COMPREHENSIVE SECURITY PROVIDED BY THE MOBILITY EDGE™ PLATFORM

Honeywell's cybersecurity provided by the Mobility Edge Platform has received prestigious recognitions from the United States Department of Defense.

Honeywell

TABLE OF CONTENTS

INTRODUCTION

In a technology-based world, the Mobility Edge™ Platform's ability to deliver unsurpassed security, provides customers at the highest levels with the durability and confidence they need to operate safely. The U.S. Department of Defense recognized Honeywell for its security through the Mobility Edge Platform with the gold standard in security designations – a Security Technical Implementation Guide (STIG).

Following a two-year series of ever-increasing cybersecurity milestones, Honeywell has been awarded the STIG certification for the Mobility Edge platform ruggedized mobile computers (i.e., CT40, CT40XP, CT60, CT60XP, CN80, CN80G, CK65, RT10A, and Thor™ VM1A, and VM3A.) and can now be listed on the DoD Approved Products List (APL).

This is the green light that allows Honeywell-approved devices to be plugged into the DoD Information Network. The CN80G was the very first ruggedized device ever to be listed on the APL.

What is unique for this certification is that it's on the Honeywell Android Mobility Edge platform, and not just on one device. This affirms the Mobility Edge platform's strength and design as a true platform and top choice for DoD and commercial enterprises.

WHAT IS A STIG

1

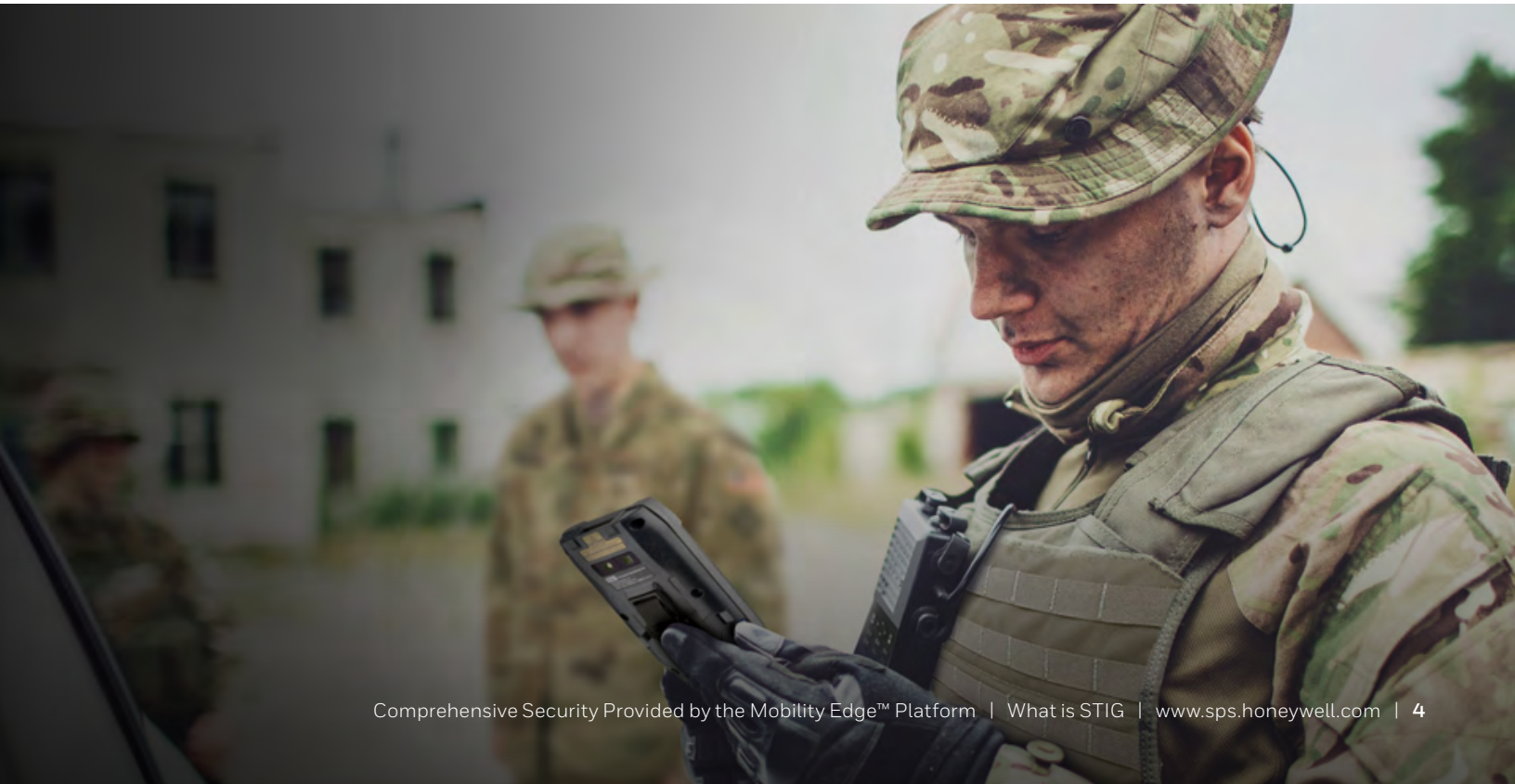
The United States Department of Defense (DoD) cybersecurity requirements are among the most stringent in the world and are established by the Defense Information Systems Agency (DISA).

