NASCIO STATE IT RECOGNITION AWARDS

Modernizing & Securing Critical Public Safety Infrastructure

CATEGORY
Cross-Boundary Collaboration

START DATE
July 1, 2020

END DATE
May 5, 2024

COLORADO
Governor's Office of Information Technology

Brandi Wildfang
Chief Communications Officer & PIO
brandi.wildfang@state.co.us
720-601-5470

Yvonne Quest
Program Manager
yvonne.quest@state.co.us
720-557-7926

EXECUTIVE SUMMARY

The Colorado Crime Information Center (CCIC) system is a vital linchpin for information sharing among 23,000 users across 23 Colorado criminal justice agencies. CCIC provides access to state and national crime information databases, including FBI CJIS, Nlets, and state motor vehicle data. The system faced significant challenges due to aging and unreliable hardware, and an outage would be catastrophic, resulting in law enforcement agencies losing access to critical information, hindering their ability to perform duties effectively. Recognizing the risk to public safety and potential disruptions to law enforcement operations, the Governor's Office of Information Technology (OIT), in collaboration with the Colorado Department of Public Safety (CDPS) and Colorado Bureau of Investigation (CBI), initiated a project to modernize the system by migrating it to a vendor-hosted cloud environment with improved disaster recovery capabilities.

The project plan involved a phased approach over an extended period, including hardware upgrades, migration to a vendor-hosted cloud data center in Chicago for geographic diversity, and establishing a new Disaster Recovery (DR) environment. However, the project encountered immediate challenges, including protracted contract negotiations and a nine-month delay in hardware deliveries due to the COVID-19 pandemic. In May 2024, aging infrastructure and a renewed focus on modernizing and better securing state IT infrastructure led to an accelerated migration to the new cloud environment.

Under the leadership of OIT's Program Manager, OIT and CDPS/CBI teams, the vendor and various other partners executed a rapid and successful migration in just nine days, showcasing extraordinary dedication and collaboration. This ensured continuous access to vital information for law enforcement and minimized disruption to critical services. The success of this project provides a strong model for other states facing similar challenges in modernizing critical IT infrastructure.

The CCIC Production Cloud Migration project significantly improved system reliability, security and scalability. Key benefits include enhanced disaster recovery capabilities, geographic diversity, increased protection of sensitive data (Criminal Justice Information System [CJIS] data and Personally Identifiable Information [PII]), and streamlined ongoing maintenance and support. By transitioning to a vendor-hosted Software-as-a-Service (SaaS) model, ongoing maintenance and support are ensured, and the state shifts from managing hardware to consuming a managed service.

IDEA

Disruptions to law enforcement operations can severely impact public safety and erode trust. CCIC is a critical system that supports information sharing across 23 criminal justice agencies and is used by 23,000 professionals. However, it was aging and needed updates. In 2019, legislative funding was obtained to migrate the system to a hosted or cloud environment.

The intended outcomes of modernizing the systems were many: 1) reducing the potential for system failures, data loss, and security breaches, 2) disruptions to law enforcement operations, 3) improved interagency collaboration, 4) enhanced reliability and security of data, especially CJIS data and PII, and 5) improved disaster recovery capabilities.

Further, it would address principles universal to all states:

- Maintaining the security and reliability of critical law enforcement information systems.
- Modernizing legacy IT infrastructure.
- Improving disaster recovery and business continuity.
- Protecting sensitive data (CJIS and PII).
- Supporting interagency collaboration and information sharing.

The project, launched by OIT in collaboration with CDPS and CBI, encountered immediate challenges, including protracted contract negotiations and hardware delivery delays caused by the COVID-19 pandemic. A renewed commitment to modernizing IT infrastructure and security across the state reinvigorated this effort.

This migration project addressed a critical business problem: ensuring that law enforcement agencies (LEAs), which rely on essential business systems and processes, could maintain mission-critical operations even during technology failures. The goal was to empower LEAs to respond to incidents and uphold public safety.

Beyond operational continuity, the migration also aimed to improve interagency collaboration and enhance the reliability and security of data, particularly CJIS data and PII. This move bolsters the state's ability to protect sensitive information, foster seamless cooperation among agencies and ensure public trust in our law enforcement agencies and systems.

IMPLEMENTATION

The initial plan was to upgrade CCIC hardware to the vendor's current standards, host CCIC production in a vendor-hosted cloud data center in Chicago (for geographic diversity), and upgrade hardware at an OIT location for improved disaster recovery capabilities. Significant project dates included:

- November 2019: Contract negotiations begin
- May/June 2020: Contract executive
- June 2020: Discovery begins
- July 2023: Test planning and testing begin
- September 2024: Go live

In 2020, unexpected events, including the significant disruption of supply chains resulting from COVID-19 and internal issues, impeded project progress. In July 2023, a new program manager and project team member joined the project, putting it back on track. In May 2024, the project timeline was accelerated, and ultimately, it was completed four months ahead of schedule.

From the beginning, many people were involved in the project, including an OIT Program Manager and various OIT Infrastructure, Security, Network, Service Desk, Deskside Support, and Active Directory & Messaging staff. Other participants included CDPS, CBI, vendors, criminal justice agencies, and local LEAs.

