

Built Into Every Release: Application Security Testing Aligned to the SDLC for a NYS Government Agency

CLIENT TYPE**NYS Government
Agency****ENGAGEMENT****Embedded AppSec
Testing****PROGRAM****Legacy Mainframe
Modernization****DURATION****Multi-Year, Phase-
Gated**

01 The Challenge

A NYS Government Agency was in the middle of a multi-year effort to replace a legacy mainframe system serving hundreds of thousands of members, employers, and beneficiaries with a new, modern web application. The system was rolled out in phases, each adding significant new functionality, from self-service registration through benefit calculation, enrollment, and payment processing. With that much surface area changing continuously, security testing couldn't be a one-time, end-of-project checkbox. It had to move at the same pace as development, or risk becoming the bottleneck that delayed a critical modernization program relied on by the public.

02 Our Approach

Cyber Castellum was brought in as the embedded application security testing partner for the program, structuring testing around the software development lifecycle itself rather than a fixed calendar date:

● Phase-Gated Testing

Each major release phase, from initial self-service functionality through more complex benefit calculation, enrollment, and payment features, was tested as its own scoped effort before moving forward, so new capabilities were vetted before reaching production.

● Development-Through-Production Methodology

Testing followed the code through the pipeline: starting on the development system, continuing through regression testing as fixes were applied, and concluding with validation in production.

● Standards-Based Application Testing

Every workflow and user role was tested with automated tooling and manual exploitation, benchmarked against the OWASP Top 10, and run both with and without valid credentials to catch authorization gaps a scanner alone would miss.

Closed-Loop Remediation

Every identified vulnerability was retested as its own dedicated task after remediation, so fixes were verified to actually hold before a phase was considered complete.

03 **The Results**

Across multiple release phases spanning several years, Cyber Castellum identified and validated the remediation of vulnerabilities in each new set of application features before they reached end users, protecting a system that directly touches the financial security of the people who depend on it. The agency has continued the partnership across every phase of the program, including the final phase retiring the legacy mainframe system entirely.



Security testing structured around the SDLC itself, not treated as a final gate before launch.

04 **The Impact**

By structuring security testing around the SDLC itself rather than treating it as a final gate, the agency was able to modernize a mission-critical legacy system on schedule, with confidence that each new capability was tested under real-world conditions and verified after remediation before it reached the people relying on it.

KEY TAKEAWAY

Embedding security testing into the release cadence — not the project timeline — let a mission-critical modernization program ship on schedule without trading away assurance.

ABOUT CYBER CASTELLUM

Cyber Castellum specializes in SDLC-integrated application security testing and penetration testing for government agencies undergoing large-scale system modernization across New York State.