These standards, referred to as STIGs (Security Technical Implementation Guides), help prevent unauthorized access and malicious attacks by fortifying and protecting information systems and software.

STIG is the criterion DoD organizations set themselves for standardizing security protocols with networks, servers, computers and more. Before they are allowed on their networks, all DoD IT assets must meet STIG compliance, thus proving they can provide configurable operational security guidance for products being used by the DoD.

STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which support system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF).

Various DoD agencies use STIGs to configure and assess a product's security profile, and determine authorization to operate these products, ensuring confidentiality, integrity, and availability of the DoD Information Network (DoDIN) for the warfighter.



WHAT STIG MEANS TO HONEYWELL CUSTOMERS

2

While Honeywell's STIG certification is an essential milestone for working with the DoD, it also provides assurances to our world-wide customer base that Honeywell Mobility Edge™ Platform devices can stand up to the strictest of cybersecurity standards. Security is our top priority and we design it into our products, policies, and processes.

Our security built-in, design-to-delivery process has a strong emphasis on programming security into products to anticipate and mitigate risk. We do this by embedding deep domain knowledge of industry-leading security practices throughout our full design and development process to ensure our solutions are as secure as possible from the very beginning.

We also take extra measures like continuous testing, authentication safeguards, and adherence to best programming practices, to safeguard our solutions from attack as much as possible. To continue our focus and lead the way in the industry, we put in place the industry's first Cybersecurity Risk Manager and developed strategic partnerships with leading cybersecurity product vendors, ensuring customers feel safe, protected, and secure in every environment.

STIG CERTIFICATION PROCESS AND SIGNIFICANT MILESTONES

3

To earn this prestigious designation, Honeywell endured an extensive multi-year process of testing and verifying from the DoD. After the initial forms were completed and meetings fulfilled, Honeywell had to prove that their devices were applicable to the security standards of the DoD and could uphold the strict requirements to the highest level.

Honeywell's devices were assessed using a technology-specific DoD Security Requirements Guide (SRG), which reflects what a technology family should be capable of in order to be secure. Honeywell's devices passed with flying colors to earn a STIG, and now reflects what our devices can do in a particular release and possible patch level.

STIG Certification Earned by Passing Significant Milestones
Honeywell gained STIG Certification by meeting and passing significant and rigorous milestones performed in accredited labs. These are independent assessments of the security capabilities of Honeywell devices.

National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) IAW CNSSP #11.
NIAP certification is a commercial cybersecurity product certification mandated by federal procurement requirements (CNSSP 11) for use in U.S. National Security Systems (NSS). Its primary purpose is to certify commercial technology or products which will be used to handle sensitive data.

With the NIAP certification, Honeywell's security features and capabilities of the Mobility Edge platform devices have been evaluated and confirmed by a neutral third-party and verified by NSA's NIAP office. The devices can be used in any of the following applications:

- Intelligence activities
- Cryptographic activities related to national security
- Command and control of military forces
- Equipment that is an integral part of a weapon or weapons system(s)
- Critical to the direct fulfillment of military or intelligence mission (not including routine administrative and business applications).

