DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MEMORANDUM FOR: SEE DISTRIBUTION

FEB 26 2016

SUBJECT: Implementation of Microsoft Windows 10 Secure Host Baseline

After consultation with Department leadership and through discussions with the DoD Chief Information Officer (DoD CIO), I am directing the Department to complete a rapid deployment and transition to Microsoft Windows 10 Secure Host Baseline (SHB). This decision is based on the need to strengthen our cyber security posture while concurrently streamlining the IT operating environment.

I am directing US Cyber Command (USCYBERCOM) through US Strategic Command (USSTRATCOM), to lead the implementation of this directive in consultation with the Chairman of the Joint Chiefs and the DoD CIO. I expect the full cooperation of all critical implementation components to include the Defense Information Systems Agency (DISA) and the National Security Agency (NSA).

DoD Components are responsible for planning, resourcing and executing the Microsoft Windows 10 SHB deployment consistent with this memorandum, including compliance with the attached Windows 10 SHB Implementation Task and Requirements Checklist.

This Windows 10 SHB deployment will be completed no later than January 31, 2017. The DoD CIO may update and refine my direction, as required, during the implementation of this directive.

Robert O. Work

Attachment:
As stated

DISTRIBUTION:

Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries Of Defense
Deputy Chief Management Officer
Chief of the Military Services
Chief of the National Guard Bureau
Commandant of the United States Coast Guard
Commanders of the Combatant Commands
General Counsel of the Department Of Defense
Director, Cost Assessment and Program Evaluation
Inspector General of the Department Of Defense
Director, Operational Test and Evaluation
Department of Defense Chief Information Officer
Assistant Secretary Of Defense for Legislative Affairs
Assistant to the Secretary Of Defense for Public Affairs
Director, Net Assessment
Directors of the Defense Agencies
Directors of the DoD Field Activities

ATTACHMENT

Implementation Task and Requirements Checklist
Microsoft Windows 10 Secure Host Baseline (SHB)

Rationale

1. Microsoft Windows 10 is intended as a cross-platform release and will be a ubiquitous operating system for desktops, laptops, and tablets.
2. Microsoft Windows 10 enterprise edition provides security features that are not available in older versions of Windows.
3. These new features, when employed, are critical to mitigating advanced network threats.
4. In the interest of Information Technology (IT) effectiveness and increased security, the Department of Defense is implementing the Microsoft Windows 10 operating system utilizing the secure host baseline (SHB) which provides a "build from" process for CC/S/As to develop releases for operational implementation.
5. Establishing and maintaining an enterprise level secure configuration, for both host systems, their network connections, and National Security Systems (NSS) is critical to achieving operational resilience to attack and exploitation.
6. Rapid implementation to Microsoft Windows 10 will improve our cybersecurity posture, lower the cost of IT, and streamline the IT operating environment.

Directive

1. Combatant Commands, Services, Agencies and Field Activities (CC/S/FAs), under the direction of the DoD Chief Information Officer (DoD CIO), will begin the rapid implementation of the Microsoft Windows 10 SHB system throughout their respective organizations for all DoD IT systems to include NSS currently utilizing Microsoft Desktop, Laptop, and Tablet operating systems, including virtualized instances, effective immediately.
2. Implementation of the Microsoft Windows 10 SHB is expected to be complete by 31 January 2017 for all applicable systems for which no waiver has been approved.
3. US Strategic Command (USSTRATCOM) through US Cyber Command (USCYBERCOM) will lead and manage the implementation of Microsoft Windows 10 across the enterprise with Defense Information Systems Agency (DISA) and the National Security Agency (NSA) leading the SHB development initiative.
4. USSTRATCOM through USCYBERCOM will provide waiver and reporting requirements via subsequent TaskOrds to CC/S/As.
5. This Windows 10 implementation applies to platform IT (PIT) and Weapons Systems to the greatest extent practicable given acceptable levels of risks and final approval by Lifecycle System Owners.
6. This Windows 10 implementation does not include Microsoft Server Operating Systems. Some server operating systems may require an appropriate upgrade to operate with computers running Windows 10. Additionally, this implementation does not apply to Windows phones and other cellular phone devices but would apply to tablet computers with cellular capabilities running a Windows operating system.

