WHITE PAPER: TOUGHBOOK® MOBILE DEVICES

Built In-house for Enhanced Security

Here's why it matters where your device is built

When firefighters, soldiers, and others in-high risk professions put their lives on the line in the course of their duties, they need equipment that won't let them down. That's why they turn to ruggedized, weather-resistant, and impact-resistant mobile devices to communicate, gain situational awareness, and more.

But they also need devices that are as resistant to hacking and data breaches as they are to the physical environment in which they operate. And that's a big reason that where their devices are made is critical for many mobile device users. When it comes to security, where a device has *been* is as important as where it is. This holds especially true for mission-critical functions in the U.S. government, which has codified security into procurement requirements in regulations such as the Trade Agreements Act (TAA).

TAA is an important regulation for systems integrators managing large government contracts in part because it is designed to provide an additional layer of cybersecurity protection for connected devices, reducing security risks introduced in the manufacturing process.

> **Investigators found that a U.S.-based chipmaker had code hidden in its chips during manufacture in China. "It's an example of the worst-case scenario if you don't have complete supervision over where your devices are manufactured."**
>
> **Jay Tabb**, former senior FBI official

IDG Communications Inc.

A recent high-profile case illustrates why TAA matters. Investigators found that a U.S.-based chipmaker had code hidden in its chips during manufacture in China. "It's an example of the worst-case scenario if you don't have complete supervision over where your devices are manufactured," commented a former FBI official in a story about the case.

But ensuring that the devices government agencies purchase originate entirely within TAA-designated countries is harder than it might first appear because many components come from non-compliant jurisdictions for later assembly into devices in a compliant country.

Fortunately, some devices are made entirely in TAA-compliant countries, components included, providing a way for customers to follow both the letter and the intent of TAA.

How Panasonic builds TOUGHBOOK rugged devices

Under TAA terms, only U.S.-made or designated-country end products can be specified for Government Services Administration (GSA)-awarded contracts. So far, so good. But there's a loophole that can create security risks for purchasers, users, and the critical missions under their purview.

Many equipment manufacturers contract the manufacturing of their devices to companies in non-TAA-approved countries. If a customer special-orders a TAA-compliant device, that item then gets pulled off the assembly line in the non-TAA-approved country and is shipped to a TAA-approved country to complete the build process.

Final assembly in an approved country may comply with the letter of the law, but not the intent because—as the microchip manufacturer example shows—bad actors can introduce nefarious code and backdoors early on in the manufacturing process. By the time the components get to the TAA-designated country for assembly, it may be too late to ensure the device's security.

Panasonic closes this loophole by making critical components of its devices for government customers within TAA-approved countries, ensuring security throughout the manufacturing and assembly process. "We design and control the whole supply chain and manufacturing process at the factory," confirms Jeff Henderson, strategic account manager for Army/Special Services at Panasonic.

Panasonic even completes circuit board assembly in its own facilities. That means, in contrast to other devices—whose manufacturers more typically contract this aspect of assembly out to third parties in non-TAA-compliant countries—circuit boards going into Panasonic TOUGHBOOK® devices have their components soldered to the boards in-house.

Panasonic builds its TOUGHBOOK devices on assembly lines owned (and often designed) by Panasonic. The majority of these assembly lines are in Japan and Taiwan—both TAA-compliant countries. Customers need not order special versions of the devices they need because all TOUGHBOOK devices are TAA-compliant—from start to finish.

Complete TAA compliance lets defense agencies and system integrators confidently use TOUGHBOOK mobile devices for mission-critical activities, including situational awareness, logistics, and controlling UAVs

(unmanned aerial vehicles). "We've operated in the tactical space for 25 years," Henderson says. "That includes laptops in tanks, police cars, and aircraft."

As a result of robust security, rugged construction, and reliability in the field, Panasonic devices appear on multiple U.S. government procurement lists, including:

- Air Force AFWay
- Air Force NETCENTS-2
- Army ADMC-3
- Army CHS
- Defense Logistics Agency TLS
- DHS First Source II
- GSA 2GIT BPA
- NASA SEWP V
- Navy NAVSEA MAC
- Marine Corps MCSC
- USDA BPA

Why users rely on TOUGHBOOK devices in the field

Government users rely on TOUGHBOOK® solutions to get the job done when failure is not an option. One example is Panasonic's mission-critical situational awareness solution that combines the TOUGHBOOK N1 Tactical device and ATAK software.