SIGNIFICANT MILESTONES

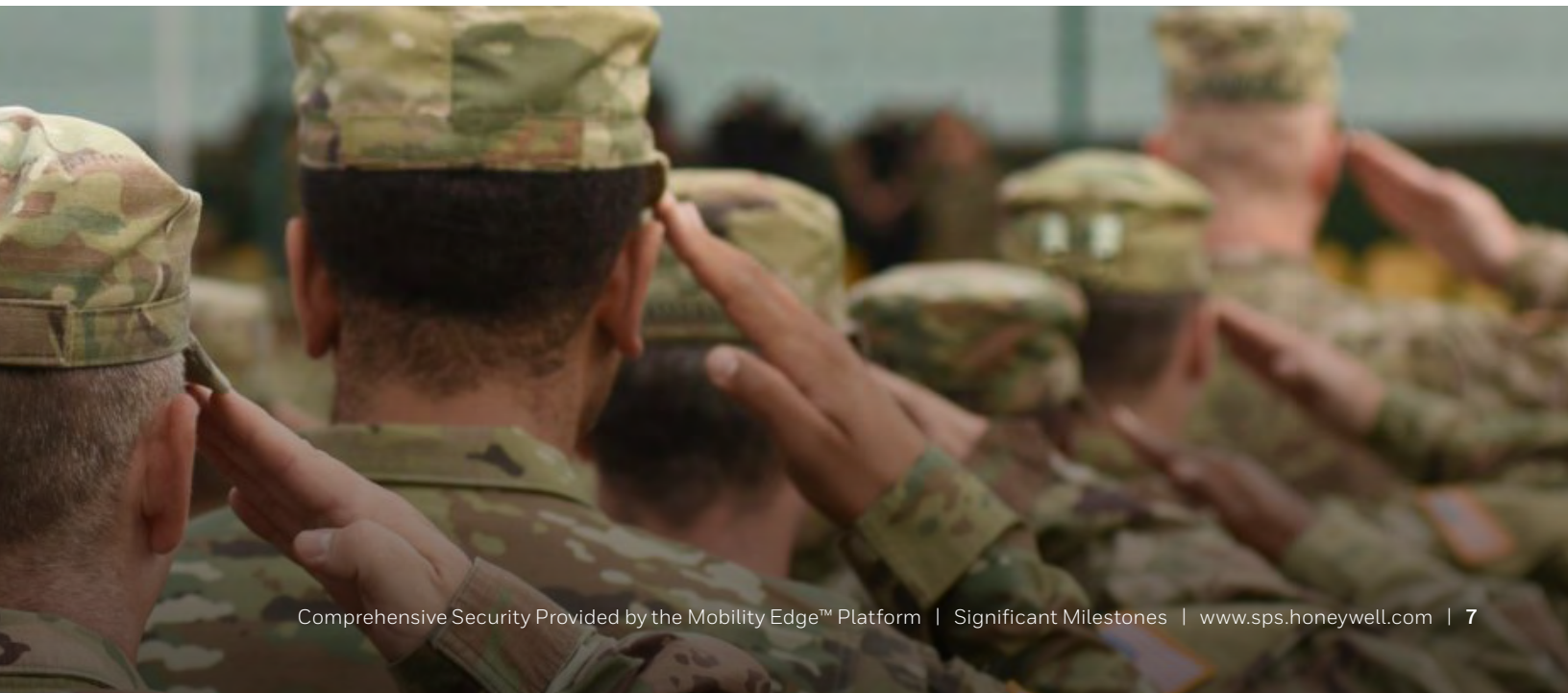
4

National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) IAW Federal/DoD mandated standards.
The agency provides the FIPS certification. FIPS stands for Federal Information Processing Standard, and the FIPS-140 series is a collection of computer security standards set by the National Institute of Standards & Technology (NIST) for the United States government. FIPS-140-2 refers to the benchmark for validating the effectiveness of cryptographic hardware, and is recognized as the best practice for testing and validating cryptographic hardware. FIPS 140-2 certifications:

- Signify that product has been formally tested and validated by the U.S. and Canadian Governments.
- Assures users that a specific technology or hardware has passed rigorous testing by an accredited lab.
- Ensures that the tests have been validated and that the product can be used to secure sensitive data.

DoD Information Network (DODIN) Capabilities and Approved Product List (APL) IAW DoDI 8100.04.
The Department of Defense Information Network (DoDIN) Approved Products List (APL) is the single consolidated list of products that have completed Cybersecurity (CS) and Interoperability (IO) certification.

The DoDIN APL process is used to test and certify products that affect communication and collaboration across the DoDIN and is an acquisition decision support tool for DoD organizations interested in procuring equipment to add to the DISN to support their mission.



