

FAQ:

Q) In light of the recent end of life for Windows XP, can DSS provide their position on continued use of Windows XP now that it is no longer supported by the vendor, making it a legacy operating system?

A) DSS in addressing this question regarding the use of Windows XP will publish the following guidance in the next revision of the ODAA Process Manual. The guidance addresses the use of all legacy O/S, which includes those which are accredited, but later become non-compliant due to lack of vendor support.

Legacy (non-compliant) Operating Systems

Legacy O/S are those systems that are no longer receiving support from the vendor. ODAA may approve legacy O/S when required for operational necessity and program requirements. Use of the legacy O/S will be included in contractual requirements or the government customer must provide a letter (signed by the Contracting Officer, the Contracting Officer's Representative, the Contracting Officer's Technical Representative, or the Government Program Manager) stating there is a program requirement to use the legacy O/S and the GCA acknowledges the risk associated with its use.

When information systems are accredited by DSS and subsequently the O/S loses vendor support, continued operation IAW the SSP is authorized; however, a Plan of Action and Milestones (POA&M) entry will be made to address the transition to an operating system with continued vendor support at the time of reaccreditation. In those cases where a legacy O/S cannot be upgraded due to operational necessity or incompatibilities with program requirements, or the manufacturing process, the ISSM must submit a risk acknowledgement letter from the GCA, as described above.

A mature program or old manufacturing process should not require approval of additional legacy systems. Any growth in the program should be accomplished by use of compliant operating systems.

Self-certification will not be granted for new information systems requiring the use of legacy O/S; however, the ISSM may replace workstations (as necessary) on currently accredited information systems which operate with the legacy O/S to maintain the effectiveness of the program. If an MSSP contains multiple O/S, that MSSP may still be used for self-certification of new IS using only those O/S which have continued support by the vendor.

When necessary for reaccreditation of a system requiring continued use of a legacy O/S, the signed customer letter must be provided along with the system documentation when requesting an accreditation decision. The customer letter must identify the following information:

- § System UID
- § Operating System
- § Operating environment
- § NISPOM requirement(s) that cannot be met and how the requirement is mitigated
- § Acknowledgement of the associated risk with the legacy O/S

Once approved, the signed customer letter must be retained as an attachment in the IS profile as security relevant documentation for the specific system. Continued use of the legacy O/S must be revisited during each subsequent reaccreditation.

Q) Is the contractor required to establish a POAM for their current systems or as a part of their reaccreditation package? Also, will a POAM be required if the systems are contractually required?

A) If an O/S becomes unsupported, a POAM is required for the current system to identify the vulnerability and plan for reaccreditation with an approved O/S. Reaccredited systems will not have legacy O/S, so no associated POA&M entry is necessary unless the legacy O/S is operationally required. If the legacy O/S is still operationally required at the time of reaccreditation, a POA&M will be required addressing the vulnerability, along with a letter from the customer addressing the operational necessity and acknowledging the risk associated with its continued use.

Q) Are UNIX O/S included in this guidance? Since there is no real vendor, how do we determine when it is no longer supported? Are we going to have a list of "legacy" operating systems to share with industry?

A) Yes, known versions of Unix based O/S which are unsupported by the vendor are included in the guidance for legacy O/S. It is up to the ISSM to determine and identify these O/S to ODAA when they become unsupported. Each instance will be considered on a case by case basis and no "list" will be maintained by DSS.