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

IN REPLY REFER TO: Chief Information Assurance Executive (CIAE)

16 October 2012

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Intrusion Detection and Prevention Systems (IDPS) Security Requirements Guide (SRG) Version 1

Reference: DoD Directive 8500.1

1. In preparation for the conversion from DoD 8500 Information Assurance (IA) controls to the NIST Special Publication (SP) 800-53 entitled, "Recommended Security Controls for Federal Information Systems and Organizations", DISA Field Security Operations (FSO) has accomplished the following:

a. DISA FSO decomposed the NIST 800-53 IA controls into single, actionable, measureable requirements called Control Correlation Identifiers (CCIs), in an effort to move towards future automation for compliance reporting.

b. FSO then reviewed the CCIs and categorized the controls into two basic groups: technical CCIs versus non-technical CCIs. A CCI was deemed technical if it was measurable at the asset level (Operating System, Application, or Network). A CCI was deemed nontechnical if it was a policy-based requirement or had an architectural nature to it.

c. Using the technical CCI lists as the source, FSO developed the Network SRG. This IDPS SRG adds technology family specific tailoring to the generic CCIs.

2. The IDPS SRG contains all requirements flagged as applicable from the Network SRG and will be the basis for future product specific Security Technical Implementation Guides (STIGs).

3. DISA hereby releases the IDPS SRG, Version 1, for immediate use as a DoD-approved security requirements guideline. This document is available on http://iase.disa.mil.

4. Point of contact for this action is FSO STIG Customer Support, email: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

ORNDORFF.MARK.STEPHEN.1045813610
Digitally signed by ORNDORFF.MARK.STEPHEN.1045813610
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=ORNDORFF.MARK.STEPHEN.1045813610
Date: 2012.10.16 13:00:53 -04'00'

MARK S. ORNDORFF
Chief Information Assurance Executive

UNCLASSIFIED