THE CN80G: IN A CLASS OF ITS OWN

5

The CN80G was the very first ruggedized device ever to be listed on the APL.

The Honeywell CN80G is a ruggedized handheld computer ideal for logistics, warehouse and field mobility solutions for the United States Government agencies, contractors, and third-parties. The CN80G's rugged construction allows for all working conditions in the most challenging and extreme environments.

The Honeywell CN80G device offers both a large touchscreen and a numeric or QWERTY keypad choice, allowing users to pick the best input method for their environment today and be ready for the touch-centric applications of the future.

The ultra-rugged Honeywell CN80G mobile computer features a fast processor, advanced network connectivity, and enhanced 1D/2D scanning, plus extended battery life lasting twice as long as previous generations to keep workers connected and productive throughout multiple shifts.

The large, vivid, 106.7 mm (4.2 in) touchscreen display can be read easily indoors and out and used with finger, glove, or stylus – making it ideal for warehouse, cold storage, field mobility, and other challenging environments.

5.1 THE CN80G: FEATURES AND BENEFITS

Significant features and benefits of the CN80G include:

- The Mobility Edge hardware platform and enterprise lifecycle tools drive an integrated, repeatable, scalable approach for accelerated and secure development, deployment, performance management, and lifecycle management.
- The Honeywell CN80G device provides future-proof investment protection with support for Android generations, starting with Android 7.1 (N) and extending through at least Android 12.
- The large touchscreen with a 23-key numeric or 40-key QWERTY keypad supports legacy key-centric applications and newer touch applications. Keypads allow input in extremely harsh environments and optimize efficiency in all environments.
- Ultra-rugged construction withstands 3.0 m (10 ft) drops to concrete per MIL-STD 810G and 2,000 1.0 m (3.3 ft) tumbles. IP65/IP67 ratings against dust/water spray.
- Enhanced 1D/2D scanning/data capture with reading ranges of 0.15 m to 15.2 m (6" in to 50' ft) typically required in today's warehouses. Optional scan handle for flexibility to switch between handheld and pistol grip operations.
- The CN80G device is offered with an attachable and dockable common access card reader, or personal identity verifier (PIV), and a full suite of accessories sourced from Trade Agreements Act (TAA) countries to secure the integrity of user data.