The TOUGHBOOK N1 puts a slim and rugged handheld device running the Android operating system in the hands of soldiers, firefighters, and other users working in extreme conditions. It gives people in tough jobs a versatile, all-in-one tool for communications, situational awareness, and more.

Of critical importance is a long-duration battery. "In real-world world exercises, I've gotten 13 to 14 hours of operation," Henderson says. And that's before swapping out the battery, a capability not typically available on consumer-grade devices. Users can warm-swap in a new battery, meaning they can do so without shutting down the device. And that can mean the difference between success and failure, according to Henderson. "I supported a 72-hour mission last year," Henderson says. "I just gave every soldier an N1 and three batteries, and we did the whole mission on those."

Consumer-grade devices were no match for the elements. "I watched raindrops target our friendly forces. The soldier was trying to target one area and a raindrop was targeting another area. You can see how that could be a big problem."

Jeff Henderson, strategic account manager for Army/Special Services at Panasonic

Built-in multi-carrier voice and cellular capabilities with dual SIM cards and the ability to survive seven-foot drops along with extreme temperatures are among the other features making the N1 ideal for demanding conditions. The touchscreen even functions reliably in the rain and for users wearing gloves, something Henderson says could save lives.

Lives can and do hang in the balance when N1 users depend on an especially critical software platform running on the device: ATAK. Android Team Awareness Kit (in its civilian iteration) or Android Tactical Assault Kit (for military users) lets military and other users locate themselves and others in whatever terrain they find themselves in to collaborate, share information, and communicate via chat and voice. Users can send files, highlight geographical points of interest, and more. ATAK is used to fight fires, conduct rescues, and, as Henderson points out, call in air support for ground troops.

"In ATAK, you can actually call in an air strike from an aircraft," Henderson says. He recalls an exercise in which soldiers used N1 devices alongside consumer-grade devices in the rain to coordinate air support. Consumer-grade devices were no match for the elements. "I watched raindrops target our friendly forces," he says. "The soldier was trying to target one area and a raindrop was targeting another area. You can see how that could be a big problem."

But none of a TOUGHBOOK's advanced features matters without robust security. That means security built-in from the circuit board up.

How built-in security keeps users and data safe

In the case of the TOUGHBOOK® N1 running ATAK, software defenses prevent hackers from gaining access to the device and accessing information about the location of teams, team members, and their mission.

For military applications, much of the security comes from how the device connects to others and to the network. "They'll typically disable Bluetooth and Wi-Fi," Henderson says of mission commanders. "There will be no SIM cards, no way that device connects to anything other than a military radio, and those are typically crypto radio."

Administrators can also constrain functionality to keep data locked down. "One common security vulnerability is an application accessing something on a system that it shouldn't," Henderson says. To close that vulnerability, TOUGHBOOK devices come with sandboxing features that isolate applications from others, giving them data only on a need-to-know basis. For example, if an application has no reason to access geolocation data, the system won't grant that access.

That ability to isolate applies to user access as well. "We can lock a device down to where you only have access to the system tools that you need," Henderson explains. That enhances data security by preventing unneeded applications from running and potentially corrupting or accessing sensitive data.

But software safeguards are only as good as the trustworthiness of the underlying hardware.

As recent cases have shown, backdoors and other hacks introduced in the factory can undermine any software running on a device. "If you deployed ATAK devices, and even though you locked down the communications, something is communicating without your knowledge, that can be problematic," says Henderson. Problematic as in jeopardizing the mission and putting lives at risk.

That's why, along with rugged features such as impact, temperature, and moisture resistance needed for mission-critical applications, complete control over manufacturing may make TOUGHBOOK mobile devices the best choice for meeting government acquisition requirements as well as the intent behind those requirements.

The bottom line

For mission-critical applications with lives on the line, mobile devices with security built-in at the point of manufacture are essential. And where they get built absolutely matters, Henderson says. "Some manufacturers, to check the TAA box, will say, 'Okay, I'm gonna round up all these components from wherever, and then I'm going to put them together somewhere in the U.S.'" In contrast, Panasonic controls the entire supply chain. "So the odds of some malicious component getting into them is extremely unlikely, if not impossible." Panasonic builds the TOUGHBOOK to ensure mission success without compromise, not just check boxes.

Learn more about how TOUGHBOOK mobile devices ensure TAA-compliance for the military and other critical government needs at **toughbook.com**

Panasonic CONNECT