Use of Windows 7 Legacy Operating System and Adobe Flash after December 31, 2020

References:

(a) DCSA Assessment and Authorization Process Manual (DAAPM) Version 2.2, August 31, 2020;

(b) DoD 5220.22-M, National Industrial Security Program Operating Manual, February 2006, as amended.

The purpose of this information is to provide guidance for the upgrading of DCSA authorized Information Systems containing Microsoft Corporation operating systems that reached EOL in 2019. Microsoft has ceased to provide security support for their Windows 7 and Server 2008 operating systems after that date, unless Extended Security Updates (ESU) have been purchased to extend security patches. NISP contractors were permitted to leverage the Microsoft ESU for up to one year, but not beyond December 31, 2020. As of January 1, 2021, NISP authorized systems still using Windows 7 or Server 2008 will no longer be eligible for the ESU program and are required to do the following:

- Update the system security plan to reflect accurate Plan of Action and Milestones (POA&M) describing the contractor ongoing effort to update authorized information system operating systems to Windows 10.

- To allow continued use of Windows 7 beyond the December 31, 2020 deadline, DCSA would require official communication from the government customer acknowledging the continued use of legacy solutions as necessary. This acknowledgement can be in the form of a memo on government customer letterhead or by contract language stating the requirement for work to continue with Windows 7 systems while the contractor moves forward with migration activities.

- Follow DAAPM Section 6 and Section 7 and complete the CAC-1 requirements to submit the system package.

- Follow configuration management plan, coordinate planned upgrade (POA&M) with your DCSA ISSP

- Update appropriate eMASS system description and artifacts (i.e. software & hardware baseline, network diagram, etc.) to reflect status

- Provide ISSM Certification Statement in eMASS as artifact that the upgrade conforms to the existing authorization security controls.

- Update eMASS systems description and artifacts (i.e. software & hardware baseline, network diagram, etc.) and appropriate controls (e.g. CM-2, CM-3, CM-4) reflecting planned upgrade within eMASS

- ATD will remain the same and industry must plan to re-authorize the system prior to expiration as appropriate

Additionally:

Microsoft has released update KB4577586 to Windows 10 that removes Adobe Flash Player due to vendor end-of-support of the Flash application on December 31, 2020. This update applies to all versions of Windows 10 and Windows Server, as well as Windows 8.1. The update is being provided now to give customers time to find alternative solutions for business critical applications and information systems.

The removal of Adobe flash will be automatic upon installation of the Windows Update, and the application cannot be directly re-installed. Adobe Flash will still be installable on updated Windows systems as a third-party plugin, however the vendor (Adobe) will no longer provide security updates or manufacturer support.

As such after December 31, 2020 NISP authorized systems leveraging Adobe Flash on Windows systems will be categorized as operating "legacy" software/applications. This mandates removal of the application or the creation of a Plan of Action & Milestones (POA&M) for any current NISP-authorized information systems utilizing Adobe Flash and must be addressed in submission of any System Security Plans moving forward. Please reach out to your assigned ISSP for additional information and guidance regarding this security-relevant update.

The point of contact for this information is your locally assigned DCSA ISSP.