Evaluating Handheld Computing Devices for Support of DoD Operations
The U.S. military was one of the earliest adopters of handheld computers, and is today one of the largest users of the devices. DoD personnel all over the world use wireless handheld computers to take inventory of supplies and equipment, record inspection and maintenance data, manage shipments and support other military operations. Many of these activities take place in remote locations that require specialized, ruggedized mobile computers. While the handheld computers need to be specialized, they also must be standardized to meet the DoD’s specific and demanding information technology (IT) requirements, including the “Gold Disk,” Information Assurance (IA) security standards, DoD 8100.2 specifications and DISA Security Technical Implementation Guides (STIGS).

These specifications and requirements are oriented to desktops and laptops, and are not always applicable to wireless handheld computing devices, which are used primarily for data collection. This white paper is intended to help DoD personnel qualify handheld computers for their operations. It describes the handheld-specific features and functionality required to make devices suitable for use in military operations, and highlights the relevant standards that handhelds must satisfy to be authorized for use in military networks and information systems. This paper also identifies specifications that are not applicable or appropriate for handheld computers, and suggests alternative standards, features and certifications to consider when selecting a device. Finally, the paper describes how handheld computers from Intermec can satisfy military usage requirements and equipment specifications.

Overview: Military Mobile Computer User Needs
Desktop and laptop computers are most commonly used for keyboard-intensive activities such as creating and editing documents, working on spreadsheets, sending e-mail and accessing online material. In contrast, most handheld computing operations are not heavily dependent on key data entry. Software applications provide prompts to users and may ask for only simple confirmations or a few characters of text. For more input-intensive operations, data is collected through integrated bar code, RFID, touch memory or Common Access Card (CAC) readers. These technologies are collectively called automated identification technologies, or AIT. AIT capabilities improve ease-of-use for data collection, ensure data is entered accurately, and greatly reduce the time needed to review entries and correct errors.

Military handheld computers also share many characteristics with their desktop, notebook and laptop cousins. First and foremost is security. Data must be securely stored within the computer, and handhelds must also satisfy all wireless communication and network security requirements. While many applications are unique to handhelds, the application software needs to integrate with central systems, and data must pass seamlessly between mobile devices and headquarters systems.

The security regulations within the U.S. Department of Defense stipulate that all computers operating on DoD networks must comply with established security protocols. These requirements include support for Windows operating systems, 802.11 WiFi wireless network compatibility and data-at-rest (DAR) encryption functionality, all while ensuring compliance with DoD Instruction 8500.1 IA security requirements.

To ensure DoD computers and their operating systems meet established security requirements, the Defense Information Systems Agency (DISA) developed the “Gold Disk.” The Gold Disk is a tool designed to assist developers and system administrators in successfully testing and securing the Windows operating system, desktop applications and Internet Information Services in accordance with the applicable IA standard. These IA standards are identified in the Gold Standard (Gold Policy) as well as DISA STIGS.

The Gold Disk standards set forth for desktop and laptop computers do not completely apply when utilizing handheld computers. Other actions, like software vulnerability scans, can cause confusion as well. Portable devices will not always be powered on, and may not be connected to the network at all times. These differences can raise questions when going through the IA certification and accreditation approval process for mobile devices. This white paper is meant to assist users in simplifying the process.

Standard Microsoft Office applications typically aren’t used on handheld computers, and both the application software and underlying operating system for handhelds differ from those on laptops and desktop PCs. The Windows Mobile operating system is highly advantageous for use on handheld computers, because it has received multiple DoD security certifications and has many compatibilities with the Microsoft Windows operating systems that are approved on the Gold Disk. Windows Mobile is the leading handheld computer operating system, is widely supported with commercial-off-the-shelf (COTS) software tools and applications, and offers stability and flexibility for developers and system support staff. Many of the same development tools and management systems used for desktop and laptop Windows operating systems can also be used for Windows Mobile devices, which enables IT support personnel to work in familiar environments and leverage existing skills without having to learn additional programming languages.

As noted, usage environment is another key difference between handheld and desktop PCs, and is an important factor in device selection. Handhelds are frequently used outdoors in all conditions, they must be extremely rugged, weather sealed, reliable and easy to use, since there may be no tech support in the vicinity. Handheld computers also need long-life batteries for all day operation in the field, and enable a simple battery swap when it is needed. These are some of the non-security related items that should be evaluated when considering different devices.

