# INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)
# SRG REVISION HISTORY

## Version 2, Release 3

## 28 July 2017

## Developed by DISA for the DoD

| REVISION HISTORY | | | |
|---|---|---|---|
| **Revision Number** | **Document Revised** | **Description of Change** | **Release Date** |
| 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 |
| V1R2 | IDPS SRG V1R1 | - Corrected spelling of IDPS in vulnerability discussion of SRG-NET-000113-IDPS-00189.<br>- Corrected spelling of IDPS in Rule Title of SRG-NET-000392-IDPS-000218.<br>- Fixed line spacing in Rule Title of SRGNET-000392-IDPS-00219.<br>- Changed ISSM/ISSO to ISSM or ISSO for SRG-NET-000384-IDPS-000209 to clarify.<br>- Changed ALG to IDPS in Vulnerability Discussion:<br>  SRG-NET-000392-IDPS-000217<br>  SRG-NET-000392-IDPS-000218<br>  SRG-NET-000392-IDPS-000219<br>- 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:<br>  SRG-NET-000335-IDPS-000014<br>  SRG-NET-000385-IDPS-000211<br>  SRG-NET-000392-IDPS-000214<br>  SRG-NET-000392-IDPS-000215<br>  SRG-NET-000392-IDPS-000216<br>  SRG-NET-000392-IDPS-000217<br>  SRG-NET-000392-IDPS-000218<br>- In SRG-NET-000335-IDPS-000014: Changed "real-time" to "less than a second", which was previously defined in the vulnerability discussion.<br>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." | 24 July 2015 |

| REVISION HISTORY | | | |
|---|---|---|---|
| **Revision Number** | **Document Revised** | **Description of Change** | **Release Date** |
| | | - 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." | |
| V1R1 | IDPS SRG V1R1 | - Initial Release | 14 November 2014 |