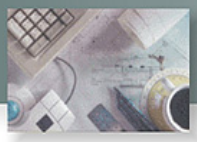

Technology Area

DEFINITION	
Name	Intrusion Detection Systems (IDS)
Description	Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusion Detection Systems (IDS) are software or hardware products that automate this monitoring and analysis process.
Rationale	Intrusion detection allows State of Missouri organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be *whether* to use IDS, but which IDS features and capabilities to use.
Benefits	• IDS prevents problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse a system. • IDS detects attacks and other security violations that are not prevented by other security measures. • An IDS can act as a quality control for security design and administration. • IDS provides useful information about intrusions that do take place, allowing improved diagnosis, recovery, correction of causative factors, and data for potential prosecution.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
Associated Compliance Components	
List the Compliance Component Names	• Host-Based IDS • Network-Based IDS • Application-Based IDS
Associated Product Components	
List the Product Component Names	

TECHNOLOGY AREA DETAIL			
Supporting Documentation	NIST SP 800-31 Intrusion Detection Systems (IDS)		
Document Source Reference #	www.csrc.nist.gov/publications/nistpubs		
Standard Organization / 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 Keywords	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse		
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	3/27/2003	*Date Accepted / Rejected*	05/14/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			