The number of mobile computing devices used by federal employees is predicted to climb steeply. This trend is driven by the proliferation of personally owned mobile devices and by federal agencies’ overall desire for lower costs, improved service, and more flexibility.

But as mobility options expand, federal agencies must build security and manageability into digital government services so that confidentiality, integrity, and availability are preserved. Choosing the right mobile device is key to providing employees with the mobile performance they want and the security and manageability IT departments need.

Intel® architecture-based 2-in-1 devices and tablets offer distinct advantages to federal agencies compared to consumer-oriented mobile devices. A high level of security and manageability helps agencies maintain compliance. Enterprise-quality performance improves user experience and enables agencies to take full advantage of the estimated USD 2.6 billion worth of labor hours in federal productivity enabled by mobility.

While tablets are ideally suited for those highly mobile government workers who read documents, access the Web, and perform limited data entry, for most employees, these activities represent only 70 percent of their workload. For the other 30 percent, they need a laptop. As shown in Figure 1, Intel architecture-based 2-in-1 devices support both usage models: responsive, touch-enabled capability in the field, and full PC performance and productivity in the office—all in a single device.

Rushing toward Mobility

In 2011, the Federal Government began allowing employees to use mobile devices other than BlackBerry® devices. Publication of the Federal Digital Government Strategy in 2012 set the stage for the expansion of mobility. The Federal Mobility Strategy is currently in the outline stage.

Learn More at intel.com/federal
Federal agencies are taking notice:

- A December 2012 CIO Council study found that all but one of the agencies interviewed had either expanded or planned to expand mobility options for employees.
- A 2013 Gartner Inc. study indicated that mobility has moved from tenth to fifth place on government CIOs’ priority list.

The Federal Digital Government Strategy outlines an approach to mobility that stresses access to high-quality digital information and government services anywhere, anytime, on any device. It balances highly available access with stringent security and privacy requirements so that “innovation happens in a way that ensures the safe and secure delivery and use of digital services to protect information and privacy.”

The Strategy states that agencies should “procure and manage devices, applications, and data in smart, secure, and affordable ways.”

Standardizing on Intel architecture-based 2-in-1 devices and tablets—business-class devices that deliver the necessary security, remote manageability, and performance—provides agencies with an opportunity to meet the Digital Strategy objectives.

Choosing a Device that Meets Workers’ and IT’s Needs

The right mobile devices can improve agency productivity while protecting sensitive data in the field. Government agencies may benefit from standardizing on Intel architecture-based 2-in-1 devices and tablets running Microsoft Windows® 8 for the following reasons:

- Meet government mobile workers’ needs for increased portability and connectivity. Longer battery life means employees can stay in the field longer.
- Combine the advantages of the traditional mobile business PC with an improved mobile experience without compromising on the factors important to both employees and IT.
- Address employee demand for the user experience and innovations that are available on consumer devices while providing IT with the manageability and security features required for a cost-effective, compliant computing environment.
- Provide compatibility with millions of existing Windows-based applications and countless peripheral devices, enabling employees to use productivity programs they are already familiar with to perform job duties.

IMPROVING MANAGEABILITY AND SECURITY WITH INTEL® VPRO™ TECHNOLOGY

Federal agencies who invest in Intel® architecture-based 2-in-1 devices and tablets powered by the latest generation of Intel® Core™ vPro™ processors can realize the benefits of mobile manageability and security. These devices feature Intel® vPro™ technology, which is a combination of processor technologies, hardware enhancements, remote management features, and security technologies that allow remote access to mobile devices—including monitoring, maintenance, and management— independent of the device’s OS or power state.

