COMPLIANCE COMPONENT

DEFINITION	
Name	Intrusion Prevention Systems (IPS)
Description	Intrusion Prevention Systems collect and analyze information from within network traffic for the purpose of preventing, detecting and mitigating malicious activity.
Rationale	IPS has become a necessary addition to the security infrastructure. IPS is deployed as part of a multi-tiered approach to security to protect the system from internet based threats.
Benefits	• Identifies malicious internet based threats and prevent attacks. • Identifies patterns that may lead to attacks • Identifies deviations of protocol states by comparing observed events with predetermined profiles • An IPS can correct cyclic redundancy (CRC) errors, defrag packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Intrusion Prevention Systems
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**General IPS Requirements** • Administrators shall be trained on the IPS before implementation. • IPS shall be controlled directly from a central location(s). **IPS Deployment Requirements** • IPS shall be installed on any internet egress points where sensitive or critical information is transmitted. **IPS Analysis Requirements** • IPS must submit logs to the Security Information and Event Management (SIEM) system. • IPS must:

	o Drop malicious packets o Reset malicious connections o Block traffic from malicious source address o Use heuristic methods and Anomaly Detection o support customized signatures • Administrators shall follow a schedule for checking the results of the IPS to ensure attackers have not modified the system. **IPS Response Requirements** • IPS must respond in real-time. • IPS must provide active responses to intrusions by: o Collecting additional information; o Turning up the number of events logged, or o Capturing all packets, not just those targeting a particular port or system o Changing the environment by: • Terminating the connection • Blocking packets from the intruder's IP address • Blocking network ports, protocols or services • Resetting all connections that use certain network interfaces • IPS should provide passive responses requiring subsequent human action to intrusions by: o Generating alarms and notifications or o Reporting alarms and alerts using SNMP traps and plug-in central network management consoles. • All IPS communications shall be secure and use encrypted tunnels or other cryptographic measures. • IPS shall create output with the following information for each intrusion detected: o Time/date o Sensor IP address o Specific attack name or anomaly o Source and destination IP addresses o Source and destination port numbers o Network protocol used o Description of the attack type o Attack severity level • IPS reports should combine redundant attack entries and make attacks of highest importance stand out.
Document Source Reference #	NIST SP 800-94 (www.csrc.nist.gov/publications/nistpubs) Guide to Intrusion Detection and Prevention Systems (IDPS)

Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	buffer overflows, sniffing, exploit, probes, heuristics, anomaly, malicious, suspicious, IDS, NIDS

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION		
Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	

Migration Strategy	
Document the Migration Strategy	

Impact Position Statement	
Document the Position Statement on Impact	

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	04/03/2003	*Date Approved / Rejected*	5/14/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	11/15/2016
Reason for Update	Vitality		