CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Program Management								
Security Policy-setting + Advisory	CISO's Office	CISO's Office	EIS, Agencies	Develop, implement, and maintain the full spectrum of administrative security policies necessary to create and maintain an appropriate Statewide information security program. Compliance to the Statewide security policies is mandatory for each State agency.	Participate as the Subject Matter Expert (SME) on the DAS policy group to develop and guide security policies.	Understand and comply with policies. Provide input and feedback as draft policies are developed or existing policies are being reviewed for potential updates.	Understand and comply with policies. Provide input and feedback as draft policies are developed or existing policies are being reviewed for potential updates.	
**** Statewide Security Management Plan***	CISO's Office	CISO's Office	EIS, Agencies	Develop, implement, and maintain the Statewide Security Management Plan (SMP), which describes the way in which information security and risk management is achieved by the security program.	Due to resource constraints and other priorities, CSS is not providing this service at this time.	Create System Security Plans for all systems.	Create System Security Plans for all systems.	
Security Program and Resource Management	CISO's Office	CISO's Office	EIS, Agencies	Build, maintain, and improve the Statewide information security program including requesting and providing State funding and State resource management for security efforts. Note: Agency funding and resources are the responsibility of the agency.	The State CISO's office develops the State's security program for the Executive Branch. This includes funding and other resource requests and strategic planning that aligns with the Enterprise Information Services Strategic Framework.	Participate with the CISO office as needed to provide input and support the program.	Participate with the CISO's office as needed to provide input and support the program. Follow program guidance, policies and directives.	

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Governance, Risk and Compliance								
Working Group(s) Sponsorship	CISO's Office	CISO's Office	EIS, Agencies	Chair and facilitate security working groups for communication and collaboration, including a CIO Working Group and a working group for agency-specific security personnel.	The State CISO chairs the Information Security Council with is comprised of staff from Agencies, Boards and Commissions who have a security role or are heavily involved in implementing operational security for the Agency. Additionally non-Executive branch security staff also participate. The Deputy CISO participates monthly in the State CIO Council to share information, gather feedback, etc.	Provide appropriate representation and participation in the Information Security Council.	Provide appropriate representation and participation in the Information Security Council.	
**** CISO Communication Network***	CISO's Office	CISO's Office	Agency Leadership	Conduct periodic 1-on-1 meetings to communicate Statewide security program updates and discuss agency-specific feedback and news.	The State CISO meets with Agency Directors to discuss current status of the program, the State's security posture and upcoming items. Also discussed is plans the Agency may have and how CSS could be engaged and provide assistance.	Meet with the State CISO, share information about upcoming or ongoing Agency activities so that CSS can engage and provide assistance as needed.		
Requirements-setting + Advisory	CISO's Office	CISO's Office	EIS, Agencies	Provide guidance for security requirements beyond the requirements established at the State level. Requirements help EIS and agency operations satisfy policies. Note: Agencies are accountable for specific legal/regulatory requirements where applicable.	The BISO team is available to consult with agencies about security requirements that may be needed which are beyond the standards set for the State.	Agencies are accountable for specific legal/regulatory requirements where applicable.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
General Security Awareness Training	CISO's Office	GRC	EIS, Agencies	Develop, conduct, and maintain a Statewide general security awareness-training program that includes annual security training, quarterly security awareness campaigns, Cyber Security Month every October, and sponsored secure coding training. *Note: Specific legal/regulatory-mandated training is the responsibility of agencies where applicable.*	* Provide annual security training through the State Learning Management System * Provide Quarterly Security Awareness material: Short videos, email templates, & printed material *Provide a Phishing Simulation program *CSS does not currently provide secure coding training	Agencies need to support, disseminate and publish the materials and provide time for staff to participate and complete assigned trainings. Agencies need to provide secure coding training to developers and work with CSS to have new and modified code for external facing systems scanned for vulnerabilities prior to release.		

