February 7, 2025

RE: FIPS 140-3 Compliance

Ascom Americas
300 Perimeter Park Drive
Morrisville, North Carolina 27560
USA

To Whom It May Concern:

This letter is in reference to the readiness of Ascom's Myco 4 smartphone for operation in a FIPS-compliant manner.

As issued by the National Institute of Standards and Technology (NIST), the Federal Information Processing Standard Publication 140-3 (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. Cryptographic modules can achieve FIPS-validation by undergoing a rigorous evaluation process overseen by the Cryptographic Module Validation Program (CMVP), co-sponsored by NIST and the Canadian Centre for Cyber Security (CCCS).

To support claims of "FIPS compliance", Corsec ensures that a vendor's product or solution has some or all of its cryptographic security functions provided exclusively by cryptographic sources with active FIPS validations. The crypto source could be integrated into the product's application code or leveraged from the product's operational environment. Further, the product should employ the validated source(s) strictly according to the guidance specified in the cryptographic module's published Security Policy.

Ascom is a world-leading supplier of critical, near-real-time solutions for highly mobile, ad hoc and time-sensitive environments, and is a global solutions provider focused on healthcare information and communications technologies (ICT) and mobile workflow solutions. Ascom offers a uniquely comprehensive portfolio of products and services including smartphones, DECT and VoWiFi phones, nurse call systems, pagers, apps, and the Digistat and Unite software suites.

Ascom's Myco 4 smartphone leverages FIPS-Approved cryptographic services (including symmetric encryption/decryption, digital signature functions, hashing, message authentication, cryptographic key generation, and key derivation) from FIPS-validated sources. Based on a review of product architecture, features, operation, and testing results performed in Ascom's development facilities, Corsec Security, Inc. has made the following determinations:

- The Myco 4 smartphone (running the Android 14 operating system) implements cryptographic services provided by Google's BoringCrypto.

  BoringCrypto is a software library providing a C-language application program interface (API) for use by applications that require cryptographic functionality. BoringCrypto (version 2023042800) completed a FIPS 140-3 level 1 validation on 1/26/2025. The validation was awarded validation certificate #4953 and has a sunset date of 1/25/2027.

- The Myco 4 smartphone does not implement any additional FIPS-Approved security functions within the vendor-developed product software. All FIPS-Approved cryptography is leveraged from the source noted above.

- Usage of any non-Approved cryptographic algorithms within the Myco 4 smartphone is limited to non-security-relevant operations and non-FIPS-related services.

In summary, when operated following all applicable guidance provided in the Security Policy document for the validated module noted above, Ascom's Myco 4 smartphone has been deemed **COMPLIANT** by Corsec's "FIPS Verified" evaluation for FIPS 140-3 compliance. It is the user's responsibility to follow all applicable operator guidance provided in the validated module's Security Policy to ensure compliant operation of the device.

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

Sincerely,

Digitally signed by John Morris
Date: 2025.02.07 15:03:16 -05'00'

John R. Morris
President, Corsec Security, Inc.

JM:hs