Carrier Corporation
13995 Pasteur Boulevard
Palm Beach Gardens, Florida 33418

The attached document is a Letter of Attestation of the independent security evaluation performed for Carrier Corporation WebCTRL 10.0, dated September 22, 2025.

This Letter of Attestation is confirmation that Tangible Security has worked with Carrier Corporation, as a third-party security company, to provide a penetration assessment for WebCTRL 10.0 from August 4, 2025 to August 8, 2025.

Sincerely,

Cody Margaretten, PMP
Chief Operating Officer
7048 Knightdale Blvd
Suite 220B
Knightdale, NC 27545
Mobile: 919-999-7418

Carrier Corporation WebCTRL 10.0

Who is Tangible Security

Since 1998, Tangible Security has served the Defense, Intelligence, Federal, Civilian and Corporate sectors with both enterprise and product cyber security services. We provide adversary-centric assessments of cyber security posture and readiness with respect to industry best practice frameworks. In addition to policy, process and posture, we supplement client personnel skill-sets as well as knowledge in cyber security technologies. Our personnel set us apart. They have served on classified projects, written industry leading books, presented at cyber security conferences, conducted original research and participated on expert panels.

Tangible Security has provided the highest level of security services to clients that range from Las Vegas Casinos to Global 500 corporations. We serve the healthcare, energy, manufacturing, financial, hospitality, retail, and other industries.

Third Party Security Evaluation

Tangible Security has worked with Carrier Corporation, as a third-party security company, to provide a penetration assessment for WebCTRL 10.0. A penetration assessment was performed within a predetermined time constraint and focused on common vulnerabilities.

The assessment resulted in no critical or high issues. Overall, Tangible Security assessed the WebCTRL 10.0 system at a **Low** risk.

The following represents a high-level overview of the validation activities performed during the assessment:

- Authentication Mechanism and Verification attacks
- Roles and Permission, Federation of duties
- 3rd party inclusions
- API Interactions and Fuzzing
- User input validation
- Storage of sensitive data
- Application Fuzzing
- Business Logic Exploitation
- Network Protocol Fuzzing
- Resilience Testing (Denial of Service)
- Casual Inspection of applications communication
- Unauthorized Access
- Web application (OWASP)
- Logging and Export
- Insecure Configurations
- Information Disclosures

To perform the assessments, generally a gray-box testing approach was taken. The components of the WebCTRL 10.0 product that were in scope are as follows:

- OWASP Top 10 testing of the WebCTRL 10.0 web application.

Summary

The WebCTRL 10.0 system has undergone an independent third-party security evaluation. *Tangible's process uses internally developed testing methodologies, which are aligned with industry best practices.* In addition to these testing methodologies, business logic and application logic testing was conducted against the deployment to identify unique, uncommon, and often-unforeseen weaknesses.

Penetration testing methodologies were performed on the WebCTRL 10.0 system.

Details on the security and vulnerability findings across all the WebCTRL 10.0 components were provided to Carrier Corporation.

I hereby affirm that the above security evaluations were conducted against WebCTRL 10.0 provided by Carrier Corporation based on the scope defined within this Letter of Attestation, at the time such evaluations were performed. Any upgrades or changes to the product assessed within the scope of this attestation are excluded from this Letter of Attestation.

Cody Margaretten, PMP

Chief Operating Officer

James Baucom

Lead Security Consultant