Red Teaming and Penetration Testing for the Administrative Office of the U.S. Courts

The Administrative Office of the U.S. Courts had to coordinate security across 22 interconnected subsystems holding sensitive legal data while maintaining continuous authorization. InterSec ran red team and penetration testing with policy review and user education to keep the judiciary's systems assessment-ready.

CLIENT	PROFILE	STATUS
Administrative Office of the U.S. Courts	Technology and operations for the federal courts nationwide	Completed

22
Interconnected subsystems secured

100%
Continuous authorization held

FISMA + DOJ
Requirements fully met

0
Authorization lapses

ENVIRONMENT	MANDATES	METHOD	HUMAN LAYER
22 interconnected subsystems	DOJ requirements and FISMA	Red team and advanced pen testing	Policy review and training

THE CHALLENGE

The office faced coordinating security across many subsystems while keeping judicial functions running without interruption. Three factors made it hard: the subsystem architecture was complex, the data sensitivity was extreme with legal documents and judicial records, and the regulatory environment, DOJ mandates and FISMA, required maintaining authorization to operate at all times.

THE APPROACH

InterSec deployed a systematic red team strategy, paired with policy reviews and user-awareness training, so each subsystem was tested against both external attackers and insider threats. The work combined red team simulations that replicated sophisticated attacker tactics, policy and user education addressing the human layer, and iterative risk assessments that kept authorization readiness current as the environment changed.

> **An architecture only reveals its weakest path when someone is paid to hunt for it.**

THE SOLUTION IN PRACTICE

InterSec used advanced penetration testing tools and documented each finding, delivering targeted remediation steps rather than a raw vulnerability list. The team helped the office simplify maintaining and renewing authorization, reducing documentation friction. Staff training equipped personnel to recognize and resist social engineering, and red team exercises probed the subsystems the way a real adversary would, surfacing issues conventional testing tends to miss.

RESULTS & IMPACT

- ✓ Issues exposed by the red team exercises were patched promptly.
- ✓ Continuous authorization was maintained across all 22 subsystems.
- ✓ DOJ and FISMA security and privacy requirements were fully met.
- ✓ A more secure environment upheld the strict standards of the federal judiciary.

KEY TAKEAWAYS

Red teaming finds what scans miss.
Replicating real attacker tactics surfaces the chained weaknesses a checklist-based test passes over.

The human layer is part of the attack surface.
Phishing and data-handling training close the gap technical controls cannot.

Authorization is maintained, not achieved once.
Iterative risk assessments keep a complex multi-subsystem environment continuously ready.

Findings need remediation steps, not just ratings.
Targeted, documented fixes are what turn a test into an improvement.

CAPABILITIES DEMONSTRATED

Red Teaming | Advanced Penetration Testing | Policy Review and User Education | FISMA and DOJ Compliance | ATO Maintenance

Protecting sensitive systems across a complex architecture takes testing that thinks like an attacker.
InterSec runs red team and penetration testing programs for federal organizations that must stay authorized.

Let's talk →