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Security Architecture								
Standards-setting + Advisory	CISO's Office	CISO's Office	EIS, Agencies	Provide guidance while working closely with Strategy & Design for security standards beyond the standards established at the State level. EIS and agency operations implement standards to satisfy requirements. *Note: Specific legal/regulatory standards are the responsibility of agencies where applicable.*	Participate in the development, publication and maintenance of security standards.	Provide input and feedback on proposed security standards.Agencies will need to support, implement and adhere to security standards	Provide input and feedback on proposed security standards. Agencies will need to support, implement and adhere to security standards	

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Infrastructure and Data Protection								
Endpoint Security Baseline Guidance	CISO's Office	Operations	DCS, Agencies	Provide endpoint (server and client) security baseline configuration guidance to entities responsible for building server infrastructure and client devices for users.	Provide infrastructure and support for recurring benchmark scans and reporting.	Identify hosts and related benchmarks for recurring scans. Manage host adherence to selected benchmarks.	Identify hosts and related benchmarks for recurring scans. Manage host adherence to selected benchmarks.	Future service leveraging CIS benchmarks (available at no cost via MS-ISAC) and Tenable scanning infrastructure. May require additional scanners in some cases.
**** SDLC Process Framework + Advisory***	CISO's Office	GRC	Agencies	Establish, review, and maintain a Statewide software development lifecycle (SDLC) process framework to be adopted and adapted as necessary for developing secure applications, with advisory as requested.	Due to resource constraints and other priorities, CSS is not providing this service at this time.	Have a defined and documented software development lifecycle process framework that they follow.		
**** Data Protection Configuration Guidance***	CISO's Office	Operations	DCS, Agencies	Provide data protection configuration guidance to entities responsible for building and maintaining PKI infrastructure and other data protection mechanisms.	Provide guidance and help evaluate security risks of agency proposed systems.	Contact ESO Info for guidance.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Network Operations Consulting	CISO's Office	Operations	DCS, Agencies	Provide network-related advisory services upon request. This includes perimeter security control review or guidance, zoning and resource placement strategy review or guidance, and endpoint admission policy review or guidance. Includes border and edge network controls.	Network security services provides the core technical security infrastructure and related service offerings that agencies rely on to effectively support their mission. Network security services manages software, hardware, processes, and procedures to ensure all data and communications are appropriately secured for availability and access. Specific Services Includes: Firewall configuration SSL Termination SSL VPN IPSec VPN Proxy Server Load Balancing Dos/DDoS Services	Agencies submit requests through our customer portal (S3)	Submit requests through our customer portal (S3)	
Service	**Accountable Owner**	**Execution Responsibility**	**Consumer**	**Description**	**CSS Services**	**Agency Responsibilities**	**EIS (DCS/CDO, CTO, etc…) Services**	**Comments**
Identity and Access Management								
**** Identity Lifecycle Management + Advisory***	CISO's Office	GRC	EIS, Agencies	Establish and maintain a Statewide identity lifecycle process to be adopted and adapted as needed, with advisory as requested. Lifecycle process includes identity-proofing requirements, personnel badging processes, and the use of directory services.	Due to resource constraints and other priorities, CSS is not providing this service at this time.	Continue to apply their identity control methods.	Continue to apply their identity control methods.	

