



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Apple OS X 10.9 (Mavericks) Workstation Security Technical Implementation Guide (STIG) Version 1

Reference: DoD Instruction 8500.01

DoD Instruction 8500.01 tasks DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders” and DoD Component heads “ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs.”

DISA considered all the applicable technical NIST SP 800-53 requirements while developing this STIG. Requirements which are applicable and configurable are included in the final STIG. DoD information systems require password complexity and account management for authentication and confidentiality. Apple OS X 10.9 natively does not provide these capabilities. In order for systems to meet these requirements, they must be connected to an Active Directory infrastructure or similar LDAP solution. A report marked For Official Use Only (FOUO) is available for further items that did not meet requirements. The compliance report is available to component Authorizing Official (AO) personnel for use in their certification and risk assessment. AO requests for the compliance report may be sent via email to disa.stig_spt@mail.mil.

In accordance with DoD Instruction 8500.01, the Apple OS X 10.9 (Mavericks) Workstation STIG Version 1 is released for immediate use. The document is available on <http://iase.disa.mil>.

Point of contact for this action is STIG Support Desk, email: disa.stig_spt@mail.mil.

JOHN J. HICKEY, JR.
Risk Management Executive

UNCLASSIFIED