2025

State of Arizona Agency: Department of Child Safety (DCS)
Award Category: Digital Experience – Enterprise Solutions
Project Title: Cybersecurity Modernization Initiative – Safeguarding Arizona's Child Welfare Systems
Project Dates: January 2024 – May 2025
Contact: Lyndee Ho, Chief Information Security Officer, DCS
Lyndee.Ho@azdcs.gov

IDEA (25%)

What problem or opportunity does the project address?

The Department of Child Safety (DCS), responsible for managing sensitive and high-risk data involving Arizona's most vulnerable children and families, faced growing cybersecurity challenges. With increasing threats from ransomware, phishing, and data exfiltration, DCS needed a strategic overhaul of its cybersecurity posture. Under the leadership of CISO Lyndee Ho, the agency launched the Cybersecurity Modernization Initiative to protect mission-critical data, support secure digital transformation, and uphold public trust.

Legacy systems lacked robust defenses against modern attacks, and risk assessments revealed vulnerabilities in identity management, privileged access controls, endpoint protection, and data loss prevention. The initiative aimed to close these gaps and future-proof the agency's cybersecurity framework.

Why does it matter?

Without this initiative, DCS risked exposing personal data on children, families, and providers. Such breaches could compromise investigations, lead to legal liabilities, disrupt services, and erode stakeholder trust. Child welfare systems rely on real-time data exchange across agencies, and a single cyber incident could halt coordination efforts and jeopardize safety.

CISO Ho's initiative matters because it enhances confidentiality, integrity, and availability of data, ensures federal and state compliance, and equips DCS to securely integrate AI, cloud computing, and mobile access into future service delivery models.

What makes it different?

Rather than relying on reactive security practices, DCS took a proactive, risk-based approach. Lyndee Ho applied a zero-trust architecture model, developed a cybersecurity playbook tailored to child welfare use cases, and integrated security into DevSecOps pipelines.

Key differentiators include:

- A security-by-design framework embedded across all IT initiatives.
- Federated identity management integrated with multi-factor authentication (MFA).
- Centralized security operations center with automated monitoring.
- A cybersecurity scorecard for executive reporting, tied to business outcomes.

What makes it universal?

Every agency that handles personally identifiable information (PII), protected health information (PHI), or case-sensitive data faces similar cybersecurity challenges. DCS's approach aligns with federal standards (NIST 800-53, FISMA, CCWIS), enabling it to serve as a model for:

- State health and human services departments
- K-12 and higher education systems
- Any agency adopting hybrid cloud or remote work infrastructure

The strategies used are scalable, cost-conscious, and replicable.

IMPLEMENTATION (25%)

What was the roadmap?

The initiative followed a phased roadmap:

Phase 1 (Q1 2024)

- Security Risk Assessment and Gap Analysis
- Implementation of Zero Trust Architecture framework
- Enhanced Endpoint Detection and Response (EDR) deployment

Phase 2 (Q2 2024)

- Cloud Access Security Broker (CASB) configuration
- MFA rollout across staff and third-party partners
- Encryption-at-rest for sensitive datasets in Azure

Phase 3 (Q3 2024 - Q2 2025)

- Establishment of real-time alerts and security integration
- Security Awareness Program (monthly simulations, phishing drills)
- Automation of vulnerability management and patch lifecycle

Who was involved?

- CISO Lyndee Ho and DCS Cybersecurity Division
- State of Arizona DOA IT Security Office (partnership on SOC oversight)
- Third-party MSSP and cloud vendors (Azure, CrowdStrike, Tenable)
- DCS Program and Application Owners (integrated governance)

How did you do it?

The modernization effort was managed using agile security project management, incorporating:

- Security sprint planning and backlog refinement
- Automated policy enforcement via group policy objects (GPOs)
- Continuous integration of security into CI/CD pipelines
- Frequent tabletop exercises and penetration testing

IMPACT (50%)

What did the project make better?

- Strengthened cybersecurity posture with zero-trust enforcement across 900+ endpoints.
- Reduced incident response time from 48 hours to under 4 hours.
- Implemented data loss prevention (DLP) policies for all outbound communications.
- Achieved MFA compliance among users and third-party vendors.
- Enabled secure data exchanges with SSA, Medicaid, and law enforcement agencies.

How do you know?

- Quarterly security audits now pass with no major findings (down from 6 in 2023).
- Simulated phishing test failure rate dropped from 21% to 3%.
- Mean time to detect (MTTD) and mean time to respond (MTTR) metrics show over 85% improvement.
- Staff training participation rate rose from 62% to 98%.

Testimonial: "This initiative gave us peace of mind. We handle some of the most sensitive information in state government, and now we know it's protected by world-class cybersecurity." – Regional Program Administrator, DCS

What now?

DCS is now:

- Expanding zero-trust model to mobile devices and field staff
- Integrating AI-based anomaly detection into the security platform
- Launching shared threat intelligence partnerships with other agencies
- Scaling policy-as-code models across all infrastructure

The Cybersecurity Modernization Initiative ensures DCS can meet tomorrow's cyber threats with resilience, agility, and confidence.