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Security Operations Center								
NIDS Monitoring	CISO's Office	SOC/Operations	DCS, Agencies	Provide a Network Intrusion Monitoring Service through the identification and assessment of relevant events triggered by Intrusion Detection System (IDS) devices.	Enterprise-level network threat detection for north-south traffic as well as limited monitoring of east-west traffic.	Investigate and provide feedback on all reported anomalous activity related to IDS events.		Currently includes MS-ISAC Albert service, CSS SOC implementation of QRadar Network Insights (QNI), CSS deployed Snort IDS sensors and the perimeter firewall's IDS capabilities.
Firewall Log Monitoring	CISO's Office	SOC	DCS, Agencies	Provide a Firewall Monitoring Service through the identification and assessment of relevant events within Enterprise-scoped firewall logs collected centrally.	Currently accept security event logs from the enterprise perimeter firewalls for analysis in CSS SOC SIEM (QRadar). Future plan is to mature the capability with Managed Security Service Provider (MSSP) and possible expansion of security events from border firewalls.	Investigate and provide feedback on all reported anomalous activity related to firewall security events.		Need a comprehensive list of firewalls to identify gaps in coverage
Platform Log Monitoring	CISO's Office	SOC	DCS, Agencies	Provide monitoring of security-related event logs from Enterprise-scoped platform devices collected centrally.	Limited capability/capacity with current implementation primarily focused on the state data center (DCS). Future plan is to add capacity and mature the capability with MSSP.	Investigate and provide feedback on all reported anomalous activity related to platform log monitoring. Provide access to requested security events in platforms managed by the agency.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Security Advisories	CISO's Office	SOC	DCS, Agencies	Publish security advisories using third party and internally-generated data sources and threat information. *Note: Management of agency-specific industry, legal, or regulatory sources are the responsibility of each agency.*	Service currently provided by CSS SOC. Future plan is to mature the capability with MSSP.	Provide CSS SOC an email distribution list (DL) for delivery of advisories. Notify the CSS SOC of any relevant agency-specific advisories.		Currently includes MS-ISAC, CISA and other select advisories and state generated intelligence with the latter being extremely limited. Dependent on agencies providing a DL for notification.
Incident Recording	CISO's Office	SOC	DCS, Agencies	Record security incident details to allow CSS to correlate reported incidents and identify potentially wider problems, and to aggregate reported incidents to identify Enterprise-wide incident trends. *Note: Agencies are responsible to notify the SOC of security incidents they identify to support this service.*	Act as a centralized repository for all cyber security incidents that occur within the executive branch.	Report all known or suspected incidents within 24 hours. Review any alerts/information provided by CSS and assess whether there is an impact to the Agency's systems and data in their custody.		
Incident Consulting	CISO's Office	SOC	DCS, Agencies	Provide consultation for management and staff at any stage of the security incident response process, from initial triage to appropriate response to the final closeout report. *Note: Agencies may request help from the SOC team at any time during incident response.*	Service currently provided by CSS SOC. CSS SOC also has vendors on retainer for larger scale incidents. CSS SOC also has an agency Incident Response (IR) plan template available for agency use. CSS SOC will also support tabletop exercises with agencies. Future plan is to mature the capability with MSSP.	All agencies must have an incident response plan and should perform regular tabletop exercises against the plan. The CSS SOC provides a template that agencies can use to establish an IR plan. Agency must notify CSS of any incident and provide regular updates on status and progress. State CISO will notify LFO if appropriate.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Incident Response	CISO's Office	SOC	DCS, Agencies	Provide Incident Response (IR) services to entities without the expertise or capacity to perform them, and lead incident response for all incidents which may be delegated back to the agency below objectively defined thresholds. The SOC will help coordinate and craft public communications about incidents.	Service currently provided by CSS SOC. CSS SOC also has vendors on retainer for larger scale incidents. CSS SOC also has an agency Incident Response (IR) plan template available for agency use. CSS SOC will also support tabletop exercises with agencies. Future plan is to mature the capability with MSSP.	All agencies must have an incident response plan and should perform regular tabletop exercises against the plan. The CSS SOC provides a template that agencies can use to establish an IR plan. Agency must notify CSS of any incident and provide regular updates on status and progress. State CISO will notify LFO if appropriate.The State CISO must be notified prior to any public release being made and must be provided a copy of the proposed release.		CSS does not participate in the crafting of public communications other than to advise on technical details and the extent to which specific information should be shared.
IT Forensics	CISO's Office	SOC	DCS, Agencies	Make advanced technical forensic examination or expertise resources available as part of incident investigations.	CSS SOC has limited forensic capabilities in-house. Microsoft contracts and IR retainers are available for service augmentation. Future plan is to mature the capability with MSSP.	Contact CSS at ESO SOC to advise when assistance is needed.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Internal Vulnerability Scanning	CISO's Office	SOC	DCS, Agencies	Provide monthly internal vulnerability scans through the use of a general-purpose vulnerability discovery tool identifying missing patches, unsupported software, and common system misconfigurations. The tool supports both authenticated and unauthenticated scans. Scan reports are provided for remediation.	CSS-SOC provides the infrastructure and related support enabling agencies to perform vulnerability scanning. In the near future, CSS-SOC will provide an agency vulnerability management plan template to help each agency facilitate a comprehensive approach to risk-based vulnerability management.	Schedule weekly scans of all servers and end point devices. Review the results to identify potential issues. Address any issues found.		
External Vulnerability Scanning	CISO's Office	SOC/GRC	DCS, Agencies	Provide monthly unauthenticated vulnerability scanning for registered internet- facing assets. Scan reports are provided for remediation.	CSS-SOC will coordinate CISA vulnerability scanning of agency IP address space for registered Internet-facing assets. Weekly reports will be provided to the agencies for tracking and remediation. CSS-GRC Assessment Team currently conducts external vulnerability scanning for registered internet-facing assets during assessments.	Agency provides IP address space to be scanned to the SOC as well as a distribution list (DL) to which their weekly report will be delivered. Agency remediates any vulnerabilities identified by the scan.		
Vulnerability Prioritization	CISO's Office	SOC	DCS, Agencies	Provide vulnerability remediation prioritization recommendations with vulnerability scan results based on vulnerabilities per host (VPH), host type, and host criticality where available.	CSS-SOC will be migrating from the critical per Host (CPH) to a risk-based metric. Additionally, CSS-SOC will work with agencies to segregate their assets to more readily identify risk. (This ties into the Agency's required VM Plan noted above)	Agencies need to work with CSS-SOC to appropriately segregate their assets based on risk.		

