DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

FEB 26 2016

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Trend Micro Deep Security 9.x 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 that are applicable and configurable are included in the final STIG. A report marked For Official Use Only (FOUO) is available for those 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 of Trend Micro Deep Security 9.x. 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 Trend Micro Deep Security 9.x STIG Version 1 is released for immediate use. The document is available on http://iase.disa.mil.

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

JOHN J. HICKEY, JR.
Risk Management Executive