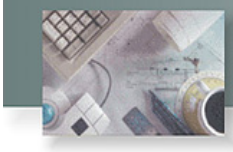

Compliance Component

DEFINITION	
Name	Network-Based Intrusion Detection Systems (NIDS)
Description	Network-Based Intrusion Detection Systems (NIDS) detect attacks by capturing and analyzing network traffic. NIDS are dedicated software or hardware systems that "sit" on a network and analyze network packets. NIDS often consist of a set of single-purpose sensors placed at various points in a network. These sensors monitor network traffic, performing local analysis of that traffic and reporting attacks to a centralized console.
Rationale	The first step in delivering an efficient and secure network intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods should be employed to ensure comprehensive coverage. The failure to secure State of Missouri networks with NIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State of Missouri services can also include inconvenience to citizens and the loss of public confidence.
Benefits	• NIDS identify and prevent security threats from compromising secure networks. • The deployment of NIDS has little impact on network performance. NIDS are usually passive devices that listen on a network without interfering with the normal operation of a network. • NIDS can be made very secure against attack and even made invisible to many attackers.

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

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**General NIDS Requirements** • Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are

	necessary to manage any IDS.
	• It is preferred to have the NIDS controlled directly from a central location(s). However, the NIDS may be agent-based where response decisions are made at the agent.
	• IDS administrators shall be able to create or change policies easily.
	
	NIDS Deployment Requirements
	• NIDS shall be deployed in conjunction with Host-Based IDS to fully protect the system.
	• It is recommended that organizations install the NIDS first on critical networks. Once administrators are familiar with the NIDS, it may be installed on the remainder of the organization's networks.
	• NIDS shall be installed on any Network where sensitive or critical information is transmitted.
	• It is preferred to install IDS Management software on a dedicated system in the target networks being monitored.
	• It is preferred to have the NIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
	• It is preferred that Server agents poll the manager at periodic intervals for policy changes or new software updates.
	
	NIDS Analysis Requirements
	• NIDS shall utilize information from operating system audit trails and system logs.
	• NIDS shall have easy-to-use tools to analyze the logs.
	• NIDS shall detect, and preferably prevent, the following:
	  • System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active systems, operating systems and software in use),
	  • Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
	  • Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
	• NIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may include Anomaly Detection (abnormal, unusual behavior) components.
	• Administrators shall follow a schedule for checking the results of the NIDS to ensure attackers have not modified the system.
	
	NIDS Response Requirements
	• NIDS shall respond in real-time.
	• It is preferred that IDS provide active responses to intrusions by:
	  • Collecting additional information:

	• Turning up the number of events logged, or • Capturing all packets, not just those targeting a particular port or system. • Changing the environment: • Terminating the connection, or • Reconfiguring routers and firewalls to: • Block packets from the intruder's IP address, • Block network ports, protocols or services, or • Sever all connections that use certain network interfaces. • NIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users. • NIDS may provide passive responses requiring subsequent human action to intrusions by: • Generating alarms and notifications with popup windows, cellular phones, pagers and email, or • Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles. • All NIDS communications shall be secure and use encrypted tunnels or other cryptographic measures. • NIDS shall create output with the following information for each intrusion detected: • Time/date • Sensor IP address • Specific attack name • Source and destination IP addresses • Source and destination port numbers • Network protocol used • Description of the attack type • Attack severity level • Type of loss expected • Type of vulnerability exploited • Input validation (buffer overflow or boundary condition) • Access validation (faulty access control mechanism) • Exceptional condition • Environmental (unexpected interaction with an application and the operating system or between two applications) • Server Configuration • Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation)

	• Design • Software types and versions vulnerable • Patch information to counter the attack • References to advisories about the attack or vulnerability • It is preferred that NIDS reports combine redundant attack entries and make attacks of highest importance stand out.
Document Source Reference #	NIST SP 800-31 (www.csrc.nist.gov/publications/nistpubs) Intrusion Detection Systems (IDS), NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)

Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
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 Accepted / Rejected*	5/14/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			