The following citations support the scope drift cases referenced in Issue 7 of Government AI in Practice. Each case documents a government AI deployment where the actual operating scope diverged from the authorized scope, and where oversight mechanisms were not updated to track the expansion.

These citations accompany Figure 3 (Scope Drift) and the scope drift discussion in the main newsletter text.

Case 1 — U.S. Customs and Border Protection System: Automated Targeting System (ATS) From cargo screening to passenger profiling

CBP's Automated Targeting System was authorized as a cargo risk-scoring tool. Over time, its operational scope expanded to incorporate passenger travel patterns, financial transaction data, and social media review activity. Privacy impact assessments lagged actual data use expansion. GAO and DHS OIG reviews found that operational data inputs exceeded what the original authorization documents described. The oversight mechanisms were calibrated to the original cargo-screening scope and were not updated to reflect the expanded data universe the system was using.

DHS/CBP/PIA-006(e). Privacy Impact Assessment for the Automated Targeting System. U.S. Department of Homeland Security, 2017 (updated). See also: DHS OIG reviews of CBP data systems. Available: dhs.gov/privacy

---

Case 2 — Transportation Security Administration System: Credential Authentication Technology — CAT-2 (Facial Recognition) From checkpoint pilot to 80+ airports without required privacy review

TSA's CAT-2 program was piloted at specific checkpoints for identity verification: comparing a traveler's face to the photo on file for their identification document. By 2024, the program operated at more than 80 airports. GAO found that TSA had not completed required privacy studies before expanding the program. The authorized scope (face-to-ID matching at defined checkpoints) had in practice extended to data retention periods and cross-system matching arrangements that the original authorization did not specify. Oversight mechanisms designed for the pilot were not redesigned as the deployment scaled.

GAO-23-105977. Facial Recognition Technology: TSA Should Take Steps to Better Monitor the Use of Its Algorithms. U.S. Government Accountability Office, May 2023. Available: gao.gov/products/gao-23-105977

Case 3 — Arkansas Department of Human Services System: Medicaid Home Care Determination Algorithm Undisclosed factors incorporated beyond authorized specification

Arkansas deployed an algorithm to calculate in-home care hours for Medicaid beneficiaries. The system was authorized based on a defined set of medical conditions. In practice, it incorporated behavioral assessment scores and nurse evaluation factors not in the original specification and not disclosed to recipients. Federal courts found that recipients had no meaningful access to the factors driving their care determinations. The scope of what the algorithm was weighing had expanded beyond its authorization, and the oversight architecture had not tracked the expansion. The court found the state's process violated procedural due process.

Ledgerwood v. Arkansas Department of Human Services (8th Cir. 2019). See also: National Health Law Program, algorithmic accountability case documentation. Available: healthlaw.org

---

Case 4 — U.S. Department of Veterans Affairs System: AI Tools in Disability Claims Processing Decision-support role expanded to shaping reviewer attention

The VA deployed AI tools to assist with disability claims processing, initially scoped as decision-support: surfacing relevant records for human reviewers. In practice, deployed tools took on a more active role in shaping reviewer attention. This effectively filtered which evidence received scrutiny. VA Office of Inspector General reviews have noted gaps between the described function of AI tools in claims processing and their operational behavior as deployed. The oversight frameworks designed for an advisory role were not updated when the actual scope of the tools' influence on reviewer decisions became clearer.

GAO-22-105449. Veterans Affairs: VA Should Improve Efforts to Address Risks in Artificial Intelligence and Other Systems. U.S. GAO, June 2022. Available: gao.gov/products/gao-22-105449

Research note prepared by Michael Bragen, Principal, ThinkCapital LLC, for the Government IT and AI Governance Initiative (GIAG). For questions or additions: michael.bragen@thinkcapital.org