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
*** Penetration Testing**	CISO's Office	GRC	DCS, Agencies	Make penetration testing resources available as part of an overall vulnerability management program.	CSS-GRC Assessment Team works with agency to determine scope of penetration testing	Agency requests Penetration testing from CSS		
Threat Hunting	CISO's Office	SOC	DCS, Agencies	Provide limited scenario threat hunting to determine if an incident has occurred before detection. Results feed into the SOC's incident response process.	CSS-SOC currently performs ad hoc threat hunting. Future plan is to mature the capability with MSSP.			
Red/Blue Teaming	CISO's Office	GRC	DCS, Agencies	Work with CSS, DCS or agency resources in a red team/blue team exercise to conduct advanced tests of incident detection and response processes and tools.	[Future] CSS-SOC will work with the National Guard to test detection and response capabilities of the CSS-SOC on behalf of agencies and DCS. Future plan is to mature the capability with MSSP. CSS-GRC Assessment Team conducts threat emulation using Mitre Att&ck Framework activities in coordination with other EIS divisions and agency personnel.	Agency works in collaboration with CSS-GRC Assessment Team to monitor tests and report events	CSS and DCS works in collaboration with CSS-GRC Assessment team to monitor tests and report events	Assessment Team conducts threat emulation activities as part of the CIS and Risk Assessment. Currently Threat Emulation is a 'purple team' exercise. In the future CSS-GRC will conduct red team exercises in collaboration with CSS and agency resources.

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Security Administration								
**** Release Management Requirements + Advisory***	Agencies	GRC	DCS, Agencies	Provide security impact assessments for all major changes introduced via release management processes and reviewed in the CAB.	Due to resource constraints and other priorities, CSS is not providing release management requirements. However, CSS can provide guidance and advice around risks related to a particular release upon request through the BISO team.	Continue to follow and mature internal release management processes. Reach out to CSS for advice as needed.		
Change Management Requirements + Advisory	CISO's Office	Operations	DCS, Agencies	Provide security impact assessments of non-routine changes introduced via change management processes and reviewed in CRBs against procedural, logical, or technical controls.	Each DCS/CSS formal change goes through a security impact review prior to implementation	Agencies have the ability to review each change and view the security impact of a given change.Agencies should utilize their own internal change review process. For those who don't have one, they should implement a basic change review process.		

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Systems Integration								
**** Secure Technology Transformation Guidance***	Agencies	GRC	DCS, Shared Services, Strategy & Design, Agencies	Provide technology transformation guidance to assist with managing the integration of disruptive technologies in a secure manner without negatively affecting the security program and infrastructure.	Due to resource constraints and other priorities, CSS is not providing this service at this time.			