Intel® vPro™ technology includes Intel® Active Management Technology (Intel® AMT), which provides support for efficient remote management, diagnosis, and repair of mobile devices:

- Provides full control of the power state of the entire managed fleet
- Reduces costly support visits and speeds diagnosis and repair times
- Enables remote, out-of-band management devices, even when the OS is non-functional
- Allows Service Desk technicians to remotely manage devices using a management console

These capabilities reduce IT costs and improve business continuity.
Federal Employees Want High Performance, Access to Existing Enterprise Applications, and Ease of Use

Employees want a device that delivers a positive user experience and productivity. They also want high performance, ease of use, and access to familiar enterprise applications. Intel architecture-based 2-in-1 devices and tablets deliver all these capabilities, and allow employees the flexibility to choose touch, stylus, typing on-screen, or a detachable keyboard. The longer battery life of both 2-in-1 devices and tablets lets employees stay in the field longer and be more productive.

Ultrabook™ devices combine PC performance, a sleek design, and tablet-like features such as instant-on and constant connectivity—offering enhanced flexibility, versatility, and responsiveness. When federal employees are traveling or meeting with clients, they can flip the touch screen and use it as a tablet. When they’re ready to write a report or respond to an email, they can easily transform the device into a laptop with a fully functioning keyboard.

Business-class tablets are available in a range of sizes. Powerful performance capabilities and compatible technology let users work quickly, multitask with ease, print wirelessly, and share information across devices.

Federal IT Departments Want Security and Remote Manageability

Federal agencies need security features that enable encryption, multifactor authentication, backup/restore of devices, remote lock and wipe of the devices, and automatic software updates. Therefore, for government IT departments, the built-in security features and remote manageability capabilities of 2-in-1 devices and tablets (see Figure 2 and Table 1) are of primary interest.

- **Device management.** The combination of Windows 8 and Intel architecture offers flexible device management with enhanced security features, such as domain joining and group policies, and remote management capabilities on Intel® Core™ vPro™ processor-based devices. These capabilities can help mitigate the risks of a consumerized enterprise environment and minimize the number of unmanaged devices on the network.

- **Authentication.** Intel architecture-based 2-in-1 devices and tablets running Windows 8 include Intel® Identity Protection Technology (Intel® IPT), which is a hardware-assisted layer of security that provides enhanced authentication and support for directory services integration. In addition, these devices support alternative authentication options such as a fingerprint reader or facial-recognition software.

**Figure 2. The security and manageability capabilities of Intel® architecture-based 2-in-1 devices and tablets can help mitigate the risks of a consumerized enterprise environment—and minimize the number of unmanaged devices on the network.**

MIGRATING DIRECTLY FROM MICROSOFT WINDOWS* XP TO WINDOWS 8

With Windows* XP support ending soon, staying with Windows XP is untenable. An unsupported OS can compromise information security, negatively affect performance and productivity, and hinder adoption of emerging usage models involving touch computing, context-aware computing, and other new capabilities. Therefore, federal agencies are faced with a decision: migrate straight to Windows 8, or make an interim migration to Windows 7.

A direct route is best. Migrating from Windows XP to Windows 8, combined with appropriate hardware upgrades and migration best practices, can reduce total cost of ownership, enhance productivity, and accelerate innovation in workflows and usage models. New OS features, combined with optimization for new Intel® architecture-based devices, enable Windows 8 users to work in ways not possible with Windows 7. For example, Windows 8 is optimized for touch interaction, and therefore can support the growing number of agencies’ touch-enabled and touch-optimized applications.

Windows 7 migration not operationally efficient or cost-effective. The second option, migrating to Windows 7, may seem reasonable initially, but closer inspection reveals hidden costs. Just like a growing family that moves to a small apartment, then nine months later needs a bigger house, agencies that migrate to Windows 7 would soon have to migrate to Windows 8 anyway. Moving twice will double the costs, time, and effort. Plus, agencies that take this route would miss out on the significant end-to-end performance, security, and user interface improvements available with Windows 8 on new hardware.
No computer system can provide absolute security under all conditions. Built-in security features available on select Intel processors may require additional software, hardware, services, and/or an Internet connection. Results may vary.

In addition to the above benefits, Intel architecture-based devices with Windows 8 are designed to work with an agency's existing IT infrastructure. For example, the technology is compatible with already-deployed x86 applications, peripherals, and device drivers. Also, they work directly with management consoles. Because the technology works directly with existing management and security solutions, there's no need to purchase additional software.

