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

MEMORANDUM FOR DISTRIBUTION

30 March 2015

SUBJECT: Microsoft Windows 2012 Server Domain Name System (DNS) 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."

This STIG considered all the applicable technical NIST SP 800-53 Rev 4 requirements as defined in the DNS Security Requirements Guide (SRG) Version 2. It provides the technical security policies and requirements for applying security concepts to domain name system implementations. This STIG will be used for all Windows 2012 / 2012 R2 DNS servers, whether Active Directory-integrated, authoritative file-backed DNS zones, a hybrid of both, or as a recursive caching server. This STIG should also be used for Windows 2012 DNS servers being used as a secondary name server for zones whose master authoritative server is non-Windows.

In accordance with DoD Instruction 8500.01, the Microsoft Windows 2012 Server DNS 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

HICKEY.JOHN.JOSEPH.JR.1058753994

Digitally signed by HICKEY.JOHN.JOSEPH.JR.1058753994
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=HICKEY.JOHN.JOSEPH.JR.1058753994
Date: 2015.03.30 08:13:45 -04'00'

JOHN J. HICKEY, JR.
Risk Management Executive