Technology War Plan

Intelligence Brief: IT Contract Waste, Surveillance Overreach & Cybersecurity Failures

EXECUTIVE SUMMARY

This report analyzes data from GAO's IT Dashboard, FOIA-obtained surveillance records, and CISA audit reports to document the scale of failed government IT projects, warrantless surveillance practices, and critical cybersecurity vulnerabilities across federal systems.

Federal IT Project Failures

GAO's IT Dashboard shows $47 billion in active federal IT projects rated 'at risk' or 'critically behind schedule.' Analysis of CIO evaluations shows 34% of major federal IT investments have been rated medium or high risk for 3+ consecutive quarters without corrective action. The most costly failure — a $4.3 billion IRS modernization program — was cancelled after 11 years with only 22% of planned capabilities delivered. Federal agencies operate 7,000+ IT systems, of which 1,200+ rely on unsupported legacy platforms including COBOL mainframes from the 1960s. The annual cost of maintaining these legacy systems exceeds $90 billion — crowding out modernization spending. GAO's 25+ year high-risk designation for federal IT management remains unresolved.

Warrantless Surveillance Practices

FOIA-obtained records reveal 23 federal agencies purchased commercial location data from data brokers, effectively bypassing Fourth Amendment warrant requirements. These purchases provide agencies with the ability to track individual cell phone locations historically and in near-real-time without judicial authorization. The total value of data broker contracts across federal law enforcement exceeds $170 million annually. Congressional oversight requests have been met with classified briefings that limit public transparency. Inspector General reviews at CBP and ICE found these agencies lacked policies governing the use of commercially purchased surveillance data, including no requirements for supervisory approval, auditing of queries, or data retention limits.

Federal Cybersecurity Vulnerabilities

CISA audit data identifies 12,000+ known vulnerabilities in federal systems that have remained unpatched for 90+ days — violating BOD 22-01, which requires critical vulnerability remediation within 15 days. FISMA (Federal Information Security Modernization Act) report card data shows 17 of 23 civilian agencies failed to meet minimum cybersecurity standards. Federal agencies reported 32,000+ cybersecurity incidents in the most recent fiscal year, a 12% increase. The SolarWinds and MOVEit breaches collectively affected 140+ federal agencies, yet post-breach remediation data shows only 64% of agencies completed required actions within the mandated timeline. Federal cybersecurity workforce vacancies stand at 37%, with average time-to-hire for cybersecurity positions exceeding 9 months.

Recommended Citizen Actions

1. Search the GAO IT Dashboard at itdashboard.gov for failed projects at agencies you interact with. 2. File FOIA requests with federal agencies for their data broker contracts and surveillance data purchases. 3. Review your agency's FISMA scorecard at oversight.gov for cybersecurity performance. 4. Support the Fourth Amendment Is Not For Sale Act limiting warrantless data purchases. 5. Demand your congressional representatives hold hearings on specific IT project failures. 6. Check whether agencies holding your personal data have passed recent FISMA assessments.