With the strong project manager coordinating the accelerated efforts, managing stakeholders and driving the project, the project management approach was characterized by:

- **Rapid Deployment Approach:** An agile, reactive approach resulting in a nine-day sprint.
- Monitoring and Follow-up: After CCIC was partially restored, potential defects were actively monitored, and follow-up meetings and calls were scheduled, showing ongoing management and attention to the system's health.
- **Collaborative Approach:** Emphasizing epic collaboration among various teams and stakeholders, working closely together for extended periods.
- **Incident Management Approach:** Following incident management procedures with clear communication, assigned roles, and real-time troubleshooting.
- **Phased Approach:** A phased approach to migration was used, even with the accelerated timeline.
- **Vendor Collaboration:** Close collaboration with the vendor (CPI) for hosting, support, and expertise.
- **Monitoring and Follow-up**: After CCIC was partially restored, potential defects were actively monitored, and follow-up meetings and calls were scheduled, showing ongoing

management and attention to the system's health.

Key stakeholders were kept informed throughout the accelerated timeline, both before and after, using communication methods such as briefings, incident reports, agency-specific communication, etc.

The architectural shift from an aging, on-premises hardware setup to a vendor-hosted cloud environment matters for several reasons:

- **Enhanced Reliability and Availability.** The old system was prone to hardware failures due to outdated components. Moving to a cloud-hosted environment provides greater redundancy, reliability, and uptime, ensuring that law enforcement agencies have continuous access to critical information. Why it matters: This directly impacts public safety, as delays or outages in accessing CCIC data can hinder law enforcement operations.
- **Improved Disaster Recovery (DR) and Business Continuity.** The previous DR setup had limitations, making it difficult to fail back after an outage. The new architecture provides geographical diversity, ensuring the system can withstand localized disasters and recover quickly. Why it matters: This safeguards against data loss and extended service interruptions, ensuring law enforcement can continue operating even during major disruptions.
- **Increased Security**. The cloud environment is managed by a vendor specializing in data center security and is likely to have more robust security measures than the previous on-premises setup. This is especially crucial for protecting sensitive data like CJIS information and PII. Why it matters: Protecting this sensitive data is paramount for maintaining public trust and complying with regulations. Security breaches could have severe consequences.
- **Modernization and Scalability.** The old hardware was aging, unsupported and incapable of handling increasing demands. The new architecture provides a modern platform that can be scaled as needed, ensuring the system can continue to support the growing needs of 23,000 users across 23 criminal justice agencies. Why it matters: This ensures that the system remains effective and efficient, allowing law enforcement to adapt to evolving challenges and information needs.
- **Support for Interagency Collaboration.** CCIC acts as a central hub for information sharing among various agencies. The new architecture supports this role by providing a robust, reliable, and secure platform for exchanging data, enhancing interagency collaboration. Why it matters: Effective collaboration is essential for coordinated law enforcement efforts and efficient criminal justice operations.

IMPACT

An outage of the critical CCIC would mean law enforcement agencies losing access to vital information, hindering their ability to perform their duties effectively. The CCIC Production Cloud Migration project significantly improved the system. It also enhanced public safety by ensuring the reliability and availability of CCIC, the backbone of information sharing for 23,000 users across 23 criminal justice agencies. Further, the quick response to the May 2024 hardware damage minimized disruption and prevented potentially severe consequences for law enforcement operations.

Before the Project	After the Project
• Aging, unreliable and unsupported hardware. • On-premises data center with limited disaster recovery capabilities. • Risk of system failures, data loss and security breaches. • Potential for significant disruptions to law enforcement operations. • Single point of failure with no geographical diversity.	• Modern, vendor-hosted cloud environment. • Improved disaster recovery and business continuity. • Increased security, particularly for CJIS and PII data. • Enhanced reliability and availability of the CCIC system. • Geographical diversity with production in Chicago and backup in Colorado. • More scalable and maintainable infrastructure.

The key stakeholders - the Colorado Department of Public Safety and the Colorado Bureau of Investigation - are pleased with the outcome. Each year, the CBI holds an awards ceremony to recognize its employees who contributed to the Bureau's greatest accomplishments of the year. In October 2024, CBI named OIT's Program Manager Yvonne Quest as the recipient of their CBI Award of Appreciation, noting, "Not only did she assist and guide our testing process, during the week of migration, Yvonne worked around the clock to help gather OIT and vendor resources needed to connect Colorado Law Enforcement Agencies and would not take no for an answer. Her tireless efforts pushed the migration to the finish line."

This project is worthy of the initial and ongoing investment because it safeguards a critical law enforcement resource, ensuring public safety across Colorado. The CCIC system is essential for information sharing among users, and its reliability and security are paramount. The initial investment addressed the urgent problem of aging hardware and potential system failures, preventing significant disruptions. Ongoing investment is justified to maintain the modern cloud

environment, ensure robust disaster recovery, and protect sensitive data. Without this investment, the state risks system outages, data loss, security breaches, and diminished law enforcement capabilities, severely affecting public safety and trust in government. Therefore, continued investment is essential to ensure CCIC remains a robust and reliable resource for Colorado's criminal justice agencies:

- Ongoing Maintenance: The vendor will provide ongoing support and maintenance for the CCIC system in the cloud environment.
- Disaster Recovery Plan: Continue maintaining and testing the upgraded disaster recovery environment.
- Monitoring and Security: Continuous monitoring of the system's performance and security, ensuring compliance with CJIS and PII regulations.
- Scalability: Plan for future scalability to accommodate the growing needs of the 23,000 users and 23 criminal justice agencies.
- Updates and Upgrades: Implement a process for regular updates and upgrades to the CCIC system to ensure it remains current and effective.