DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
INDUSTRIAL SECURITY FIELD OPERATIONS
NISP AUTHORIZATION OFFICE
27130 TELEGRAPH ROAD
QUANTICO, VA 22314

MEMORANDUM FOR NISP Contractors with DCSA Authorized Information Systems (IS)

DATE: 11 September 2020

SUBJECT: Upgrading IS using Microsoft Operating Systems that reached End of Life (EOL) in January 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 memorandum is to provide guidance for the upgrading of DCSA authorized IS containing Microsoft Corporation operating systems that reached EOL on January 20, 2020. Microsoft will cease to provide security support for their Windows 7 and Server 2008 operating systems after that date.

The following will apply to all upgrades stemming from the EOL:

- Microsoft Windows 7 only upgraded to Microsoft Windows 10
- Microsoft Server 2008 only upgraded to Microsoft Server 2012/2016/2019
- System hardware upgrades only to allow full functionality of new operating system
- Only the above listed upgrades will not require a new DCSA authorization

NISP contractors will process upgrades of these IS with documentation in eMASS using the following procedures.

Information Systems registered in eMASS with current ATOs – system(s) has little/no evidence of security controls in eMASS as a result of the OBMS to eMASS transition.

- 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 change
- Provide ISSM Certification Statement in eMASS as artifact that the upgrade conforms to the existing authorization security controls
- DCSA will validate new operating system configuration settings at the next regularly scheduled system assessment
- ATD will remain the same and industry must plan to re-authorize the system prior to expiration through eMASS as appropriate

Information Systems authorized in eMASS with current ATOs,

- Follow configuration management plan, coordinate planned upgrade (POA&M) with your DCSA ISSP
- 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
- Provide ISSM Certification Statement in eMASS as artifact that the upgrade conforms to the existing authorization security controls
- DCSA will validate new operating system configuration settings at the next regularly scheduled system assessment
- ATD will remain the same and industry must plan to re-authorize the system prior to expiration as appropriate

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

Karl Hellmann

Karl Hellmann
Assistant Deputy Director
NISP Authorization Office
DCSA