ATTACHMENT

Implementation Task and Requirements Checklist
Microsoft Windows 10 Secure Host Baseline (SHB)

RESPONSIBILITIES:

DoD CIO

1. In collaboration with the USCYBERCOM, DISA and Component strategic communications staffs, establish a strategic communications message for the execution of the Microsoft Windows 10 SHB implementation. The message will include talking points to address media inquiries about DoD's Microsoft Windows 10 SHB implementation.

USCYBERCOM

1. Lead and manage the implementation of Microsoft Windows 10 across the enterprise with DISA and the NSA leading the SHB development initiative.
2. In collaboration with the DoD CIO, DISA and Component strategic communications staffs, establish a strategic communications message for the execution of the Microsoft Windows 10 SHB implementation. The message will include talking points to address media inquiries about DoD's Microsoft Windows 10 SHB implementation.
3. Provide waiver request procedures and reporting requirements via subsequent TaskOrds to CC/S/As.

DISA

1. With NSA, co-lead a joint SHB working group (JSHBWG) to prepare the Microsoft Windows 10 SHB standard desktop configuration to comply with the DoD Security Technical Implementation Guides (STIGs) and include secure settings for other commercial software in wide use across DoD.
2. Publish technical artifacts required for the Microsoft Windows 10 SHB implementation as tasked in subsequent TaskOrds.
3. In collaboration with the DoD CIO, USCYBERCOM, and Component strategic communications staffs, establish a strategic communications message for the execution of the Microsoft Windows 10 SHB implementation. The message will include talking points to address media inquiries about DoD's Microsoft Windows 10 SHB implementation.

NSA

1. With DISA, co-lead a JSHBWG to prepare the Microsoft Windows 10 SHB standard desktop configuration to comply with the DoD STIGs and include secure settings for other commercial software in wide use across DoD.
2. In coordination with COCOMS, Services, and Agencies, develop technical specifications documents for the Microsoft Windows 10 SHB implementation.

DoD Components will:

1. Implement the Windows 10 SHB enterprise edition upon receipt of this order and complete implementation of the Windows 10 SHB by 31 January 2017. This implementation applies for all existing Windows clients on DoD information networks, on all unclassified, Secret fabric, and Top Secret Collateral DoD information systems, including DoD programs,

special access programs, mission systems, and strategic, tactical, and research, development, training, and evaluation systems. It also applies to all computing systems currently running Windows operating systems including PIT, and weapons systems to the maximum extent practicable.

2. Be responsible for planning, resourcing, and executing the Microsoft Windows 10 SHB implementation. Component Services/Executive Agents will ensure resourcing to fund all required hardware and software upgrades to accommodate the Windows 10 implementation and all administrative and operational Microsoft Windows 10 SHB implementation related travel and expenses internal to their organizations.
3. In collaboration with the DoD CIO, USCYBERCOM, and DISA, establish a strategic communications message for the execution of the Microsoft Windows 10 SHB implementation through their strategic communications staffs. The message will include talking points to address media inquiries about DoD's Microsoft Windows 10 SHB implementation.
4. Identify personnel supporting the Microsoft Windows 10 SHB implementation and ensure the appropriate administrative and logistical support actions are completed to enable participation in this endeavor as required.
5. Obtain DOD SHB releases, to include the Microsoft Windows 10 SHB content, from DISA's Information Assurance Support Environment portal site, at https://disa.deps.mil/ext/cop/iase/000-images/pages/index.aspx.
6. Execute training requirements associated with the Microsoft Windows 10 SHB implementation.
7. Ensure all component computer hardware meets minimum specifications for fully utilizing all Microsoft Windows 10 security features to be considered in compliance with this order.
8. Submit a **waiver request**, if unable to meet the target implementation date, with an attached Plan of Action and Milestones (POAM) to their respective CC/S/As CIO, who may approve **waiver request** for up to 12 months past the target implementation date. **Waiver requests** greater than 12 months will require DoD CIO approval.