INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) SRG
REVISION HISTORY

Version 2, Release 6

24 July 2020

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R6	IDPS SRG, V2R5	- V-55595 - Removed requirement. The product failing secure is not a configurable item, but is a capability of the product. V-55341 - Changed SCAs to System Administrators.	24 July 2020
V2R5	IDPS SRG, V2R4	- V-55331, V-55363, V-55379, V-55387, V-55389, V-55391, V-55393 - Changed SCA to individual designated ty the SCA (SA recommended). - V-55385 - Removed reference to SCA and replaced with SA at a minimum. - V- 55597 - Changed SCA to system administrator in VulDiscussion.	25 October 2019
V2R5	IDPS SRG, V2R4 Overview	- Updated STIG Distribution section	25 October 2019
V2R4	IDPS SRG, V2R3 Overview	- Updated section 2.2 to add guidance for IDS (monitoring) versus IPS (blocking) requirements. - Updated Section 3.2 to clarify IDS verses IPS functions in the IDPS solution/implementation.	26 October 2018
V2R3	IDPS SRG, V2R2	- V-55347 - Changed pattern recognition pre-processors to anomaly detection so less vendor-specific terminology is used in the SRG.	28 July 2017
V2R2	IDPS SRG, V2R1	- Corrected spelling of IDPS in vulnerability discussion of SRG-NET-000113-IDPS-00189. - Corrected spelling of IDPS in Rule Title of SRG-NET-000392-IDPS-000218. - Fixed line spacing in Rule Title of SRGNET-000392-IDPS-00219. - Changed ISSM/ISSO to ISSM or ISSO for SRG-NET-000384-IDPS-000209 to clarify. - Changed ALG to IDPS in Vulnerability Discussion: SRG-NET-000392-IDPS-000217 SRG-NET-000392-IDPS-000218 SRG-NET-000392-IDPS-000219 - Added "The ISSM or ISSO may designate the SCA or other authorized personnel to receive the alert within the specified time, validate the alert, and then forward only validated alerts to the ISSO" to the vulnerability discussion in: SRG-NET-000335-IDPS-000014 SRG-NET-000385-IDPS-000211	24 July 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		SRG-NET-000392-IDPS-000214 SRG-NET-000392-IDPS-000215 SRG-NET-000392-IDPS-000216 SRG-NET-000392-IDPS-000217 SRG-NET-000392-IDPS-000218 - In SRG-NET-000335-IDPS-000014: Changed "real-time" to "less than a second", which was previously defined in the vulnerability discussion. Added "The IDPS must either send the alert to a management console that is actively monitored by authorized personnel or use a messaging capability to send the alert directly to designated personnel." - Deleted paragraph 2 of SRG-NET-000235-IDPS-000169 to clarify applicability. Replaced with "This requirement applies to the device itself, not the network traffic." - Reworded second paragraph of SRG-NET-000265-IDPS-000199 to include stronger justification for this 800-53 required control by adding the following statement: "If the IDPS traffic monitoring and detection functions fail for any reason, the IDPS must stop forwarding traffic altogether or maintain the configured security policies. For this reason, device redundancy rather than a policy of failing open is vital to maintaining network availability while protecting DoD networks."	
V2R1	- N/A	- Initial Release.	14 November 2014