# Product Component

| DEFINITION | |
|---|---|
| *Name* | CS-MARS – (Cisco Monitoring, Analysis and Response System). |
| *Description* | CS-MARS is a hardware and software device which can include single or multiple appliances used to perform network security functions. |
| *Rationale* | It offers the ability to centrally monitor network security devices, perform threat management and the ability to mitigate suspect activity to maintain network security compliance. |
| *Benefits* | • Can be distributed within an agency network based upon segment, group, physical location, etc.<br>• Scalable<br>• Correlates and aggregates logs with events from SNMP supported network devices, security devices and appliances, hosts, applications, and network traffic into a central database.<br>• Uses a customized rule base to reduce false positives.<br>• Cost is not based upon number of devices monitored. |

| ASSOCIATED TECHNOLOGY AREA | |
|---|---|
| *List the name of the associated Technology Area* | Intrusion Detections Systems |

| KEYWORDS | |
|---|---|
| *List all Keywords* | IPS, IDS, detection, security, devices, compliance, anomalies, attacks |

| VENDOR INFORMATION | | | |
|---|---|---|---|
| *Vendor Name* | Cisco | *Website* | www.cisco.com |
| *Contact Information* | | | |

| POTENTIAL COMPLIANCEORGANIZATIONS/GOVERNMENT BODIES<br>**Standard Organizations** | | | |
|---|---|---|---|
| *Name* | | *Website* | |
| *Contact Information* | | | |

| Government Bodies | | | |
|---|---|---|---|
| *Name* | Sarbanes-Oxley, the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA) in the United States, and the EU's Revised Basel Capital Framework (Basel II). | *Website* | |
| *Contact Information* | | | |

## COMPONENT REVIEW

### Platform Information

| | |
|---|---|
| *Hardware Platform Support* | No additional hardware is required to install and operate CS-MARS |
| *Operating System Support* | Hardened Linux operating system software. |

### Review Aspects

| | |
|---|---|
| *List Desirable aspects* | • Provides network intelligence to correlate network anomalies and security events<br>• Validates incidents<br>• Mitigates attacks by taking advantage of existing network and security infrastructure<br>• Monitors systems, network, and security operations to aid in compliance |
| *List Undesirable aspects* | • Proprietary system<br>• No professional training is available<br>• Product is in infancy stage<br>• May require other Cisco products to be fully implemented |

## ASSOCIATED COMPLIANCE COMPONENTS

### Product

| | |
|---|---|
| *List the Product-specific Compliance Component Names* | None |

### Configuration Links

| | |
|---|---|
| *List the Configuration-specific Compliance Component Names* | None |

## COMPONENT CLASSIFICATION

| | |
|---|---|
| *Provide the Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* |

## 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* | |

## AGENCIES

| | |
|---|---|
| *List the Agencies Currently Utilizing this Product* | DOLIR, OA, OSCA |

## CURRENT STATUS

| | |
|---|---|
| *Provide the Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* |

## AUDIT TRAIL

| | | | |
|---|---|---|---|
| *Creation Date* | 06/08/06 | *Date Accepted / Rejected* | 06/13/06 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |