. Fix the component once, then apply it everywhere it is used.

The Role of the CMS in Maintaining Standards

A Content Management System (CMS) is the engine that ensures accessibility remains consistent over time. USWDS is platform-agnostic, meaning it can be integrated into both Drupal and WordPress environments, which is a critical advantage for agencies managing a diverse portfolio of sites.

Drupal is particularly well-suited for high-complexity government sites. Its robust architecture allows for a component-based approach, where USWDS patterns are baked directly into the theme. This ensures that even as different departments publish thousands of pages, the underlying structure remains compliant. In Drupal, accessibility is managed at the configuration level, meaning the system can be set up to prevent editors from accidentally breaking the layout or skipping necessary accessibility tags.

WordPress offers similar consistency through purpose-built themes and block patterns. By providing editors with a library of pre-approved USWDS blocks, agencies can limit ad hoc page building. This strategy treats the design system as the single source of truth, ensuring that every new update follows the same accessibility rules as the homepage.



Build Accessibility into the Full Lifecycle

Most accessibility efforts stall because they start with a long list of defects and no way to prevent the same issues from returning. Sustainable compliance comes from repeatable governance and steady execution.

Start by prioritizing based on service impact. Combine automated scans with manual testing, then focus on the top service journeys that residents use most. High-volume pages, forms, and time-sensitive updates usually deliver the biggest return.

Next, remediate shared components first. Templates, themes, headers, footers, search, and form patterns can produce the same defect across hundreds of pages. Fixing the pattern removes defects at scale.

Then, add checks to how work is delivered. Accessibility belongs in definition of done, not as a last-minute scramble before launch. Automated testing, linting, and periodic manual reviews help teams avoid reintroducing old problems.

Do not overlook content. Many failures are not in code. They are in missing alternative text, unclear link labels, poorly structured headings, or uncaptioned video. Short, role-based training for content editors reduces repeat issues.

Consider Accessibility Widgets Carefully

→

Accessibility widgets can offer useful controls for some users, such as text resizing or contrast options. They can also provide a feedback channel. However, a widget is not a substitute for conformant templates, accessible forms, or properly structured content. If an agency chooses to use a widget, treat it as a supplement with governance, testing, and a plan for ongoing maintenance.

Choose Platforms That Support Compliance and Security

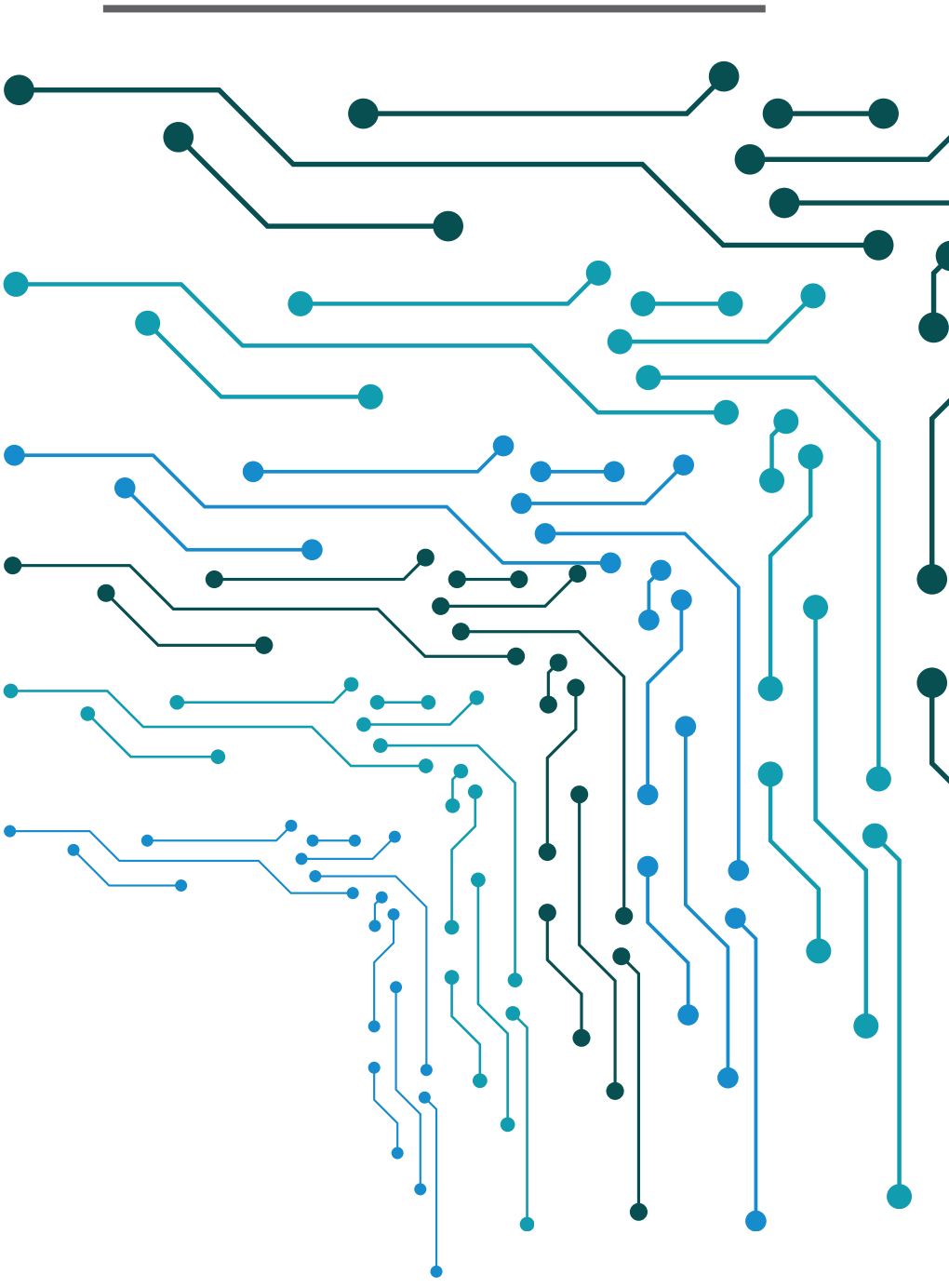
Accessibility and cybersecurity are both pillars of public trust. A site that is accessible but insecure risks data breaches that can harm vulnerable populations; conversely, a secure site that is inaccessible remains unusable. For public sector teams, the most effective way to manage these risks is to host their CMS on a FedRAMP-authorized platform.

FedRAMP authorization ensures that the hosting environment meets rigorous federal security standards. While a secure platform does not automatically make a website accessible, it provides the stable, predictable environment necessary for accessibility tools to function correctly. By utilizing enterprise-grade hosting for Drupal and WordPress, agencies can focus their resources on user experience and content, rather than worrying about the underlying infrastructure or security vulnerabilities that could compromise the service during a crisis.

A Strategic Imperative for 2026

The 2026 and 2027 deadlines represent a turning point for digital experiences in the public sector. For years, web accessibility was treated as a secondary concern, often ignored until a legal challenge arrived. Under the new Title II rule, that era has ended.

Meeting these requirements is a significant undertaking, but it is also an opportunity to modernize aging digital infrastructure. By adopting standardized systems like USWDS and embedding accessibility into the procurement and content lifecycles, agencies can move beyond mere compliance. The goal is to build a digital front door that is truly open to every resident, ensuring that essential services remain reachable by everyone, regardless of how they navigate the web. The roadmap is clear; the time to begin the work is now.





FSU COLLEGE OF COMMUNICATION & INFORMATION

SUPPORTS LOCAL TECH

Community Events

CCI partners with local tech organizations, tech companies, the Florida Tech Council, and state agencies to host events and connect students with employers.

Tech Programs

The College offers several tech programs, including

BACHELOR'S IN INFORMATION TECHNOLOGY

BACHELOR'S IN INFORMATION, COMMUNICATION, AND TECHNOLOGY

MASTER'S IN INFORMATION TECHNOLOGY
RANKED #8 OVERALL, #6 AMONG PUBLIC SCHOOLS, AND #5 FOR VETERANS BY U.S. NEWS & WORLD REPORT

#4
BEST COLLEGES FOR INFORMATION TECHNOLOGY IN AMERICA (PUBLIC)
NICHE 2026

#10
BEST COLLEGES FOR INFORMATION TECHNOLOGY IN NORTH AMERICA
EDURANK 2025

Workforce Contributions

1,324 IT Graduates since 2020
(885 undergrads, 439 master's)

Where they work:

Google, AT&T, amazon, citi, Spotify, RAYMOND JAMES, L3HARRIS, RELIAQUEST, Microsoft, JM Family Enterprises, LOCKHEED MARTIN, Deloitte., gm

Learn more at cci.fsu.edu



ALLEGIANT
STRATEGIES GROUP

Trusted by leading tech companies to connect the dots in Florida

allegiant360.com

From Prison Walls to Silicon Valley Calls: A Story of Technology and Transformation

By Perservere



Each morning at Wakulla Correctional Institution began with the same sounds. Steel doors echoing through concrete corridors. The mechanical count. The steady rhythm of a world where time stood still. For Vincent M. Gordon Delemos, those sounds marked days that blurred together, each one indistinguishable from the last.

As technology evolved at a dizzying pace beyond the prison walls, Delemos watched his future seemingly contract. In a world increasingly driven by digital innovation, he faced the stark reality awaiting many upon release: limited opportunities, skeptical employers, and the weight of a record that often speaks louder than potential.

Today, that same man starts his mornings differently. From his Florida home office, he logs into systems at Vant4ge's Salt Lake City headquarters, where his work as a QA Tester helps shape cutting-edge public safety technology. The transformation wasn't miraculous: it was the result of determination, preparation, and unwavering support.

From Code to Career: Inside the Transformation

Vincent's path to becoming a full-stack developer did not begin with a job offer. It began inside the walls of Wakulla Correctional Institution, where he enrolled in Persevere's intensive 12-month full-stack development program. What started as an introduction to HTML and the basics of coding soon evolved into a transformative process that reshaped his sense of identity, direction, and possibility.

Inside the classroom, Persevere instructors pushed Vincent to think like a software engineer. The program required discipline: daily standups, project sprints, peer reviews, and real-world problem-solving. As the months passed, he built increasingly complex applications while mastering front-end frameworks, back-end architecture, databases, and version control. More importantly,

he developed the professional habits the tech industry demands: persistence, collaboration, communication, and the ability to break down challenges into solutions.

But technical skills alone wouldn't be enough.

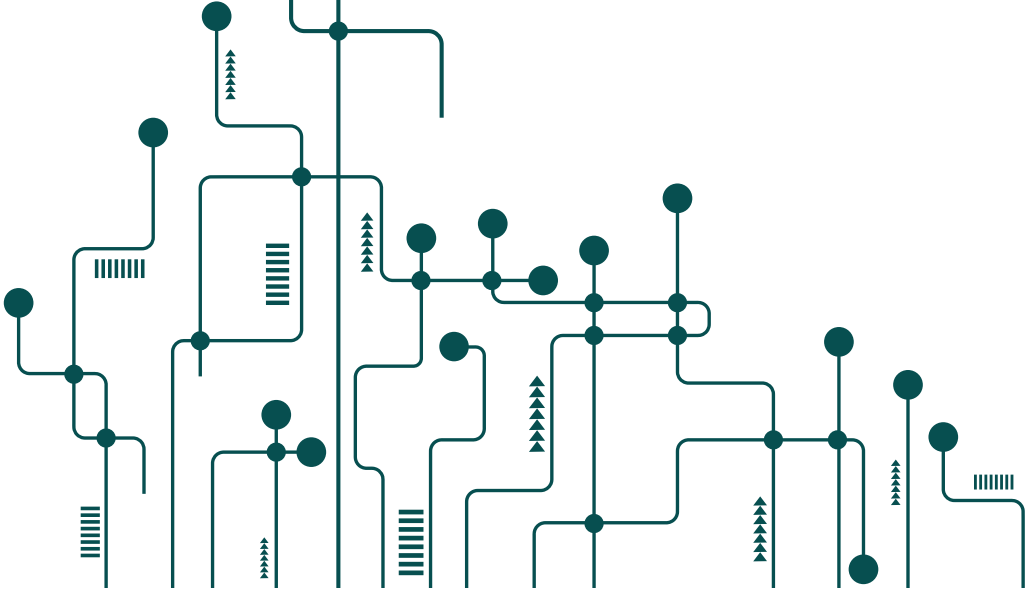
Persevere's model extends far beyond technical instruction. Vincent worked closely with mentors, case managers, and coordinators who helped him prepare for life and work outside the facility. Resume building, mock interviews, career coaching, family reconnection support, and reentry planning ensured he didn't just leave with skills. He left with a roadmap. By the time he graduated, Vincent wasn't simply proficient in code; he was prepared for the expectations, culture, and pace of the tech workforce.

When an opportunity opened at Vant4ge just two months after his release, Vincent was ready.

For Vant4ge, a public safety technology company based in Salt Lake City, Vincent's remote work proved what forward-thinking employers already know: talent isn't limited by geography or history.

"Vincent secured his offer the same way anyone does at Vant4ge: by shipping quality work," explains Sean Hosman, CEO of Vant4ge. "His QA discipline, curiosity, and pace add value on day one. When partners like Persevere prepare candidates with real skills and support, employers get high-performance team members and stronger products."

The numbers tell a powerful story. While Florida's recidivism rate sits at 21.3%, Persevere graduates maintain a rate below 3% nationwide, a stark contrast that speaks to the program's effectiveness. And 87% of graduates secure employment within six months of release, transforming skills into stable careers.



Employers interested in meeting Persevere candidates can contact employers@perseverenow.org or vsit perseverenow.org/employer-info.

"Vincent's achievement shows what happens when skill meets opportunity and support," says Stacey Books, CEO of Persevere. "Persevere prepares talented people with industry-aligned training and stands with them for a full year after release; employers gain resilient, high-output contributors who strengthen teams and deliver results."

Today, Vincent is living the life he once thought was impossible.

"Five years ago, I would not have dreamed of being where I am right now," he reflects. "I am focused on learning, growing, and giving back to people who think their situations are hopeless."

Vincent's story reflects a growing workforce trend. According to the Society for Human Resource Management (2024),81% of managers report that employees with prior justice involvement perform as well or better than their peers. In today's remote-first tech landscape, potential is no longer defined by geography or history. It's defined only by skill, dedication, and the willingness to grow.

As Hosman emphasizes, "Vant4ge strongly believes in second chances for those individuals who earn them." For employers navigating talent shortages in competitive markets, partnerships with organizations like Persevere offer access to motivated professionals who bring both technical excellence and hard-won resilience.

Each morning, as Vincent logs in to work from his Florida home, the sound that begins his day is no longer a correctional institution's bell but the quiet hum of his laptop, a simple sound that represents a future rebuilt through effort, opportunity, and unwavering support.

He's not just writing code. He's rewriting his story.

Modernization Starts With a Clear Strategy



-Fiona McFarland, Chair of the House, IT and Policy Subcommittee



-Representative Omar Blanco

By **The Florida Technology Council**

Anyone following the Florida House of Representatives' Information Technology and Policy Subcommittee has seen a long overdue shift in how Florida is addressing IT procurement and management of government information technology.

For years, state agencies have delivered essential services using aging platforms, fragmented systems, and procurement models built in a different era. Dedicated public servants have worked tirelessly within those constraints, yet those limitations have often slowed modernization, increased costs, and reduced flexibility. Technology designed decades ago now struggles to meet the pace, scale, and expectations of modern service delivery.

Leadership within the Florida House Information Technology and Policy Subcommittee has made clear that incremental change is no longer acceptable. Under the leadership of Representative Fiona McFarland, the Subcommittee has focused squarely on structural reform in how the State procures and manages technology. Ranking Member Representative Lindsay Cross has questioned whether existing State Term Contract requirements remain fit for purpose, while Representative Lopez has pressed for answers on why other states are moving faster through their procurement processes.

Representative Miller has raised concerns about IT project scopes that are unclear, overly prescriptive, or developed without the right stakeholders at the table. Representative Omar Blanco has addressed how commodity IT purchases are being slowed by rules designed for large scale projects, underscoring the need to distinguish true commodities from complex implementations. Representative Giallombardo has emphasized the importance of clearly defining best value in statute and requiring evaluation criteria that prioritize outcomes rather than price alone.

Taken together, these efforts signal that Florida is clearly pushing to move from reactive technology spending toward a disciplined, strategy driven approach that prioritizes speed, interoperability, security, and accountability. This shift marks a critical inflection point for state government. Decisions made during this transition will shape how Florida delivers services, protects sensitive data, and supports its workforce for decades to come.

From Fragmentation to Shared Direction

Fragmentation remains one of the most persistent challenges in public sector technology. Agencies operate independently with different systems, procurement timelines, and technology standards. While that autonomy supports mission specific needs, fragmentation often leads to duplication, incompatibility, and unnecessary expense.

A modern statewide strategy provides shared direction without removing agency authority. Common objectives and baseline standards align security, interoperability, and long-term value across government. That alignment allows agencies to modernize with confidence, knowing each investment supports a broader statewide mission rather than existing in isolation.

Strategy Without Centralization

Modernization efforts often raise concerns about centralization, yet effective models separate strategy from execution. A centralized strategy defines outcomes, priorities, and guardrails while agency leadership retains control over implementation. This structure ensures consistency where consistency matters and flexibility where flexibility remains essential.

Agencies continue selecting solutions that support their operational needs, but those solutions align with statewide requirements for interoperability, cybersecurity, and sustainability. Shared navigation replaces shared control. This approach allows Florida to scale modernization without slowing momentum.

Why Clear Standards Increase Speed

Some agencies worry that oversight slows progress, but uncertainty causes far more delay than clarity. Projects often stall when security requirements, interoperability expectations, or compliance standards emerge late in the procurement process. Rework and revision then consume time and resources that agencies can least afford.

Establishing standards at the beginning of a project eliminates that uncertainty. Clear expectations allow agencies to plan efficiently, move decisively, and avoid last minute disruptions. Front end discipline produces faster delivery and more predictable outcomes.

Interoperability Without Uniformity

Interoperability does not require identical tools across government. Interoperability requires systems that communicate effectively, scale responsibly, and share data securely. Defining statewide technical requirements prevents the creation of isolated technology silos while preserving agency choice.

Aligned modernization efforts also create opportunities for shared platforms, enterprise licensing, and coordinated procurement. Those efficiencies reduce redundant spending and strengthen Florida's collective buying power. Strategic alignment enables collaboration without forcing uniformity.

Supporting the People Carrying the Mission

Agency leaders and technology professionals remain central to every modernization effort. Any successful strategy must reduce friction and remove barriers rather than add complexity. Clear frameworks empower professionals to focus on outcomes instead of navigating uncertainty.

Supporting agencies with defined standards, consistent expectations, and collaborative partnerships allows modernization efforts to succeed. Agencies perform best when systems support execution rather than impede progress. Statewide alignment creates conditions for talent to deliver results.

The Path Forward

Florida has the opportunity to establish a modernization model that positions the State for long term success. Executed through a deliberate three-year rollout, this effort allows agencies to modernize in phases, incorporate lessons learned, and respond to evolving needs without losing strategic alignment.

Modernization is not a single initiative or procurement cycle. Modernization represents an ongoing commitment to clarity, alignment, and execution. With purpose and coordination, Florida can deliver technology that is faster, more secure, and better aligned with the needs of the people it serves.

That work is underway. The responsibility now is to execute it well.

-Warren Sponholtz, State CIO FLDS

-Jonathan Conrad, CEO at ISF



-Michelle McGinley,
Managing Director at Accenture

-Cole Sousa,
CIO for Children and Families



Hacking humans:
How to defend against your biggest cyber risk

Attackers are bypassing traditional cyber defenses by impersonating employees. Why help desks have become the target, and how agencies can reduce the growing risks.

By Scoop News Group

A tech support specialist at a public healthcare institution answered what sounded like a routine call: An oncologist, identifying himself as a staff member, explained he had purchased a new smartphone and needed to reset his credentials to access his accounts. The tech specialist asked a few standard identity challenge questions, but despite how easily the oncologist responded with the correct answers, something didn't feel right.

"By the way, where are you calling from?" he asked the doctor. "Well, at the moment, I'm in the ER," the oncologist replied. "I can give you the phone number if you like."

To a less-savvy help desk specialist, that response might have seemed credible. That's how convincing threat actors have become in impersonating employees and how capable they are at extracting personally identifiable information about their targets from the internet.

The tip-off in this case? The specialist knew that oncologists don't typically work in the emergency room and discerned this was a brazen breach attempt. Fortunately, it failed.

"Not all help desk individuals have that sixth sense or have the level of training needed to thwart attacks the way this individual did," says Ryan Witt, vice president of industry solutions at Proofpoint, which specializes in enterprise email risk and cyberthreat protection. "Nor do they have the level of technology and authentication capability built into their infrastructure right now to stop these types of attacks at scale."

And threat actors know it.

The Help Desk: High-Value Target Under Siege

For government agencies, institutions and enterprises

it's essential to recognize that the battle to protect enterprise resources has shifted, and why focusing on human behavior has become critical to cybersecurity operations.

Technical defenses like firewalls, continuous monitoring and remediation and AI-assisted analytics remain essential tools in that battle.However, malicious actors have found a way around those defenses, using deception and impersonation to prey upon unwitting individuals within organizations and tricking them into sharing their credentials.

The latest figures from Verizon's 2025 Data Breach Investigation Report bear that out. It found that of the 12,195 data breaches the DBIR unit investigated last year, 60% involved human interaction. Credential abuse and social actions, like phishing, were cited as leading factors. That compares to the exploitation of system vulnerabilities, which grew significantly last year but still only accounted for 20% of breaches.

What's changing, says Pablo Passera, vice president of product management and a security expert with Proofpoint, is the growing assault on help desks. Threat actors recognize that service desk agents, tasked with assisting employees and managing access, hold the keys to the kingdom.

"A service desk agent can change a password, reset credentials, manage multi-factor authentication (MFA) devices and troubleshoot access issues," says Passera. A successful impersonation doesn't just compromise one user; it provides the attacker with the legitimate tools to escalate privileges, move laterally, access sensitive data like payroll accounts or deploy ransomware, he adds. "So, the service desk is a very valuable target for threat actors right now."

Passera notes that attackers are also using the help desk to trick employees. He described a growing tactic called mail bombing, where an attacker identifies an employee within an organization and subscribes their email address to thousands of newsletters. "Imagine your inbox suddenly has 1,000 welcome emails and then someone impersonating a help desk agent contacts you, saying, 'Hey, Paul, I'm from the service desk, and we noticed you're under attack. Click on this link so we can help reslove the issue.' The employee clicks the link and suddenly they're compromised."

The Crumbling Wall of Traditional Verification

"One of the biggest challenges for service desk agents," notes Passera, "is being able to identify if someone is impersonating an employee or is the real employee."

For years, organizations relied on verifying identities by asking for Personally Identifiable Information (PII) – the last four digits of a Social Security number, a mother's maiden name, the date of birth.However, the era of massive data breaches has rendered this method dangerously obsolete. Vast quantities of PII are readily available on the dark web, allowing attackers to answer these

> **"Not all help desk individuals...have the level of training... or technology and authentication capability built into their Infrastructure right now to stop these types of attacks at scale."**
> **– Ryan Witt, vice president of industry solutions, Proofpoint**





traditional challenge questions easily. "Asking for PII doesn't work anymore," Passera says.

More recent verification methods, such as real-time video validation, where an individual displays their driver's license on camera, are no longer foolproof. The rise of AI-powered deepfakes—highly realistic fabricated video or audio—presents a relatively new but growing challenge.

Passera cites a reported example where a financial employee at a multinational firm in Hong Kong was asked to attend an internal video conference call. The call, however, was staged with deepfakes of senior officers, including the firm's chief financial officer, who duped the employee into transferring $25 million to a surreptitious account.

These and various other forms of deception create a tricky balancing act for cybersecurity officials. More stringent verification processes increase security but can frustrate users and impede productivity, especially at government agencies that serve diverse populations or share information with other agencies.

Once a malicious actor gets their foot in the digital door, however, it's just a matter of time before they gain wider access to an enterprise's network and begin their exploits, like:

- **Accessing sensitive data:** Navigating file shares, databases or cloud storage containing citizen PII, financial records or confidential government information.
- **Internal phishing:** Leveraging the compromised account's legitimacy to send phishing emails to colleagues, spreading the attack internally.
- **Privilege escalation:** Seeking ways to gain higher levels of administrative access.
- **Data exfiltration:** Copying and stealing sensitive information.
- **Ransomware deployment:** Encrypting critical systems and demanding payment.

Shifting to a Human-Centric Defense

Since attackers are exploiting human trust and behavior, IT and security officials need to develop defensive strategies that are also human-centric.

Adopting a human-centric security strategy involves taking several steps that yield a deeper, more granular understanding of user actions, context and inherent risks—particularly around email activity—rather than solely relying on technical controls, according to Passera and Witt.

Their perspective is based on Proofpoint's vast intelligence experience in monitoring 85% of the Fortune 100. Specifically, they recommend:

- **Assessing who is at greater risk** and deploying greater security controls around them. Witt points to three attributes to look for: high-profile individuals with a public persona, workers perceived to have access to valuable information and employees required to work with third-party systems.
- **Investing in specialized training,** especially for help desk staff. They need to understand the tactics used against them, recognize red flags in user requests (urgency, unusual demands, inconsistencies) and know the proper procedures for escalating suspicious interactions. Crucially, says Passera, "Service agents are not security experts." Training must be practical, synthesized and equip them to identify anomalies without overwhelming them with technical security details.
- **Re-evaluating identity verification processes** with an understanding of current threats like PII exposure and deepfakes, balancing security with usability. The key is a layered approach, potentially incorporating risk signals. For example, a simple password reset might require less stringent verification than enrolling a new MFA device, especially if the request originates from an unusual location or follows other suspicious activity indicators.



"A service desk agent can change a password, reset credentials, manage multi-factor authentication (MFA) devices, and troubleshoot access issues. So, the service desk is a very valuable target for threat actors right now."
– Pablo Passera, vice president of product management, Proofpoint

- **Deploying advanced monitoring and analytics tools that focus** on user behavior and correlate events across systems. This is where a human-centric approach diverges from traditional methods. Instead of just logging events, the focus shifts to understanding who is doing what, when, and why, and whether that behavior deviates from established norms.
- **Educating the entire workforce** about the risks of threat actors impersonating employees and the need for more vigilant cybersecurity awareness practices. Seven out of 10 working adults admitted to taking a risky action, such as reusing or sharing a password, clicking on links or QR codes from unknown senders or giving credentials to an untrustworthy source, according to Proofpoint's "2024 State of the Phish"

Integrated Human-Centric Protection

In an environment where agencies manage high volumes of sensitive information, the most effective security strategies place people at the center of protection efforts. Proofpoint's experts know this space well, highlighting how modern threat intelligence and machine learning help agencies reduce risk by identifying and stopping harmful emails before staff ever see them. When a suspicious message does slip through, a network must have the capabilities that allow security teams to quickly remove it from inboxes, limiting exposure and helping agencies maintain continuity of operations.

"Across state and local agencies, the volume and variety of email threats continue to grow, making advanced screening essential for protecting staff and safeguarding public data. Sandboxing tools must play a central role in that effort. Secure systems evaluate warning signs such as questionable IP addresses, unfamiliar or risky file attachments, and links that could redirect users to unsafe destinations. When needed, they can also rewrite or isolate URLs so employees interact only with verified sites," Witt explains.

"Protected clients have a very granular view of the most attacked individuals in their organization, based on volume or severity and sophistication of exploits being sent to them," he adds. "By analyzing email activity on a client's network, you can identify the last five people an individual emailed, or who sends email to that individual most often, or who that individual groups together."

"There is a whole other form of questioning that [a service desk agent] could ask when trying to go through the authentication and verification process," Witt notes.

Only the latest technology can compliment those capabilities by providing a holistic architecture that identifies and mitigates risk across an organization's entire digital environment, reducing the burden on end-users and the service desk.

Agencies, for instance, can track user activities across various platforms – cloud application usage, file access patterns, permission changes, email sending behavior, login locations and times. Advanced tools utilizing AI and ML can establish baseline behaviors for individuals and roles, automatically flagging deviations that indicate potential compromise. For instance, an employee suddenly accessing unusual files, attempting to change permissions or sending emails with suspicious links after contacting the help desk would trigger an alert.

Those and other capabilities led Gartner to name Proofpoint a "Leader" in its 2024 Magic Quadrant for email security platforms.



The Imperative for Government Agencies

Given the scale of highly sensitive citizen data they maintain, federal agencies stand to benefit most from advanced human-centric defenses. However, state, county and municipal governments and higher education institutions are already seeing added benefits from leveraging powerful solutions:

The City of Aurora, Colorado, struggled with high spam volumes, limited visibility into phishing attacks and lengthy response times. After adopting a highly advanced, automated email-security approach, and other tools, the city gained "optics into email threats that we never had before," according to its CISO. It also stopped targeted ransomware attacks and reduced spam and bulk mail to zero.

The Mississippi Department of Child Protection Services faced various challenges in meeting regulatory and e-discovery requirements through archiving. After deploying intelligent compliance solutions, the department is now able to easily access employees' communications, including the mailboxes of employees who have left the organization.

Princeton University needed to migrate multiple email platforms to the cloud while ensuring day[1]to-day operations and reliable communications between students, faculty, and staff. Proofpoint moved them to a secure email relay that provided the means to maintain the integrity of large volumes of outbound email while giving administrators necessary spam and malware detection and filtering capabilities.

Regardless of where government agencies are in their IT modernization journeys, agency leaders can build more resilient security postures by acknowledging that humans are both the primary target and the first line of defense.

Focusing on understanding and safeguarding human behavior, supported by intelligent technology, is the critical next step in protecting public data and ensuring the continuity of vital government services in an increasingly hostile digital world.

This special report was produced by Scoop News Group for FedScoop and sponsored by Proofpoint.



Modernize or Fall Behind: Florida's Critical Tech Crossroads

*By **David Clark**, CEO, MyGovGuide*



Technology underpins all public services, agency operations and state security in Florida. Yet, the state's current patchwork of outdated and uncoordinated systems is leading to service delays, increased security risks and inefficiencies. Modernizing Florida's IT infrastructure is now critical for our state's economic stability and performance.

> **"Why it matters: Florida's ability to lead and compete nationally is at stake if the state doesn't swiftly modernize enterprise architecture, including adopting emerging technologies."**

The Challenge: Patchwork Agency Systems Don't Work Together

For years, state agencies have been doing the best they can with old systems and fragmented tools. Agencies make decisions based on immediate needs, limited budgets and existing systems. The result is a patchwork of platforms that cannot fully integrate, are expensive to maintain and create uneven service experiences across government.

Florida cannot afford another round of independent modernization efforts.

Without a coordinated plan and governance structure, even well-intentioned investments can become harder to align and sustain over time. Agencies are managing real constraints while keeping essential services running, which makes it difficult to sequence replacements, align resources and retire higher-risk systems in a deliberate and efficient way.

A shared framework creates the conditions needed to do that work with greater confidence and consistency.

The Case for a Three-Year Rolling Plan

A static five-year document will always fall behind reality. A one-year cycle is too short to replace core systems or shift enterprise architecture.

Three-year plan for Florida's large, complex government At minimum, must include:

- Cybersecurity and Digital trust Infrastructure
- Enterprise Connectivity and Core Infrastructure
- Data, Application, and Platform Architecture

The answer is a three-year rolling plan, updated annually. A three-year plan allows for purposeful modernization with the flexibility to adapt to new challenges and emerging technology.

It also aligns with the realities of election cycles and creates predictability for the Legislature, Executive Branch and agency teams who must manage complex changes while keeping daily operations running.

Without Governance, a Plan is Just a Wish List

Good governance turns ideas into real action and results. Governance isn't about centralizing control, but about creating consistent standards.

Think of it as a playbook where a lead agency outlines the game plan, from cybersecurity, technical baselines and procurement rules, while each team picks the plays that suit them best, all within a shared strategy.

This ensures integration, security and long-term value for the state's investment.

With a clear statewide roadmap and budget aligned to a three-year plan, the Legislature and Governor's Office of Policy and Budget (OPB) can make the right investments and avoid wasting state money on short-term fixes that don't move the state forward.

For decades, Florida's Department of Transportation has proven this approach works. The FDOT Work Program uses a rolling plan to fund, manage and deliver complex infrastructure projects with transparency and efficiency.

Standardizing Cybersecurity or Risk Losing Control of Infrastructure to our Adversaries

It's not a matter of if, but when we'll see more major cyberattacks on our state.

Threat actors continue to steal personally identifiable information at unprecedented levels, often exploiting gaps in aging or unevenly secured IT infrastructure. This represents a clear and present danger. Beyond data theft, operational technology systems that support critical public services such as water, energy, transportation and health services increasingly face risk from outdated controls, limited visibility and inconsistent security practices.

In the past five years, a ransomware attack by a Russia-based criminal group disrupted the nation's largest fuel pipeline, triggering fuel shortages and panic buying across the East Coast. In Florida, a widely reported incident at a municipal water treatment facility highlighted how legacy systems, weak access controls and human error can create serious operational risk even in the absence of a confirmed cyber breach.

> **"These events underscore that infrastructure resilience depends not only on defending against advanced attackers, but on modernizing systems and governance before failures occur."**

Today, cybersecurity maturity varies significantly across agencies, despite dedicated CIOs, CISOs and information security teams working hard within real resource and system constraints. This places a complex and asymmetrical burden on individual agency leadership to interpret evolving threats and security expectations on their own. Florida must operate from a unified cybersecurity foundation, built on a consistent zero trust posture, common identity and access management, standardized endpoint protection, and shared threat intelligence. These standards should be defined at the enterprise level and applied uniformly across state government.

The Why: A Better, Safer Florida

This infrastructure will be a force multiplier for citizen experiences with government, making services work more quickly, securely and without unnecessary barriers. Systems will be faster. Data will be more accurate. Cybersecurity risk will be reduced.

It also forces the state to invest in Florida's future workforce. Modern IT environments require cloud engineering, cybersecurity specialization, data architecture and DevSecOps practices. Agencies can't build these capabilities overnight. The plan helps them find gaps and develop the talent pipeline needed to sustain modernization long term.

The bottom line: A three-year rolling plan to modernize IT infrastructure and standardize cybersecurity will create a more consistent, safer and more efficient state, with improved public services. Drawing from the Florida Department of Transportation's and other agencies' successful planning frameworks, this approach could set a new standard for digital government.

MyGovGuide provides the insights to move forward with clarity and confidence.
www.mygovguide.com



Making Rural Health Investments

Deliver the Most Impact

Rural hospitals that support vast regions do not serve neat boundaries. A single closure, staffing shortage, or surge can ripple across counties and cause undue strain across the healthcare system.

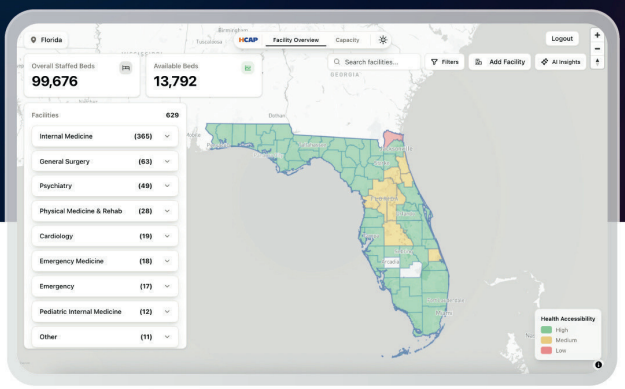
Yet investment decisions for these fragile health ecosystems are often made without a clear picture of the communities being served and their biggest needs.

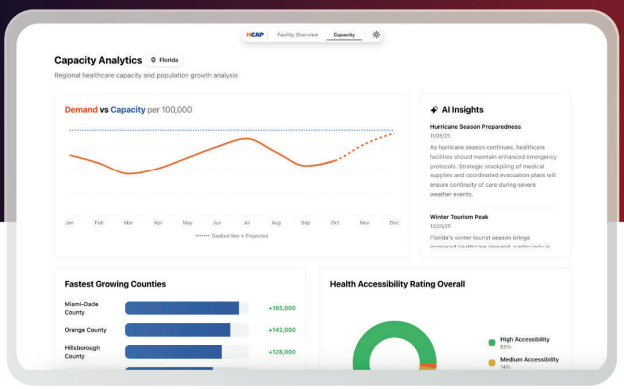
Our tools feature:

- Facility catchment analysis
- Staff and resource capacity planning
- Intuitive, tailored dashboards

Enabling you to:

- Test response scenarios
- Prioritize interventions
- Strengthen regional resilience before crises force reactive choices.





Ruvos helps states move from awareness to action in rural health strategy.

We combine catchment analysis, capacity planning, and intuitive dashboards to help leaders test scenarios, prioritize interventions, and strengthen regional resilience before crises force reactive choices. Our tools make complex data usable, transparent, and defensible, keeping human judgment at the center of every decision.

Built on decades of experience supporting public health and healthcare systems, our work helps leaders responsible for health investment decisions make confident choices, understand impact over time, and clearly communicate those decisions to the communities they serve.

Built for people who make decisions that matter.

RUVOS

ruvos.com • hello@ruvos.com

Using the Open Group Enterprise Architecture Framework to Accelerate State Digital Transformation

Co-Authored By, ***Dr. Darren Pulsipher and Hugues Morin,*** *Intel Corporation*



State governments face growing expectations to modernize. Citizens and Businesses alike expect services that are as intuitive and responsive as those offered by the private sector, while legislatures demand accountability, transparency, and measurable outcomes. At the same time, state agencies must navigate legacy systems, siloed organizations, constrained budgets, and evolving regulatory requirements. In this environment, digital transformation is not a single initiative, it is a continuous journey.

One of the most effective ways state agencies can bring discipline, coherence, and momentum to this journey is by adopting the Open Group Enterprise Architecture framework, commonly known as TOGAF®. The framework offers state agencies a practical way to bring coherence and momentum to digital transformation. More than a technology framework, TOGAF provides a disciplined approach to aligning **people, processes, data, and technology** around shared outcomes. When applied pragmatically, it helps agencies move with purpose rather than speed alone—because transformation without direction rarely delivers results.

Enterprise Architecture Is About People First

A common misconception is that enterprise architecture is an IT activity. Successful architecture efforts begin with people: agency leaders, program owners, frontline staff, and partners who design and deliver public services.

State transformations often fail not because of poor tools, but because roles are unclear, decision rights are fragmented, and change management is underestimated. Unclear strategies, underestimated dependencies, isolated change implementations – this is the fuel of unsuccessful transformations.

TOGAF explicitly addresses these challenges by providing a framework to ask the right questions, sequencing decisions, and aligning stakeholders around a shared future state across organizations boundaries.

Process Discipline Enables Sustainable and Iterative Change

Digital transformation frequently stalls when agencies digitize existing processes without questioning whether those processes still make sense. Automating inefficiency only accelerates frustration.

TOGAF encourages agencies to examine and redesign business processes as a core part of transformation. By linking business architecture to information systems and technology decisions, the framework helps ensure that new solutions are built around how services should work—not how they happened to evolve.

The framework's Architecture Development Method (ADM) supports iterative, incremental progress rather than "big bang" transformations. This aligns well with budget cycles, procurement constraints, and the need to show early wins.

Closing the Gap Between Strategy and Delivery

State strategic plans often articulate ambitious goals—digital-first services, data-driven policy, improved constituent experience—but projects on the ground struggle to translate those goals into actionable requirements.

TOGAF helps close this gap. It provides a powerful tool to map the existing state of the organization and build a step-by-step roadmap to the desired future state. Policy objectives are decomposed into capabilities, capabilities into processes, and processes into enabling systems and data. This traceability ensures that technological investments are clearly justified and that projects remain aligned with agency missions.

The result is fewer disconnected initiatives and greater confidence that limited resources are being directed where they matter most.

Managing Legacy Systems Without Paralysis

Legacy systems remain a defining challenge for state agencies. Many are mission-critical and cannot be replaced quickly, yet they constrain agility and innovation.

TOGAF supports a pragmatic approach through transition architectures. Agencies can define realistic intermediate states that balance risk, cost, and value—modernizing incrementally while maintaining continuity of service. Legacy systems are evaluated based on their contribution to outcomes, not just their age.

Progress replaces perfection. Momentum replaces delay.

Data Management: The Foundation for the Next Wave of Services

As states look toward advanced analytics, automation, and agentic AI–based services, **data management becomes foundational,** not optional. AI systems are only as accurate, fair, and trustworthy as the data that feeds them.

TOGAF explicitly elevates data as a core architectural domain. It encourages agencies to define data ownership, standards, interoperability, and governance early—before deploying advanced tools. This discipline is essential for ensuring data quality, consistency, privacy, and ethical use.

Without strong data architecture, agentic AI services risk amplifying errors, bias, and fragmentation. With it, states can enable intelligent assistants, proactive services, and real-time decision support that are accurate, auditable, and aligned with public values.

In this sense, data architecture is not preparation for the future, it is a prerequisite for it.

Governance That Enables, Not Inhibits

Effective governance is often seen as slowing innovation. In practice, the absence of clear governance leads to rework, duplication, and failed initiatives.

TOGAF promotes lightweight, decision-focused governance that provides guardrails rather than roadblocks. Clear standards, shared services, and transparent review processes allow teams to move faster with confidence, knowing expectations upfront.

Good governance does not restrict innovation; it channels it.

Acting with Intent

Digital transformation in state government is inevitable.

The Open Group's Open Digital Transformation Architecture is building on the foundation of TOGAF and offers a way to move faster by seeing the whole enterprise—aligning people, processes, data, and technology around shared outcomes. It helps agencies modernize responsibly, prepare for AI-enabled services, and build capabilities that endure beyond individual projects or administrations.

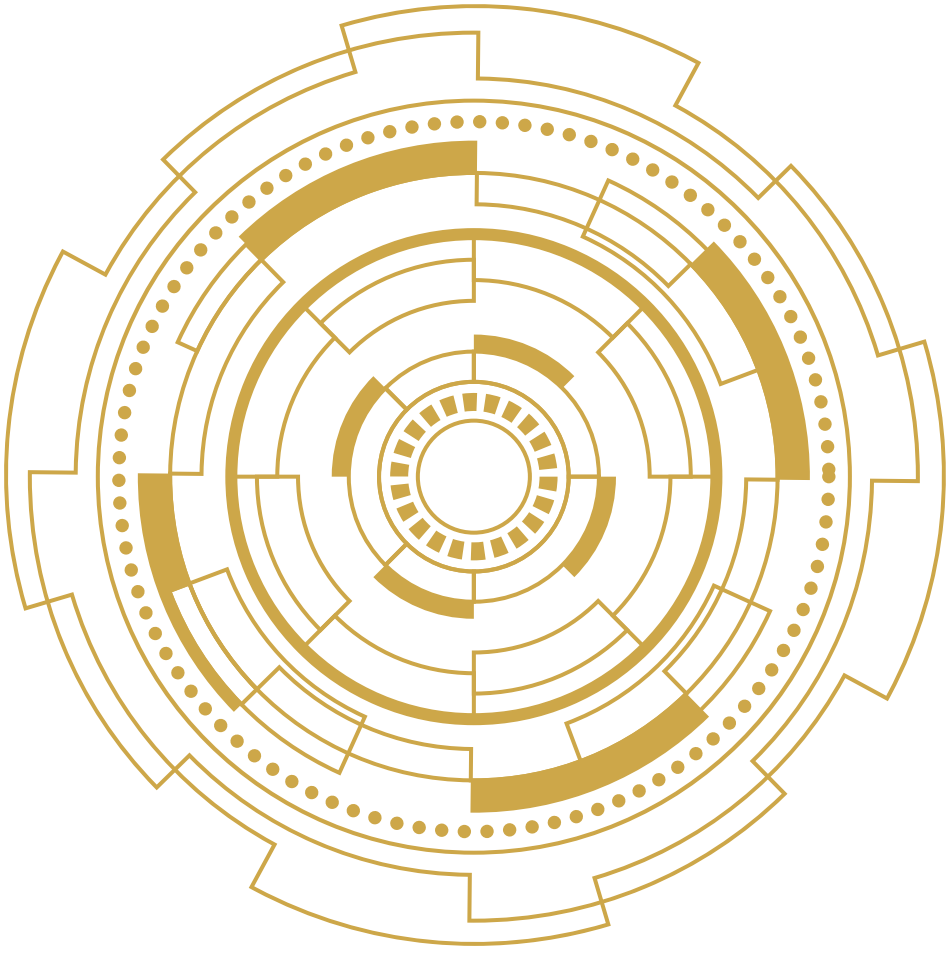
→

In an era where public trust depends on effective delivery, enterprise architecture is not overhead. It is infrastructure for change. And for state agencies ready to move from aspiration to execution, TOGAF provides a clear and proven path forward.

About the Author's

Dr. Darren Pulsipher *is Intel's PS Chief Solution Architect and the chair of the Open Group Digital Transformation Forum. Dr. Pulsipher also teaches at Vanderbilt University and hosts a popular podcast called Embracing Digital Transformation (embracingdigital.org)*

Hugues Morin *is Intel's Director for the southeast SLED Market and the main point of contact for Florida Agencies wanting to engage in a consultative discussion with its architects around TOGAF, and can be reached at Hugues.morin@intel.com*



Intel Corporation, a publicly traded company in which the U.S. government holds an approximate 10% participation, does not sell products or services directly to state agencies. Instead, Intel's role in the public sector is primarily foundational and advisory. Its technologies are embedded across much of the world's digital infrastructure, spanning edge and IoT devices, networking, data centers, cloud platforms, and AI systems that underpin modern government services. Recognized for its long-standing commitment to open standards, interoperability, and vendor-neutral architecture, Intel works across the industry's broadest technology ecosystem, collaborating with hardware manufacturers, software providers, cloud platforms, and systems integrators alike. In this context, Intel can engage with state agencies at no cost to provide architectural insight and technical guidance, helping leaders understand emerging technology trends, evaluate design choices, and align long-term digital strategies—without influencing procurement decisions or promoting specific products.



Trusted AI Governance: Florida's Path Forward A Framework for State Leaders to Balance Innovation and Responsibility

*By **Leanne Lapp**, Florida Technology Leader, IBM*

Florida stands at a crossroads. State leaders clearly see the opportunity in Artificial Intelligence—modernizing services, attracting talent, and growing the economy. At the same time, they see the responsibility that comes with it. Citizens must be protected. Systems must be accountable. Progress must be trusted.

This balance—between innovation and responsibility—is where Florida can secure long-term advantage. I've spent the past several years working with government leaders on this exact challenge.

When organizations step back from emerging technology, they do not protect themselves—they fall behind. The challenge is not whether to govern AI; it is how to govern it responsibly, so innovation and safeguards grow together.

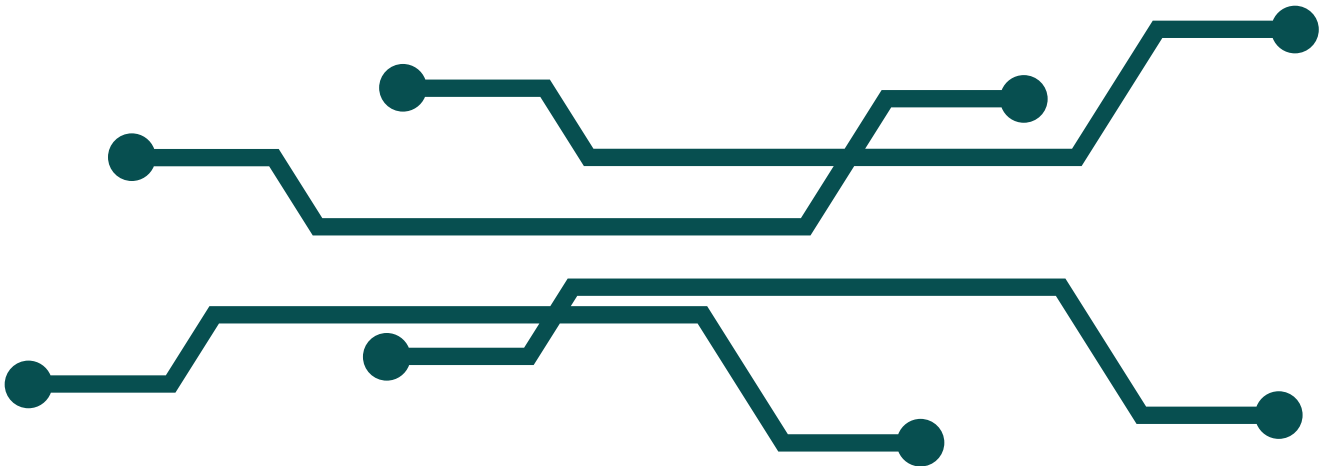
Why Florida's Instinct Is Right—But the Answer Isn't to Pause

Florida's recent proposals—an "AI Bill of Rights" and new oversight for high-risk AI—show an instinct that is exactly right. You understand something essential: technology adoption requires public trust. And trust comes when systems are transparent, explainable, and fair.

When I look at Florida, I see enormous potential. You have one of the strongest university systems in the country, with institutions committed to teaching and advancing AI the right way. You have a growing economy, ready to attract both companies and skilled talent. What is needed now is a framework that turns these assets into a durable foundation for responsible growth.

What Trusted AI Looks Like

For more than a century, IBM has partnered with governments through every technological wave. Today, IBM is helping shape



global standards for responsible AI, contributing to governance frameworks that informed policies like the EU AI Act and the AI Pact. From this work, one lesson is clear: trust in AI rests on five essential pillars.

1. **Transparency**: People deserve to know how an AI system works, what data it is trained on, and where its limits are.
2. **Explainability:** Especially in government, AI decisions must be understandable to humans.
3. **Fairness:** Every system must be tested for bias from design through deployment.
4. **Robustness:** Systems must perform reliably, even under stress, with noisy data, or in unexpected conditions.
5. **Performance:** AI should measurably improve efficiency, accuracy, or outcomes. If it does not, it is not ready for use.

Keeping Humans in the Loop

Here is what I tell every leader I meet: AI should enhance human decision-making, not replace it. That belief is central to every serious responsible AI policy around the world. Oversight is not a barrier to innovation—it is the foundation that makes innovation sustainable.

A Framework for Florida

Florida needs a principled framework that aligns with its values. That means:

- **Starting with risk-based classification.** Map use cases and govern them in proportion to their impact.
- **Requiring transparency and explainability.** Make these non-negotiable across all systems.
- **Embedding governance in the full lifecycle.** Do not treat AI governance as a one-time checkbox; systems must stay accountable over time.
- **Investing in people.** Train leaders, IT professionals, and students in AI ethics and practical oversight. This is not just a technology issue—it is a workforce issue.

The Decision Ahead

The World Economic Forum projects that 65% of children entering primary school today will work in job categories that do not yet exist. That is your future workforce—and the roles you will need to fill in your agencies. States that retreat or over-regulate will watch that talent go somewhere else.

Florida has all the right ingredients to lead this next chapter: world-class universities, a strong economy, and leaders willing to balance innovation with care. The choice now is not between innovation and regulation. It is how to pursue both—responsibly, confidently, and at scale.

About the Author

Leanne Lapp *is one of IBM's Technology Leaders for the State of Florida and works alongside clients to develop integrated solutions to address their technology challenges.*

Protecting trust at the speed of risk: Why modernization matters

Co-Authored By, ***Stephen Walsh and Chris Montgomery,*** *Public Sector Technology Advisors, Slalom*

Trust is the foundation of every public program. People rely on public institutions to deliver essential services, safeguard personal information, and manage public dollars responsibly. However, fraud and cyber risks targeting our government systems — from ransomware to deepfakes — grow more sophisticated every week. Approximately 70% of state and local government agencies reported ransomware attacks in the past two years, with a mean recovery cost of $2.8M. Florida is not immune to this threat. Our technology leaders must remain hyper-vigilant and modernize responsibly to stay ahead.



Why legacy systems fall behind

Mainframes have delivered decades of reliability. However, today's environment requires more adaptability, integration, and near real-time responsiveness. Legacy systems struggle to deliver against these modern requirements, including:

- Real-time identity verification and eligibility checks
- Cross-program data sharing
- Integration with modern analytics, machine learning, and third-party identity systems
- Consistent security control application across siloed environments
- Rapid rule, code, or configuration adjustments

Even modest improvements may require specialized skills, lengthy development cycles, and significant costs. The issue is structural: threats evolve quickly, but legacy environments do not.

> **"Cybersecurity is not only about preventing attacks, but also about protecting the continuity of the services residents rely on most. Government leaders who modernize legacy systems proactively will defend programs at the speed of risk and protect public trust."**
>
> -Chris Montgomery, Slalom
> Public Sector Sr Director and former CISO.

Cyber risk and fraud accelerating in parallel

Fraud remains a persistent challenge for government programs like unemployment insurance or Medicaid. While specifics vary by program, the

pattern is consistent: siloed systems, limited data sharing, and verification processes that cannot keep pace with evolving fraud tactics. Legacy systems often cannot support the speed, accuracy, and security needed to maintain integrity at scale.

Cyber risk now rivals fraud in scale, speed, and sophistication. Attackers automate credential harvesting, coordinate activity across compromised accounts, and exploit shared platforms. Ransomware crews target backups and steal data for double extortion. Regulatory requirements such as CJIS, IRS Publication 1075, HIPAA, and FERPA further raise expectations. Meeting these standards in legacy environments often means custom engineering rather than sustainable patterns.

What modernization unlocks

Modernized platforms strengthen program integrity and cyber resilience by letting agencies:

- Detect fraud earlier by integrating data across programs
- Update fraud and risk models quickly as threats evolve
- Strengthen identity assurance through MFA, conditional access, and federation
- Improve resilience through segmentation, encryption, and automated recovery
- Provide audit-ready evidence with real-time observability

While some of these capabilities can be implemented on legacy systems, they typically require costly customization and niche expertise. Modern cloud and hybrid environments offer a more sustainable path forward.

> **“Modernization isn’t only a technology decision – it’s a leadership decision. Modernization is how Florida’s leaders act before challenges impact our residents and communities,”**
> -Monica Corbin, Florida Client Partner, Slalom

Strengthening the front door

Improving verification before users reach the legacy system is one of the most immediate ways to reduce fraud and cyber exposure. Agencies can introduce MFA and identity federation, improve real-time transaction visibility, and shift fraud analytics into modern platforms. This approach improves security and accuracy without touching core processing, creating early wins while broader modernization continues.

Hybrid modernization: A practical bridge

A fully modernized environment is rarely delivered all at once. Successful organizations stabilize their legacy core while moving high-impact capabilities such as identity, analytics, and fraud detection into modern architectures. Streaming events from mainframes into cloud platforms creates near real-time insight without disrupting operations. Fraud rules and risk models can evolve more rapidly. Hybrid isn’t the final destination: it’s a bridge that reduces risk, accelerates value, and builds momentum.

AI strengthens modernization and risk reduction in Florida

Artificial intelligence accelerates both modernization and risk reduction when applied to challenges legacy systems cannot easily address:

- Preserve program integrity by detecting unusual activity, verifying identity and eligibility across siloed datasets, and flagging billing anomalies.
- Strengthen cyber defense with improved threat detection and accelerated investigation and response.
- Modernize systems by translating legacy code, mapping dependencies, and reducing delivery timelines and reliance on highly specialized talent.

Florida is increasingly recognized nationally for its innovative use of technology to reduce cost and risk in emergency management operations. In 2024, the Florida Division of Emergency Management (FDEM) deployed an AI-enabled anomaly detection tool. The solution saves significant time by identifying and interpreting invoice anomalies, sends notifications summarizing anomalous invoices and other invoice quality issues, and allows FDEM to better streamline the invoice process by optimizing valuable resources and enabling faster resolution. In the first year, the solution saved the State of Florida $1.8 million.

How agencies can move forward

Modernization succeeds when leaders focus on progress, over perfection. Effective programs start with small, contained steps that reduce risk without disrupting operations. Hybrid approaches allow teams to stabilize legacy systems while shifting fraud detection, identity controls, analytics, or customer-facing services into modern platforms. This creates momentum, builds confidence, and proves value early.

Choosing modernization is a leadership decision rooted in accountability, mission integrity, and public trust. Leaders who proactively position their programs to withstand rising threats and adapt to change create resilience and ensure continuity of service to communities across Florida. Those who delay face increased exposure, higher costs, and deeper scrutiny.

Trust is difficult to rebuild once lost. Modernization lets leaders protect trust, today and for the future. Slalom can help you move forward with clarity, confidence, and momentum in the face of rising cybersecurity threats. Learn more in our 2026 Government Outlook on Slalom.com.

About the Author's

Chris Montgomery, Stephen Walsh and Monica Corbin *are seasoned public sector advisors at Slalom, a fiercely human business and technology consulting company. Chris Montgomery is a recognized technology strategist and former government CISO with decades of experience in cybersecurity, resilience, and modernization strategy. Stephen Walsh is a former government CIO, and Certified Fraud Examiner with extensive experience leading complex public sector modernization initiatives. Contact Monica Corbin, Client Partner, Florida Public Sector, for more information.*



Artificial Intelligence, Fraud, and Waste in Florida Government

Why Responsible AI Is Essential to Protect Taxpayer Dollars

*By **Ernie Sanders**, Director, State and Local Inc, Peraton*



A Growing Challenge for Florida Government

Florida government oversees hundreds of billions of dollars each year across healthcare, transportation, education, public safety, and human services. With that scale comes unavoidable exposure to fraud, waste, and abuse (FWA), a challenge that is growing more complex as criminal actors adopt advanced technologies.

Today's fraud schemes are no longer manual or isolated. They are coordinated, automated, and increasingly AI-enabled, using synthetic identities, automated claims, deepfake documents, and cyber intrusion techniques that outpace traditional controls.

The uncomfortable truth is this: avoiding AI does not reduce Florida's risk—it increases it.

AI Is Already Being Used Against Government

Fraud rings, cybercriminals, and organized adversaries already use AI to:

- Generate realistic fake documents and identities
- Automate attacks on benefit and eligibility systems
- Coordinate fraud across agencies and programs
- Evade static, rules-based detection systems

Legacy controls were not designed for this level of speed or scale. As a result, investigations often occur after losses have already occurred.

Fear Is Understandable—but Misplaced

Concerns about AI bias, explainability, cybersecurity, and misuse are legitimate. Legislators and CIOs are right to ask hard questions about accountability, privacy, and transparency.

However, fear-driven avoidance creates new vulnerabilities:

- Fraud detection lags behind adversaries
- Improper payments go unnoticed longer
- Cyber threats escalate faster than response capabilities
- Investigative backlogs grow while staff are overwhelmed

The choice is not whether AI will shape government operations—it already is. The real question is whether Florida governs AI proactively or reacts after preventable failures.

AI as a Defensive Force Multiplier

When deployed responsibly, AI does not replace human judgment—it strengthens it.

High-impact government use cases include:

- Detecting abnormal spending and vendor behavior
- Identifying coordinated fraud patterns across agencies
- Flagging high-risk claims for human review
- Prioritizing audits and investigations based on risk
- Detecting cybersecurity threats earlier

In each case, AI functions as an early-warning system, allowing professionals to intervene sooner and more effectively.

Cybersecurity: The Non-Negotiable Foundation

AI systems must be treated as part of Florida's broader cybersecurity ecosystem. This means:

- Secure data handling and access controls
- Continuous monitoring and logging
- Protection against model manipulation and abuse
- Strong vendor security and transparency requirements

AI should never operate outside existing cybersecurity, privacy, procurement, and public-records frameworks.

A Practical Path Forward for Florida

Florida does not need sweeping new bureaucracy to use AI responsibly. Instead, leaders should focus on practical, defensible actions:

Use a Risk-Based Approach

Low-risk uses such as analytics and summarization require minimal oversight, while high-risk uses—such as eligibility or enforcement—require human review, documentation, and appeal rights.

Focus on Detection, Not Automation

AI should identify risk and anomalies, not make final determinations affecting citizens

Strengthen Procurement Guardrails

Require transparency, audit rights, data ownership protections, and exit strategies from AI vendors.

Pilot Before Scaling

Introduce AI through controlled pilots with clear objectives, reporting, and measurable outcomes.

Align With Existing Law

Anchor AI governance to Florida's established cybersecurity, privacy, and transparency requirements.

The Cost of Inaction

Fraud and cyber threats do not pause for legislative caution. States that delay responsible AI adoption face:

- Higher improper payment rates
- Increased cyber incidents
- Larger investigative backlogs
- Rising costs and diminished public trust

Florida's size makes it both a high-value target and a high-impact leader.

Leadership Through Preparedness

AI is neither a cure-all nor an existential threat. It is a tool—one that adversaries already use.

Florida's opportunity is to lead by embracing responsible AI grounded in governance, cybersecurity, and transparency.Doing so protects taxpayer dollars, strengthens oversight, and preserves public trust.

Preparedness — not fear — is Florida's strongest defense.

About the Author

Ernie Sanders *is the Director of Peraton's State and Local business and leader of Peraton's State and Local cybersecurity practice. Peraton has a mission to help secure our government and protect our citizens. They do so by engaging with government to innovate and drive technology.*

Meet the Florida Technology Council Team



Jonathan Conrad
FTC Chair
President, ISF, Inc.



Ken Elias
FTC Co-ViceChair
Managing Partner
TekBank Consultants Inc.



Ernie Sanders
FTC Co-Vice Chair
Director at Peraton



Jim Taylor
CEO
Florida Technology Council



Ava Lamberti
Director of Marketing
Florida Technology Council



Aiden Goldenberg
Executive Intern
Florida Technology Council



Kiara Kissel
Marketing Intern
Florida Technology Council



Gabriella Martinez
Marketing Intern
Florida Technology Council



Policy and Public Affairs Committee



JC Flores
Chair
Vice President, DCI Group



Jim Taylor
CEO,
Florida Technology Council



Josh Aubuchon
Co-Founder, WellConnector



John Breed
Account Lead, Entrepreneurship Professor and John McFarland Talent Acquisition and Staffing Leader @ Tal Search Group



Michael Briggs
Partner, Chief Revenue Officer, Trulight Consulting



Bryan Jones
Major Account Manager, TrendMicro



David DiSalvo
Manager, State and Local Government Solutions, KPMG



Ken Elias
Managing Partner, TekBank Consultants Inc.



Servando Esparza
Amazon WebServices (AWS) Manager, Southern Region, AWS State & Local Public Policy



Daymon Jensen
Associate Director, Accenture LLP



Mike Griffiths
Senior Vice President ProCom Consulting, Inc.



Shayna Long
Account Technology Leader, IBM



Stefanie Curll
Senior Service Delivery Manager, Kyra Solutions



Christophe Reglat
CEO, Coaxis International



Ernie Sanders
Director/Account Executive, Peraton

Focusing on Key Areas Impacting Florida:

- **Artificial Intelligence, Applications and Implications**
- **Unlimited Liability**
- **Cybersecurity**
- **Procurement**







UPCOMING FTC GOVERNMENT CONFERENCES







JUNE 2026 – FLORIDA GOVERNMENT AI & TECH MODERNIZATION SUMMIT

Explore real-world applications, strategic insights, and cutting-edge advancements that enhance service delivery, optimize operations, and future- proof government agencies.

NOVEMBER 2026 – FLORIDA GOVERNMENT LEADERSHIP & INNOVATION SUMMIT

Amust-attend eventfor state & localgovernment leaders, industry experts, and policymakers seeking to drive success through strategic innovation.

Arcades - Pinballs - Pool Tables - Shuffleboards



(407) 988-4463
TheManCaveWarehouse.Com

Orlando & Tampa Locations

Invest Today on Start Engine
https://www.startengine.com/offering/iqbilliards

start engine

AUGMENTED REALITY FOR BILLIARDS



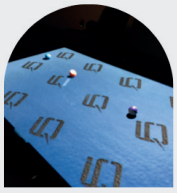
State-of-the-Art Technology

Visual stimulation and motion-enabled queueing using a Billiard Cue-Stick or hand gestures.



Mounted Projection System

Can be used on new or existing tables of any size. Intuitive self-installation and calibration



Entertainment for All

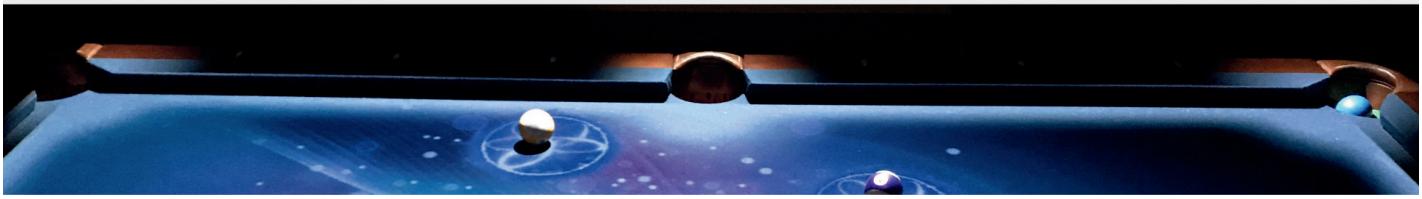
IQ supports residential and Commercial application to engage players of all demographics







IQ Billiards is an in-market producer of augmented reality projection systems that modernize the classic pool hall experience by infusing interactive state-of-the-art gameplay technology. The IQ System offers a diverse suite of digital themes, alternative games and training modes integrations to bring billiards into the digital age and engage players across all demographics.



Peraton



FLORIDA'S DIGITAL TOMORROW CAN'T WAIT FOR TODAY TO CATCH UP.

One of the largest government IT suppliers, rooted in strong cybersecurity, Peraton's digital experts go to work bringing Florida agencies into the age of the modern mission, one where agility and scalability are key and everything is in the right cloud. But we don't stop at the technology – we bring your agency's unique culture with it. Whether your agency needs cybersecurity, AI, digital transformation, digital consulting, digital intelligence, or software, Peraton partners with Florida agencies to ensure your journey to digital is a success.

peraton.com/capabilities/digital

DO THE CAN'T BE DONE.