Product Component

DEFINITION	
Name	Computer Associates InoculateIT (server)
Description	Provides virus detection and removal solution for servers.
Rationale	• Meets State of Missouri Virus Detection and Elimination criteria for servers as defined within the MAEA; • Currently operating successfully within State infrastructure; and • Listed as a niche player by the Gartner group and the Butler group, and certified by the ICSA.
Benefits	Provides comprehensive protection for enterprise servers capturing both known and new viruses before they infect multiple users.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the name of the associated Technology Area	Virus Detection & Elimination

KEYWORDS	
List all Keywords	Virus, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management

VENDOR INFORMATION			
Vendor Name	Computer Associates	*Website*	www.ca.com
Contact Information	Michael.Ramatowski@ca.com		

POTENTIAL COMPLIANCE ORGANIZATIONS/GOVERNMENT BODIES			
Standard Organizations			
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Bodies			
Name	NIST	*Website*	nvl.nist.gov
Contact Information			

COMPONENT REVIEW	
List Desirable aspects	• Terminal server support • Supports Microsoft, Linux, Sun, Netware & Macintosh operating systems • Low cost of ownership • Centralized policy management • Remote manageability • Enterprise reporting • Administrator alerting • Flexible scanning options • Expedient virus updates
List Undesirable aspects	• System performance impacts (e.g., scan at logon). • Potential software conflicts. • Less market share than other vendors – increasing risk of vendor longevity issues.
ASSOCIATED COMPLIANCE COMPONENTS	
Product	
List the Product-specific Compliance Component Names	
Configuration Links	
List the Configuration-specific Compliance Component Names	
COMPONENT CLASSIFICATION	
Provide the Classification	☐ *Emerging* ☐ *Current* ☒ *Twilight* ☐ *Sunset*

Component Sub-Classification

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☒ *Variance*	TBD	Pending results of Business Case review for agencies requesting continued use of product.
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	Though CA InoculateIT meets most of the basic criteria established for selection of server virus protection, it has been marked as Twilight for the following reasons: • It has not generated sufficient demand across the State to be considered an acceptable enterprise-wide solution. • As it is not widely used across the State, the purchase of CA InoculateIT for servers does not keep with the Enterprise Principles related to cost reduction through consolidated purchasing power. • The continued use of CA InoculateIT also impacts many of the interoperability principles of enterprise architecture including: o Convergence towards a common architecture o Elimination of "islands" of technology o Elimination of overlapping technologies and solutions o Avoiding the proliferation of technologies and solutions. • According to Gartner Research, CA InoculateIT is a niche player in the anti-virus market, not a market leader or visionary. Use of CA InoculateIT for servers requires a variance business case.
Migration Strategy	
Document the Migration Strategy	Organizations using CA InoculateIT for servers should begin investigation of the budget, training, and any conversion issues associated with moving to one of the server anti-virus products labeled as "current" within the MAEA. These organizations should look for opportunities (such as server image or O/S upgrades) to migrate to one of the MAEA approved products.
Impact Position Statement	
Document the Position Statement on Impact	Only those agencies and/or organizations within the State of Missouri actively using CA InoculateIT will be impacted. • This change should have minimal impact to the physical technical environment. • Such a migration should not have a visible impact to end-users. • The largest impact will be the conversion efforts necessary to replace CA Inoculate IT on the organizations servers with acceptable MAEA approved server anti-virus software.
AGENCIES	
List the Agencies Currently Utilizing this Product	Office of the State Courts Administrator
CURRENT STATUS	
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*

AUDIT TRAIL			
Creation Date	02/06/2003	*Date Accepted / Rejected*	02/27/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			