In summary, handheld computers need to meet the security and software compatibility requirements developed for desktop and laptop models, be lighter, more rugged, more weather sealed for outdoor use, have extended battery life, be more ergonomic for portable use and must provide considerable additional functionality, such as support for automatic identification technologies (AIT) like bar code and RFID. They must also support peripheral devices such as Common Access Card (CAC) readers.

The following sections describe some of the Gold Disk specifications for desktops and laptops, how this functionality can be accomplished on a handheld computer, and what features and functions to look for when the Gold Disk does not provide applicable guidance, and other handheld computer selection considerations.

Device & Communications Security
Separate DoD security requirements cover how data can be stored on devices and how it can be communicated over wireless network and are applicable for handheld computers. Several key DoD security requirements are outlined briefly below.
DoD Directive (DoDD) 8100.2 sets the requirements for any device to connect to a DoD wireless network. There are multiple standards and requirements within DoD 8100.2, including mobile device compliance with the IEEE 802.11i network security standard and the FIPS-140-2 standard for device authentication and data encryption. FIPS 140-2 and 802.11i can be implemented on handheld computers, so support for these protocols is an essential requirement for handheld computers for DoD use. DoD 8100.2 requires intrusion detection, which is set at the network (not device) level.

DoD 8100.2 requires that mobile devices have data-at-rest encryption capability. DAR can be accomplished through use of any of several COTS software packages and is also available within the Windows Mobile operating system.

- DoD 8100.2 also requires the use of firewalls plus antivirus software on individual devices in certain use cases. Handheld computers can support many kinds of firewalls and virtual private networks (VPNs). McAfee and Symantec are among the antivirus software providers that offer Windows Mobile versions of their products, so handheld computers with that operating system can have antivirus protection and be consistent with what is used on many desktops and laptops.

- DoD handheld computers need to be password protected and support the DoD Security Banner, which requires users to accept DoD security terms every time the computer attempts to connect to a military network. Network access is denied if security terms are not accepted.

There are numerous other specific security protocols and regulations to be met, and different models of mobile computers also offer many physical, software and communications features to further enhance security.

The biggest security differences between desktop/laptop computers and the handheld models are the environment where the devices will be used and the ability to scan the device for IA vulnerabilities. The DISA Gold Disk is oriented toward desktop and laptop computers used in traditional environments. It allows the operating system and its associated interfaces (ports, protocols and services) to be easily connected and scanned. While the host DoD system that the handheld supports can be easily scanned by automated IA security tools the handheld, as a standalone peripheral device, cannot. As a result, manual STIG reviews may have to be done by the IA validator. This validation is required by the Designated Approval Authority (DAA) as evidence to ensure the portable computing device configuration is compliant with DoD security requirements. The DISA STIGs and checklists are located at: [http://iase.disa.mil/index2.html](http://iase.disa.mil/index2.html)

**What Intermec Supports**

Intermec handheld computers can satisfy DoD 8100.2 requirements and support features for added security. Models are available with 802.11i and FIPS 140-2 wireless security, plus full support for the DoD Security Banner. Intermec handheld computers use Microsoft Windows operating systems and the integrated radios comply with 802.11 wireless standards, which enables implementation of many leading security protocols and enhancements. The Windows OS also enables the handelds to run many types of commercial off-the-shelf software, consistent with DoD policy. Intermec handhelds also support several COTS software packages that provide DAR encryption. The DoD Security Banner has been implemented within the software builds for the units Intermec provides specifically for government use.

The following chart summarizes how Intermec handheld computers can satisfy leading DoD security requirements.

