

**DEPARTMENT OF DEFENSE**6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUN 01 2016

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Updated Direction for the Implementation of Microsoft Windows 10 Secure Host
BaselineReference: (a) Deputy Secretary of Defense Memorandum, "Implementation of Windows 10
Secure Host Baseline," February 26, 2016
(b) U.S. Cyber Command Task Order 16-0043, "Microsoft Windows 10 Secure Host
Baseline (SHB)"

Several DoD Components have come to the DoD Chief Information Officer (CIO) with questions and concerns regarding the implementation of Microsoft Windows 10 Secure Host Baseline (SHB), including issues related to legacy hardware, authorization of the SHB; and deviations from the Windows 10 Security Technical Implementation Guide (STIG). This memorandum addresses those concerns and provides direction on how to proceed with implementation of Windows 10 as directed by References (a) and (b).

The National Security Agency (NSA) completed a software and security assessment (see Attachment 1) to compare the operating system security features of Windows 7 and Windows 10 using legacy hardware not equipped with the latest Trusted Platform Module (TPM 2.0) and other hardware capabilities required to support security features, such as Credential Guard. NSA determined that Windows 10 provides a more secure posture than Windows 7 and other legacy versions of the Windows operating systems when installed on the same hardware, including computers that do not support all of the Windows 10 hardware-based security features, such as Credential Guard.

In order to improve cybersecurity posture, DoD Components are directed to migrate all desktops, laptops, or tablets capable of running Windows 10 from earlier versions of the Microsoft operating system, including virtualized instances, to Windows 10, even if the hardware does not support Credential Guard and other hardware-dependent security features. Credential Guard must be enabled on Windows 10 computers that support the feature. Windows 10 implementation will continue to be reported in the DoD Cybersecurity Scorecard. To bring DoD technical standards in line with the Windows 10 STIG, the Defense Information Systems Agency is directed to make modifications to the Windows 10 STIG, downgrading the Credential Guard Category I finding to Category III.

Several DoD Components requested an Enterprise Authority to Operate (ATO) for the Windows 10 SHB. After review by the Defense Security/Cybersecurity Authorization Working Group, this issue was raised for decision to the Information Security Risk Management Committee (ISRMC). The ISRMC decided that transitioning Microsoft desktop, laptop, or tablet operating systems, including virtualized instances, to the Windows 10 SHB from any earlier version of Windows represents a risk reduction (a positive security-relevant change), does not

invalidate current ATOs, and accordingly does not require re-authorization (or re-accreditation) of systems or enclaves (see Attachment 2). Accordingly, DoD Components are directed not to expend funds on additional security testing of Windows 10 SHB; this does not prohibit DoD Components from running regression testing on mission-specific applications to be run on Windows 10. For documentation related to the Windows 10 security assessment and STIG, visit the Information Assurance Support Environment website at iase.disa.mil.

The ISRMC decision also makes it clear that deployments deviating from the Windows 10 STIG require the organization's Authorizing Official to re-authorize the systems or enclaves. These deviations must be driven by mission requirements that cannot be met by a STIG-compliant implementation of Windows 10, and the justification for the deviation must be validated by the Military Service, Component, or Coast Guard CIO, and reported to the DoD CIO via the validating CIO.

My point of contact for this matter is Mr. Mitchell Komaroff at mitchell.komaroff.civ@mail.mil, (703) 697-3314.



Richard A. Hale
DoD Senior Information Security Officer

Attachments:
As stated

DISTRIBUTION:

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF NATIONAL GUARD BUREAU
COMMANDANT OF THE UNITED STATES COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
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
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