DEPARTMENT OF THE AIR FORCE

WASHINGTON DC

OFFICE OF THE SECRETARY

AFGM2015-33-01

21 April 2015

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Guidance Memorandum (AFGM), End-of-Support Software Risk Management

ACCESSIBILITY: Publication is available for downloading on the e-Publishing web site at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

By Order of the Secretary of the Air Force, this Guidance Memorandum supersedes AFGM 2014-33-03, *Microsoft Windows XP End-of-Life*, and highlights current policies and SAF/CIO A6 authorities to mitigate cybersecurity vulnerabilities introduced by unsupported software. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails in accordance with Air Force Instruction (AFI) 33-360, *Publications and Forms Management*.

Unless otherwise noted, the SAF/CIO A6 is the waiver authority to policies contained in this AFGM. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of according to Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

Cybersecurity infused throughout a system's life cycle bolsters mission assurance for Air Force core missions. Air Force Pamphlet (AFPAM) 63-128, *Integrated Life Cycle Management*, highlights the need to plan and program for Information Technology (IT) sustainment as well as the need to conduct cybersecurity (formerly defined as information assurance) activities throughout the life cycle of a program. Inconsistent planning and programming for software, hardware, and firmware could introduce vulnerabilities and preventable risks. For example, Microsoft Windows XP extended support ended 8 April 2014, Microsoft Server 2003 extended

support ends 14 July 2015, and Microsoft Windows 7 extended support ends 14 January 2020. Microsoft will no longer provide security updates following end of extended support. DISA categorizes unsupported operating systems as a "Category I" severity vulnerability for which the exploitation will directly and immediately result in loss of confidence, availability, or integrity. Additionally, DISA Command Cyber Readiness Inspections (CCRIs) evaluate functional and program managed systems for which high risk vulnerabilities could result in disconnection from the DoD Information Network (DoDIN).

To address this problem in the near term, systems must transition away from software before it is no longer supported or develop a Plan of Action and Milestones (POA&M) that addresses vulnerability mitigation and software migration strategies (T-1). POA&Ms addressing these non-compliant security controls must be documented IAW AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP).* Additionally, systems which are unable to transition away from unsupported software must utilize a vendor Custom Support Agreement (CSA), if available, that continues to provide software security updates past end of support. AFMAN 33-153, *IT Asset Management*, provides guidance on purchasing software and enterprise licensing. Organizations may direct any questions or recommend software products for potential enterprise CSAs by contacting the Air Force Lifecycle Management Center's (AFLCMC) Software Enterprise Acquisition Management & Lifecycle Support (SEAMLS) Team at aflcmc.hica-seamls@us.af.mil. Requests to participate in an Air Force enterprise CSA for Microsoft Windows XP and/or Microsoft Server 2003 must be submitted by 31 May 2015.

To address this problem in the long term, the SAF/CIO A6 will leverage his authorities to foster cybersecurity throughout a system's life cycle. First, the SAF/CIO A6 will execute oversight through IT Portfolio Management and Capital Planning and Investment Controls IAW AFI 33-141, *Air Force IT Portfolio Management and IT Investment Review*. Second, the SAF/CIO A6 will approve the Acquisition Cybersecurity Strategy, Clinger Cohen Act Compliance, and Information Support Plan IAW AFI 63-101/20-101, *Integrated Life Cycle Management*. The SAF/CIO A6 will evaluate software sustainment and life cycle where applicable as a condition of approval for these documents which are required for milestone decision review. And third, the SAF/CIO A6 will review systems for ATO approval consideration if they have "high" or "very high" risk non-compliant controls that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality IAW DoDI 8510.01, *Risk Management Framework for DoD Information Technology*.

Questions regarding this policy can be forwarded to the SAF/CIO A6 Cybersecurity Division, usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil. This memorandum becomes void after one-year has elapsed from the date signed, or upon publication of this guidance in an AF instruction, whichever is earlier.

WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Office