New York Health Exchange Client Turnaround

ICF International

VALUE / SCOPE **$15M+ contract saved and expanded**

SITUATION

As the executive overseeing operations for the New York Health Exchange, I was responsible for a mission-critical dual-6500 Cisco HA environment supporting statewide health enrollment, claims processing, and marketplace transactions. The platform was governed by one of the most punitive SLAs in the industry—a $1,000-per-minute outage penalty—creating significant operational, financial, and political risk. During one of the Exchange's peak enrollment periods, the entire system unexpectedly crashed. The HA architecture failed to fail over, disabling all services. This triggered immediate alerts to our CEO, Dave Z., and escalations to the Office of the Governor. Within the first hour, it was clear the financial exposure was severe; by the time the event was over, the downtime reached 21 hours, resulting in $1,260,000 in SLA penalties.

TASK

I was accountable for leading the organization through the crisis—restoring the Exchange as quickly as possible, coordinating all technical and executive communication, managing vendor escalation, containing financial impact, and maintaining credibility with the Governor's office. My role required not only directing real-time engineering actions but also demonstrating command presence under highly visible, politically charged circumstances.

ACTION

I immediately activated our major-incident response framework. I opened a dedicated technical bridge and pulled in every Tier-3 network engineer with Cisco 6500 expertise. In parallel, I escalated directly to Cisco's TAC, demanding senior-level support. To manage communication at the executive and political levels, I established a separate management bridge with 10-minute rolling updates, which our CEO joined hourly before briefing the Governor.

When engineering attempted a manual failover to the secondary 6500 chassis, we discovered that the GBIC modules were also failing. Multiple replacement GBICs were installed, each failing in the same manner. Suspecting spanning-tree instability or route flapping, we performed rapid diagnostics with Cisco TAC but found no conclusive root cause. New hardware tests continued to fail. Cisco still had no actionable explanation, and the outage persisted.

Recognizing the gravity of the situation, I escalated aggressively to Cisco executive leadership and ordered brand-new 6500 chassis, Supervisor Engines, line cards, GBICs, and power supplies to be emergency-shipped and delivered within four hours. When the new equipment arrived, I directed a full rebuild—installing the new chassis pair, loading sanitized configurations, validating routing and HA behavior, and migrating NY MED services to the new platform. This restored full service after 21 hours of outage, limiting additional SLA exposure.

Immediately after stabilization, I initiated a high-severity Cisco Engineering Failure Analysis (EFA)—a costly, rarely authorized deep-engineering investigation. One week later, Cisco confirmed a defective manufacturing batch in certain Supervisor Engines. Using the serial-number range provided, I directed a full enterprise inventory analysis and identified vulnerable Supervisor modules deployed at DHS Stennis, CBP ENNS, and a major Intelligence Community program. I demanded complete hardware replacement at each site and scheduled controlled maintenance windows to eliminate the risk of widespread failures.

RESULT

The New York Health Exchange was fully restored, and despite the $1.26M SLA penalty, we retained the customer's trust due to the transparency, discipline, and rigor of the incident command structure. The Governor's office acknowledged the responsiveness and completeness of the communications, and our CEO commended the leadership and escalation strategy. More importantly, the post-incident engineering audit prevented three additional outages across high-visibility Federal programs, safeguarding tens of millions in potential SLA exposure and strengthening our enterprise-wide reliability posture. The incident reinforced our credibility with the State and demonstrated my ability to lead through complex technical crises while coordinating executive, vendor, and engineering alignment under extreme pressure.

randy.l.james@gmail.com (703) 909-7546 linkedin.com/in/randyjamescybernetops