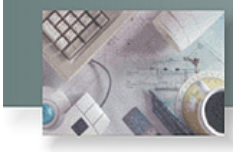

Compliance Component

DEFINITION	
Name	Logon Banners
Description	A Logon Banner is verbiage that an end-user sees at the point of access to a system which sets the right expectations for users regarding authorized and acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.
Rationale	Failure to include a logon banner regarding authorized and acceptable use of a computer system can make it difficult to prosecute violations when they occur. Legal cases exist in which defendants have been acquitted of charges for tampering with computer systems because no explicit notice was given prohibiting unauthorized use of the computer systems involved. In other cases, organizations have been taken to court for alleged violations of individual privacy because no notice was given and acknowledged regarding authorized monitoring of users' activities on computer systems.
Benefits	• Logon Banners are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers. • Pre-logon warning messages can deter unauthorized use, increase IT security awareness, and provide a legal basis for prosecuting unauthorized access. • A key to establishing that a user has no right to privacy when using State of Missouri networks and/or computer systems is the implementation of a logon banner.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Logical Access Controls
List Product Component Name	

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	Logon banners are required on all State of Missouri Information Technology access points. Such a banner shall warn authorized and unauthorized users: • What is considered the proper use of the system.

	• Only authorized users are to proceed beyond the banner. • Users who login represent that they are authorized to do so. • Unauthorized system usage or abuse is subject to disciplinary action and/or civil and criminal action. • Use of the system constitutes consent to monitoring. • Use of the system constitutes consent to the retrieval and disclosure of information stored on the network. • Users of the system shall have no reasonable expectation of privacy in the network. • Contains express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring. • Require users to "click through" or otherwise acknowledge the banner before using the system. Logon banners should not identify sensitive information about the organization, the data systems, network, hardware, operating system, system configuration, or other internal matters. • The following are two examples of logon banners that could be used for users connecting to internal computer systems: *Example 1* NOTICE TO USERS This is a State of Missouri computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized State and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning. *Example 2* WARNING! Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution or employee discipline. Authorized personnel may monitor any activity or communication on the system and may retrieve any information stored within the system. By accessing and using this computer,

	you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs and other hand-held peripherals, CD-ROMs, etc.) Descriptions of unauthorized use may be found (fill in the blank) • Each Agency should tailor its logon banners to their precise needs. • Any questions should be directed to your organization's legal counsel.		
Document Source Reference #	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	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		
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	Logon, username, welcome screen		
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	03/06/2003	*Date Accepted / Rejected*	03/24/2003
Reason for Rejection			
Last Date Reviewed	07/01/2004	*Last Date Updated*	08/10/2004
Reason for Update	Added DOJ example		