MOBILITY EDGE™ PLATFORM

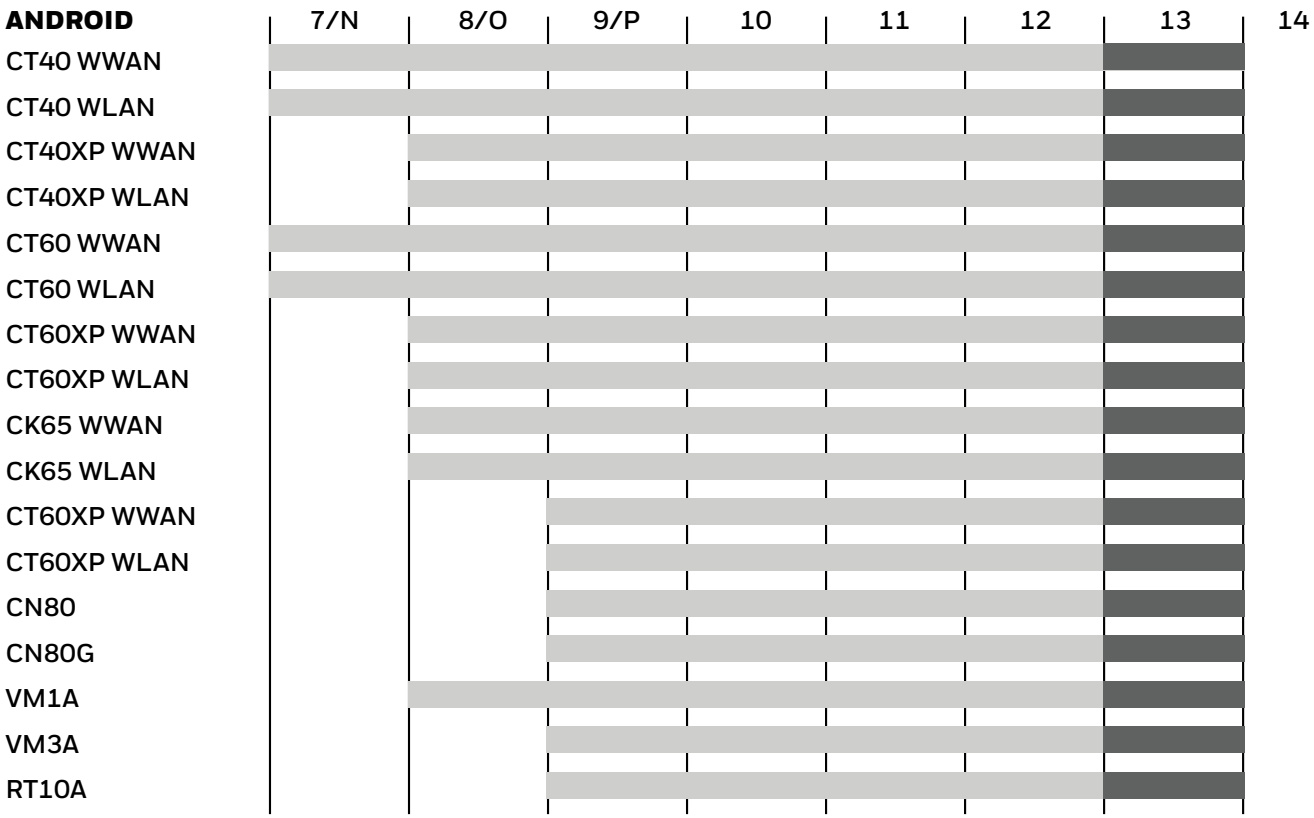
6

Honeywell's Mobility Edge™ Platform delivers an innovative solution to cybersecurity challenges and protection capabilities. Mobility Edge offers an integrated, repeatable, scalable approach to device management based on a common hardware and software platform.

Designed for Android, it delivers a unified platform on which all software solutions are based, enabling businesses to develop and deploy faster while reducing development costs.

Honeywell's commitment to the longevity and quality of the Mobility Edge platform is engrained in the past, present, and future of our products. In fact, Honeywell ruggedized devices on the Android Mobility Edge platform offer the longest lifecycle in the industry with support through at least six Android releases.

Mobility Edge Device OS Version Availability



As with our leadership on Android 12, Honeywell is committed to supporting 13 with reasonable commercial efforts.

The only way to receive the best available Android security and features is through the latest Android version, NOT through backported patches to prior versions.

KEY:

- Availability or guaranteed best security and features
- Committed

CONCLUSION

Honeywell's products are designed from the start to meet Honeywell's rigorous security standards, with security evaluations occurring throughout the development process, identifying and mitigating vulnerabilities even before products are released.

Mobility Edge devices feature a common hardware and software platform, that includes the device's CPU, memory, WWAN (in selected devices), WLAN, Bluetooth® and near-field communication (NFC). They also feature a common OS software image and a common software ecosystem, which includes not only Honeywell software, but also software from Honeywell-approved independent software vendors (ISVs).

Having a common design and OS software image provides flexibility and reduces costs for businesses to deploy additional device form factors because there are no added development or certification costs. Companies can validate all their mobile devices, use cases and software once, and then deploy across multiple devices in multiple form factors, more rapidly and at a lower cost than typical mobile deployments.

Businesses wishing to extend product lifecycle and gain a better return on their technology investment will be assured by the fact that Mobility Edge platform devices can be upgraded through at least Android 12 with a commitment to continuing efforts towards feasibility of Android 13 compatibility.

Honeywell also provides critical security updates for old Android versions, enabling Honeywell customer to patch and upgrade at their own pace.

These dynamic features enable the Mobility Edge Platform to exceed your expectations in device security, product lifecycle management, and total cost of ownership. The Mobility Edge Platform clearly separates Honeywell's devices from competitors on a multitude of levels, proving why our devices have been recognized at the highest levels of security.

The following products are built on the Mobility Edge platform: Honeywell™ CT40, CT40XP, CT60, CT60XP, CN80, CN80G, CK65, RT10A, and Thor™ VM1A, and VM3A.

Read more:

Honeywell Receives STIG from U.S. Department of Defense

CN80G – First Rugged Device to be Placed on U.S. Department of Defense Approved Product List

For more information
www.sps.honeywell.com

Honeywell Safety and Productivity Solutions
300 S Tryon St Suite 500
Charlotte, NC 28202
800-582-4263
www.honeywell.com

Comprehensive Security Provided by the
Mobility Edge™ Platform LTR | Rev A | 04/21

Honeywell