---

### Figure 1: Intermec Support for DoD Security Requirements

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Security Sub-Category</th>
<th>AIT-IV Partner or Possible Supplier</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Data Security</td>
<td>CAC authentication / authorization</td>
<td>Intermec, Apriva</td>
<td>Intermec offers clip-on CAC readers for its handheld computers plus the BT200-T Bluetooth reader from Apriva. These allow users to insert their CAC and enter their PIN in order to gain access to the handheld and initiate a network login.</td>
</tr>
<tr>
<td></td>
<td>Biometric authentication</td>
<td>Intermec (Edgeline)</td>
<td>Clip-on adapter for fingerprint collection to enable three-factor identification.</td>
</tr>
<tr>
<td></td>
<td>Data at rest encryption</td>
<td>Mobile Armor, McAfee Endpoint Encryption, Windows Mobile 6.1</td>
<td>Provides full device data encryption, policy setting and controls.</td>
</tr>
<tr>
<td></td>
<td>Personal firewall</td>
<td>Symantec, McAfee</td>
<td>Restricts access to approved locations, applications, and/or networks.</td>
</tr>
<tr>
<td></td>
<td>Antivirus</td>
<td>Symantec, McAfee</td>
<td>Scans and cleans data on the mobile device, preventing corruption from viruses and other malicious code.</td>
</tr>
<tr>
<td>Device Management</td>
<td>Device lockdown</td>
<td>Intermec, Apriva, SDTI, AirWatch, Mobile Armor</td>
<td>Device can be locked down and access can be denied unless proper two- or three-factor authentication is given based on CAC reader usage. Access to device, specific ports, specific websites, etc. can be limited, controlled or denied completely. An approved list of device applications can also be created so that only those applications on the approved list will launch.</td>
</tr>
<tr>
<td></td>
<td>Device management</td>
<td>Intermec, SDTI, AirWatch, Good Technologies, Mobile Armor</td>
<td>Enables admins to remotely deploy, manage, troubleshoot, update and wipe memory on devices when necessary.</td>
</tr>
<tr>
<td>Wireless Data Security</td>
<td>End-to-end wireless data encryption (FIPS)</td>
<td>Juniper Odyssey Access Client (DAC)</td>
<td>802.11 frames are encrypted with FIPS 140-2 validated solutions and EAP-TLS with CAC certificate.</td>
</tr>
<tr>
<td></td>
<td>End-to-End Web</td>
<td>Apriva</td>
<td>Uses CAC for authorization to a Web server. With proper crypto-suites will use FIPS-140-2 validated encryption.</td>
</tr>
<tr>
<td></td>
<td>End-to-end VPN (FIPS)</td>
<td>Microsoft</td>
<td>With proper crypto-suites will use FIPS 140-2 validated encryption.</td>
</tr>
</tbody>
</table>
Some DoD environments allow the use of wireless for computer communication and some do not. In some cases use of wireless in an environment can be extremely dangerous. Intermec has recognized this and offers options for devices with no radio or wireless capabilities. These devices would operate strictly in a batch capacity and download data to the host computer when docked.

Intermec handheld computers have standard features and options that further improve security. The integrated SmartSystem Foundation device management capabilities enable administrators to disable computers remotely, lock down access to data and applications, and wipe data from device memory. These features neutralize the threat resulting from lost or stolen devices. The device management system can be set to automatically issue alerts if the computer has not been activated or logged on to an approved network for a specified period of time. These capabilities are also available for use by third-party software like AirWatch, Good Mobile Messaging, SOTI MobiControl and other device management packages that can be used to remotely manage, control, troubleshoot, and update these portable devices. Intermec has also successfully deployed many mobile computers with various third-party security solutions, including McAfee and Symantec antivirus software, the Mobile Armor data-at-rest encryption and authentication solution, and support for VPNs and personal firewalls.

Intermec implemented and manages a specific software load for units supplied on government contracts, including AIT-IV. This software load includes items to make implementation within a government network easier. Intermec has also designed a full set of snap-on adapters and accessories that allow the portable computers to perform as many functions as the customer needs, as easily as possible.

Intermec has implemented software and hardware within its builds that make two-factor authentication as simple as possible to implement. Authentication software from Apriva is implemented on the device along with either a Bluetooth Common Access Card (CAC) reader, or a custom designed snap-on CAC reader designed by Intermec. Three-factor authentication is also possible using clip-on or Bluetooth-connected biometric devices.

**Core Device Requirements**
Handheld computers can be used anywhere – including outdoors where they may be exposed to temperature extremes, immersion in water, shock, vibration and many other hazards. Battery life is critically important, because plug-in power supplies or backup units are not usually available. The usage environment dictates a device’s core functional requirements. Handheld computers generally need to be more rugged, more reliable, have more battery life and have more data collection and communication technology options than desktops, notebooks or laptops.

**Ruggedness**
A computer’s ruggedness is measured by its compliance with MIL standards (MIL-STD) and its Ingress Protection (IP) rating. MIL standards are set by the U.S. Department of Defense for equipment to be used by military agencies. There are numerous MIL standards for resistance to shock, vibration and other conditions. The 810 series sets standards for resistance to environmental stresses (including drops, impact, shock, vibration, temperature, humidity and life cycle) and is applicable for mobile computers. MIL-STD 810G was the latest and most rigorous standard in the 810 series when this white paper was published. IP ratings are expressed by the letters “IP” followed by two numbers. The first digit, which ranges from a 0 to 6, indicates the level the device is protected against particles, and the second digit, which ranges from 0 to 8, is the protection against water.

