



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER TO: Field Security Operations (FS)

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Announcement of the DISA Field Security Operations (FSO) Draft Windows 2012 Domain Name Service (DNS) Security Technical Implementation Guide (STIG) Version 1

DISA Field Security Operations (FSO) has developed the draft Windows 2012 Domain Name Service (DNS) STIG Version 1. The STIG is available on the NIPRNet at http://iase.disa.mil/stigs/net_perimeter/other/other.html for review and comment.

This draft 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 draft 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 draft 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.

Please provide comments, recommended changes, and/or additions to the draft STIG by 18 December 2014 on the Comment Matrix spreadsheet. The spreadsheet is available at: http://iase.disa.mil/stigs/net_perimeter/other/other.html. Comments should be sent via NIPRNet email to: disa.letterkenny.FSO.mbx.stig-info@mail.mil. Include the title and version of the STIG in the subject line of your email.

ROGER S. GREENWELL
Director, Field Security
Operations

UNCLASSIFIED