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Vendor Management								
Vendor Contract Review	Agencies	GRC	DCS, Agencies	Provide vendor contract reviews to determine the security risk associated with the vendor contract and provide standard security terms and conditions for inclusion.	BISO's assigned as a security SME as part of the Agency's project team	Agency requests a BISO as a SME for their IT investment	P3 teams conducts oversight on all IT investments	
**** Vendor Security Evaluation + Advisory***	Agencies	GRC	EIS, Agencies	Evaluate potential vendors and service providers against internal security requirements and controls. Maintain an inventory of evaluations of audited vendors. Note: The inventory of evaluations does not constitute a pre-approved list of vendors. This service does not provide approval from a procurement perspective.	Participate in statewide price agreements, RFP's, contract renewals.CSS does not maintain an inventory of evaluations of audited vendors.	Agencies participate in statewide price agreements , RFP's etc.	This is a shared responsibility with EIS BaseCamp & DAS Procurement for statewide price agreements. BaseCamp keeps the approved list of vendors.	

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
Security Consulting								
Security Risk Assessment	CISO's Office	GRC	Agencies	Provide biannual information security risk assessments against CIS Controls to gauge the health of the security program, provide lists of strengths and weaknesses, and suggest a roadmap and plans to improve the security posture.	Currently the Assessment team conducts cybersecurity assessments against the CIS controls.	Agencies need to remediate the findings and be available to participate in the assessments (interviews, Scoping, Providing documentation). Agencies are to report assessments and audits that they receive outside of CSS.		With current CSS staffing we are unable to provide biannual assessments to all executive branch agencies. For 2020, the assessment team was able to complete aprox 18 assessments with current resources (includes 3 Job Rotations)CSS-SOC: In support of assessments, CSS-SOC is focused on providing services to address gaps in CIS Basic 6 and all IG1 subcontrols. Ex: DNS Filtering, Benchmarks (mentioned under SOC tab, etc.)
Business Enablement + Advisory	CISO's Office	GRC	Agencies, Boards, and Commissions	Provide expert cybersecurity policy, consulting, and advocacy services with a priority to reduce security risks.	BISO's are the Security SME expert for agencies to utilize to provide guidance on security standards and best practices while advocating reducing or mitigating security risks.	Agencies contact CSS to ask for security assistance		Future state: Align the BISO's to the Governor's 6 policy areas
**** Business Case Security Consulting***	CISO's Office	GRC	EIS	Provide security perspective and guidance for business case development of new technologies, tools, or services.	A BISO will be a security SME for all agency IT investments	Agency requests a BISO as a SME for their IT investment	This is a shared responsibility between Agencies, ASCIO's, ITPM's. A BISO will be a security SME	

CSS Service Catalog

Service	Accountable Owner	Execution Responsibility	Consumer	Description	CSS Services	Agency Responsibilities	EIS (DCS/CDO, CTO, etc…) Services	Comments
SOC Advisory	CISO's Office	SOC	EIS, Agencies	Provide guidance and advisory services upon request for the development and improvement of agency-specific vulnerability management and incident response programs. *Note: Reference SOC services for additional information on areas of expertise.*	See comments under SOC tab			
Configuration Security Review	CISO's Office	GRC	DCS, Agencies	Provide configuration reviews upon request to identify potential configuration concerns in operating systems, network equipment, and/or application servers.	GRC team will provide review of system artifacts (Vulnerability Scans, Config Scans, SSP, etc.)	Agency provides the system artifacts (Vulnerability Scans, Config Scans, SSP, etc.) to GRC for configuration review		CSS is currently perform this task, Agencies need to be capable on their end to perform the Bench Mark scanning CSS-SOC will provide Benchmark services in the near future (See SOC tab for more information)

Acronyms

ASCIO	Assistant State Chief Information Officer
BISO	Business Information Security Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CSS	Cyber Security Services
DAS	Department of Administrative Services
DCS	Data Center Services
EIS	Enterprise Information Services
GRC	Governance, Risk, and Compliance
LFO	Legislative Fiscal Office
MS-ISAC	Multi State - Information Sharing and Analysis Center
MSSP	Managed Security Service Provider
P3	Project Portfolio Performance
SME	Subject Matter Expert
SOC	Security Operations Center
SSP	System Security Plan