Separate certifications and safety ratings are needed for devices that may be used in potentially flammable or explosive environments. For these environments, handheld computers that are certified as “non incendive” or “intrinsically safe” should be selected. Non incendive designation generally means the device does not generate sparks and is incapable of igniting gases, vapors or liquids. Non-incendive devices are not necessarily sealed against gases, vapors or liquids. Intrinsically safe indicates a higher level of safety and protection. Devices designated as intrinsically safe will not spark or cause spark and can be used in areas where there are higher concentrations of combustible substances. Intrinsically safe standards apply to all equipment that can create one or more of a range of defined potential explosion sources, including sparks, flames, static electricity, electromagnet radiation, ionizing radiation and more. For more information about how non incendive and intrinsically safe designations relate to mobile computers, see Intermec’s white paper Make the Safe Choice: Understanding Requirements and for Hazardous Environments.

**Figure 2: Common Access Card Reader Options for Intermec Handheld Computers**
Intermec offers handheld computer models that meet extremely high vibration and durability specs and have earned IP 64, MIL-STG 810G and other certifications. Certified non-incendiary and intrinsically safe units are also available.

Data Collection
Mobile computing applications are designed to use automatic identification technologies to collect data instead of relying on keyboard-intensive data entry. The military supports multiple automatic identification technologies, as outlined below:

- **Bar codes** are commonly used to identify equipment, supplies, medical devices, fixed assets, other property and even locations. There are many bar code types, including two dimensional (2D) symbologies that not all scanners can read, so support for multiple bar code formats is important.

- **Unique ID (UID)** marks are a form of bar codes that are used to uniquely identify assets and are becoming common on practically all DoD assets. The UID program was created to enable DoD personnel to automatically identify, record and track assets. The actual UID symbol is generally a 2D bar code symbology. The bar code is either affixed to the item on a label, or printed directly on the item itself by direct part marking (DPM) using laser etching, dot peening or another technique.

- **Radio frequency identification (RFID)** is a wireless tracking technology widely used throughout the military to track pallets, cases and individual items. RFID tags are required on many contractor shipments to the DoD and are read to automate receiving, inventory management and shipping operations. RFID and UID data are commonly used to support program requirements.

- **Contact memory** devices (CMD, also called touch memory or touch buttons) use physical contact by a probe to transfer data stored within the button or tag to the computer. Memory buttons are typically used for asset management and facilities inspection applications.

- **The Common Access Card (CAC)** is typically used as an identification card within DoD to grant both physical access to restricted areas and virtual access to restricted networks. It stores data in a linear bar code, 2D bar code, magnetic stripe and a computer chip. The CAC is considered a smart card because of the embedded chip, so a smart card (not credit card or other magnetic stripe reader) reader is required to access all the data stored on the card. In many DoD operations, personnel are required to insert their CAC and enter their PIN when logging onto a government-owned network or device.

Readers for all of these technologies have been integrated directly into Intermec handheld computers. Integrating the functionality eliminates the need for peripheral devices, which improves reliability because there are fewer devices and cables that can break. Integrated functionality also helps users keep a hand free because they do not need to hold a separate peripheral device.

The bar code scan engines built into Intermec handheld computers can read all leading 1D and 2D bar code symbologies, including UID symbols and the PDF417 2D bar code used on CAC cards. Some scanners can read bar codes from near contact to up to 50 feet away, and provide superior performance for 2D bar code reading.

RFID reading is optional. Intermec handheld computers can be configured to read and encode ISO-18000/EPCglobal Gen 2 passive RFID tags used in item tracking and case and pallet management applications. There are also options available for reading data from active RFID tags.

Intermec provides options for reading CAC cards, including the chip component. One option is to clip a reader onto the CN3 or CK3 to provide an integrated unit. The other option is to use the card reader as a separate device that is controlled via a secured Bluetooth connection to the CN3/CK3.

The secure Bluetooth radio and integrated USB, Ethernet and RS-232 ports enable Intermec mobile computers to support many other peripheral devices, including printers, sensors, scales, industrial controllers, displays and headsets.

