May 15, 2025

RE: Rancher Government Solutions RKE2

To Whom It May Concern:

Corsec Security, Inc. has conducted an analysis of the Rancher Government Solutions RKE2 1.33+, assessing product operations for the Federal Information Processing Standard Publication 140-3 (FIPS 140-3). Corsec attests that RKE2 1.33+ has incorporated FIPS-Approved cryptographic services provided entirely by FIPS 140 validated modules and **PASSED** Corsec's **FIPS Verified** process. The Rancher Government Solutions product implements all cryptographic functions inside of a FIPS 140 validated cryptographic module.

As issued by the National Institute of Standards and Technology (NIST), FIPS 140-3 specifies the security requirements that must be satisfied by a cryptographic module used in a security system protecting sensitive but unclassified (SBU) information. Corsec has reviewed the architecture, features, operations, and testing results performed in Rancher's development facilities and provides the following conclusions:

- RKE2 1.33+ has implemented the use of an embedded validated cryptographic module and/or incorporated validated modules

- RKE2 1.33+ is utilizing the Google BoringCrypto module that has been validated against FIPS 140-3 Level 1 requirements and has been awarded certificate #4735.

- All cryptographic algorithms utilized in RKE2 1.33+ are FIPS-approved cryptographic algorithms

For any additional information I can provide on this matter, please do not hesitate to call me at (703) 267-6050.

Sincerely,

Matthew Appler
CEO, Corsec Security, Inc.