### Conclusion

Federal agencies are under pressure to give field employees improved tools, more efficient access to information, and a better way to record their work. But as information and devices become increasingly mobile, agencies must preserve confidentiality, integrity, and availability by building security into digital government services. And they are expected to do it with fewer resources.

Standardizing on Intel architecture-based 2-in-1 devices and tablets is one way that agencies can meet these seemingly conflicting goals. Agency IT departments will appreciate the security and remote manageability capabilities of Intel architecture-based 2-in-1 devices and tablets, as well as their compatibility with existing Windows-based applications and peripheral devices. Employees will value these devices' faster start-up and response times as well as lighter designs, high-performance connectivity, and longer battery life. In particular, for employees who sometimes need more than a tablet, the versatile Ultrabook 2 in 1 provides full PC performance and tablet mobility in a sleek, responsive form factor.

To learn more or request a pilot project in your federal agency, contact federal@intel.com

### Legacy applications

Intel architecture-based 2-in-1 devices and tablets support legacy applications and access to legacy data, unlike consumer-oriented mobile devices. Therefore, agencies can continue to benefit from previous hardware and software investments.

In addition to the above benefits, Intel architecture-based devices with Windows 8 are designed to work with an agency's existing IT infrastructure. For example, the technology is compatible with already-deployed x86 applications, peripherals, and device drivers. Also, they work directly with management consoles. Because the technology works directly with existing management and security solutions, there's no need to purchase additional software.

### Table 1. Security features and benefits for Intel® architecture-based 2-in-1 devices and tablets running Microsoft Windows® 8

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows® 8 and Intel® Atom™ processor</th>
<th>Windows® 8 and Intel® Core™ VPRO processor</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain join and group policy</td>
<td></td>
<td></td>
<td>Enhanced authentication and control</td>
</tr>
<tr>
<td>Intel® Active Management Technology®</td>
<td></td>
<td></td>
<td>Out-of-band management</td>
</tr>
<tr>
<td>Support for third-party browser add-ons</td>
<td></td>
<td></td>
<td>Enhanced security</td>
</tr>
<tr>
<td>Support for alternative authentication options</td>
<td></td>
<td></td>
<td>Improved user experience</td>
</tr>
<tr>
<td>Intel® Identity Protection Technology®</td>
<td></td>
<td></td>
<td>Hardware-assisted security featuring seamless user authentication and secure VPN access</td>
</tr>
<tr>
<td>• One-time password</td>
<td></td>
<td></td>
<td>Better user experience, no separate hardware or software required to generate tokens</td>
</tr>
<tr>
<td>• Public key infrastructure</td>
<td></td>
<td></td>
<td>Enhanced malware protection</td>
</tr>
<tr>
<td>Legacy application support</td>
<td></td>
<td></td>
<td>Ability to continue to benefit from previous investment</td>
</tr>
</tbody>
</table>

**Notes:**

10. Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup of your hardware, software, and IT environment. To learn more visit: [www.intel.com/technology/vpro](http://www.intel.com/technology/vpro).
11. Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results depend upon hardware and setup configuration. For more information, visit Intel® Active Management Technology.
12. Ultrabook products are offered in multiple models. Some models may not be available in your market. Consult your Ultrabook manufacturer. For more information and details, visit intel.com/ultrabook.
13. No computer system can provide absolute security under all conditions. Built-in security features available on select Intel processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information, visit security-center.intel.com.
14. No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen or higher Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://intel.com.

THE INFORMATION PROVIDED IN THIS PAPER IS INTENDED TO BE GENERAL IN NATURE AND IS NOT SPECIFIC GUIDANCE. RECOMMENDATIONS (INCLUDING POTENTIAL COST SAVINGS) ARE BASED UPON INTEL’S EXPERIENCE AND ARE ESTIMATES ONLY. INTEL DOES NOT GUARANTEE OR WARRANT OTHERS WILL OBTAIN SIMILAR RESULTS. INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.