Communications
Handheld computing applications provide a link between the user and the records, databases and other information systems required to do the job. The link has to be available whenever needed, and must always be secure. This can be challenging, since the communications infrastructure available at bases to check asset records and inventory status can be different from what is available in the field. Handheld computers therefore must support multiple communications methods, while meeting all aforementioned security requirements.

Personnel should not have to install components or reconfigure their handheld computers on the fly to access the communications network that is available. Intermec mobile computers have separate built-in radios to simultaneously support wireless LAN (802.11 a/b/g and n on some devices) and wireless wide area networks (WWAN). A built-in Bluetooth radio is also available for secure short-range wireless communication with other devices, and GPS is optional.

Intermec offers different WWAN options to support most cellular networks and to comply with different wireless communication regulations in place around the world. Users can send and receive data, access hosted applications and websites and make voice calls over 3G EV-DO and EDGE networks. The devices are also compatible with 802.11-standard wireless LANs, including the high-throughput 802.11n standard, and have CCX support for integration with Cisco networks. As noted, Intermec handheld computers support FIPS, 802.11i and other wireless security protocols.

Hazard of Electromagnetic Radiation To Ordnance (HERO)
Intermec offers units that have been tested by the U.S. Navy’s Surface Warfare Center in Dahlgren, Virginia for potential electromagnetic radiation hazards. The purpose of the HERO safety evaluation was to determine if any radiated power from the Intermec devices was of sufficient magnitude to present a danger to ordnance. The spectrum of frequencies evaluated was:

- 802.11b/g WiFi (2.4 GHz)
- Personal Communication System (cellular - 1850–1990 MHz)
- Bluetooth (2.4 GHz)

The investigation was tailored to provide the recommended safe separation distance between ordnance and a mobile computer with bar code reader in any operating mode. Intermec offers...
several different models that have been HERO tested and have been approved for use in proximity to ordnance when used in accordance with the guidelines outlined in the reports generated by the Navy testing lab.

**Conclusion**

Handheld computers used for military operations have ruggedness, data input, remote support and communications needs that are specific to their usage environments. These requirements are fundamentally different from the standard functionality needed from desktop, laptop and notebook computers. While the Gold Master provides some valuable guidance about the basic OS, software and security standards for military computers, it is meant for desktop and laptop PCs and falls short of addressing the specific needs of handheld device users. This paper has highlighted these special requirements, identified the handheld computer features and capabilities that satisfy them, and explained how Intermec handheld computers meet the needs of military users.

Intermec offers multiple handheld computing devices in different form factors to fully meet the needs of the user community. These Windows Mobile devices are available commercially and units with government specific software loads and options are available through several different government procurement vehicles. Contact Intermec to obtain specific information regarding available devices and to obtain assistance in selecting the proper device for a specific application or user scenario.

Intermec has been a trusted mobile computing and automated data collection technology provider to the DoD, NATO and U.S. government for more than 30 years and has been active during every AIT contract. Intermec develops mobile computing and data collection products specifically for demanding environments. Thousands of our products have been deployed by various branches of the U.S. military to support operations worldwide. Visit the [Case Studies section](http://www.intermec.com) of [www.intermec.com](http://www.intermec.com) to see profiles of several our military customers and projects, including:

- Anniston Army Depot
- Arkansas National Guard
- U.S. Army Property Book Unit Supply Enhanced (PBUSE) system
- U.S. Coast Guard
- U.S. Commander Naval Air Forces Reserve
- U.S. Navy General Purpose Electrical/Electronic Test Equipment (GPETE) program
- U.S. Navy Norfolk Regional Supply Office
- U.S. Navy Philadelphia Inventory Management System (PHIMS)

Intermec Inc. (NYSE:IN) develops and integrates products, services and technologies that identify, track and manage supply chain assets and information. Core technologies include rugged mobile computing and data collection systems, bar code printers, label media, and RFID. The company’s products and services are used by customers in many industries worldwide to improve the productivity, quality and responsiveness of business operations. For more information about Intermec, visit [www.intermec.com](http://www.intermec.com) or call 800-347-2636.

**Disclaimer:** The information contained in this document is prepared and presented from public sources in good faith and for general information purposes only and is subject to changes in cited rules, regulations, and requirements at any time without notice. Neither Intermec nor the Government make any representations about the completeness, reliability and accuracy of the information provided.