# Cyber Security Services

# Service Catalog

Enterprise Information Services | State of Oregon

July 2026

ENTERPRISE
information services


ENTERPRISE INFORMATION SERVICES
OREGON
STATE CYBER COMMAND

# A Letter from the CISO

Cybersecurity for the state of Oregon is about more than stopping every threat. It is about building practical, shared protections, making sound decisions early, and maintaining the ability to respond and recover when something goes wrong. In government, our mission is not only to reduce risk but to do so in a way that supports both continuity of public services and responsible stewardship of resources while earning the trust Oregonians place in us.

This service catalog is intended to help agencies understand how Cyber Security Services (CSS) partners with them to reduce risk across the enterprise. Some services are delivered centrally by CSS, some require agencies to engage CSS before acting, and some remain agency-owned capabilities supported by CSS standards, templates, or advisory services. In every case, cybersecurity is a shared responsibility. Effective cybersecurity depends on strong enterprise services, informed agency leadership, timely coordination, and a clear understanding of where ownership begins and ends.

We organized this catalog using the NIST Cybersecurity Framework 2.0 because it provides agencies with a clear and common language for governance, identification, protection, detection, response, and recovery. That structure reflects how cybersecurity works in government operations: prevention matters, but resilience, coordination, and restoration matter just as much. This catalog is meant to set practical expectations by explaining what CSS provides, what agencies are expected to do, and how we work together to strengthen the state's overall cybersecurity posture. As statewide services continue to mature, this catalog will also help agencies understand where enterprise capabilities are evolving and how those changes may affect agency planning and implementation.

I encourage agencies to use this catalog to engage CSS early, understand where statewide services are required, and strengthen the partnership needed to protect and restore critical public services for Oregonians. The strongest cybersecurity outcomes come from shared commitment, clear roles, and steady collaboration. CSS is committed to being a trusted enterprise partner in that work.

**Ben Gherezgiher**
State Chief Information Security Officer


Services in this catalog are organized using the NIST Cybersecurity Framework functions.

# Table of Contents

# 1. Catalog Overview and Expectations

## 1.1 PURPOSE AND SCOPE

This catalog describes the Cyber Security Services delivered, coordinated, or governed by Enterprise Information Services (EIS), Cyber Security Services (CSS) for Oregon state agencies, boards, and commissions. It is written in plain language so leaders, program staff, and technical teams can quickly understand what CSS does, when agencies must involve CSS, and where responsibilities remain with the agency.

## 1.2 NIST CYBERSECURITY FRAMEWORK 2.0 ALIGNMENT

CSS organizes this catalog using the NIST Cybersecurity Framework (CSF) 2.0. CSF[1] gives the state a common way to describe work across the lifecycle of cybersecurity: govern, identify, protect, detect, respond, and recover. Using that model helps agencies see that cybersecurity is more than prevention. It also includes resilience, coordinated response, and restoration of services after an event.


**NIST CSF 2.0 Core Functions:**

- **Govern (GV):** Establish statewide cyber strategy, roles, accountability, and policy oversight.
- **Identify (ID):** Understand assets, data, systems, and risk across the enterprise.
- **Protect (PR):** Implement safeguards to prevent and reduce cyber events.
- **Detect (DE):** Ensure timely discovery of threats and anomalous activity.
- **Respond (RS):** Coordinate actions to contain and mitigate cyber incidents.
- **Recover (RC):** Restore services and improve resilience after events.

CSF 2.0, together with Oregon's Statewide IT Control Standards, provides a governance-driven, nationally recognized framework that guides how Oregon state government manages cybersecurity risk across agencies. It also aligns agencies to a common, repeatable, measurable cybersecurity standard. Together, CSF 2.0 and the Statewide IT Control Standards ensure resilience is built into both governance and day-to-day operations, supporting reliable service continuity, faster recovery, and a stronger statewide cyber risk posture.

## 1.3 STATEWIDE AUTHORITY AND STANDARDS ALIGNMENT

This catalog also supports Oregon's statewide cybersecurity governance structure. EIS has authority under ORS 276A.300[2] to develop and oversee statewide cybersecurity standards[3] and policies. Services described here are intended to help agencies meet those standards, apply minimum required controls, and improve their cybersecurity posture over time.

1 Cybersecurity Framework | NIST
2 ORS 276A.300 – Information systems security in executive department; rules
3 Statewide Information Technology (IT) Control Standards

## 1.4 SERVICE CLASSIFICATION AND OWNERSHIP

CSS services are classified by how they are delivered and owned. Some are enterprise services delivered centrally by CSS, some require agency engagement before action, and others remain agency-owned capabilities supported by CSS standards, templates, review, or coordination.

Delivery timing depends on scope, complexity, request completeness, dependent teams, change windows, and competing enterprise priorities. When a service is tailored to an agency, CSS will work with the agency to define specific responsibilities and next steps.

### How this catalog classifies services

- **Mandatory Service:** an enterprise service CSS provides centrally or requires as part of the statewide cybersecurity program.
- **Mandatory Engagement:** the agency must involve CSS before or during the activity.
- **Requested Service:** the agency may request CSS assistance based on need, timing, and available capacity.
- **Required Agency Capability with CSS Support:** the agency owns the capability, while CSS provides standards, templates, review, or coordination.

## 1.5 OBJECTIVES, DRIVERS, AND PRINCIPLES

This section establishes the mission, vision, objectives, and service principles that guide how CSS delivers enterprise cybersecurity capabilities across the State of Oregon. These statements define the outcomes CSS is working toward, the partnership expected with agencies, and the principles used to prioritize and deliver services. Together, they reinforce that cybersecurity is a shared responsibility, that early engagement reduces risk, and that statewide services are intended to improve consistency, visibility, resilience, and recovery across the enterprise.

| Item | Summary |
|---|---|
| **EIS Strategic Framework Objective** | Improve Oregon's cybersecurity posture. |
| **Desired outcome** | A secure and resilient state of Oregon enterprise where agencies can deliver services confidently, recover from disruption, and meet statewide security requirements consistently. |
| **What success looks like** | Agencies work jointly with the enterprise to proactively reduce risk, use shared enterprise protections, engage CSS early, and improve their cybersecurity posture year over year. |

| Item | Summary |
|---|---|
| **Drivers** | • Provide clear statewide cybersecurity expectations and shared enterprise protections.<br>• Jointly work with agencies to achieve proactive detection and mitigation of cyber threats that threaten state critical information assets.<br>• Engage agencies early so cybersecurity is built into planning, procurement, and design decisions.<br>• Improve statewide visibility, detection, response, and coordinated recovery.<br>• Strengthen agency accountability for required controls, plans, and remediation.<br>• Improve cyber posture over time through recurring assessments, advisory support, and enterprise services. |

## 1.6 CYBERSECURITY SERVICE PRINCIPLES

- Security is a shared responsibility: CSS provides enterprise services, standards, and coordination, while agencies remain responsible for their applications, agency-owned controls, and follow-up actions.
- Early engagement produces better outcomes by reducing rework, clarifying requirements, and avoiding preventable risk in planning, procurement, and design.
- Recovery and restoration matter as much as prevention because cybersecurity also requires effective detection, response, and recovery.
- Enterprise services drive consistency, scalability, visibility, and stronger baseline cybersecurity across the state.
- Service delivery is prioritized using risk, legal or policy requirements, incident severity, urgency, compliance needs, and enterprise impact.

## 1.7 CSS SERVICE VERTICALS

The table below reflects the current CSS service vertical structure and shows how accountabilities are grouped across enterprise consulting, governance and risk management, solutions architecture and identity services, network security operations, and security operations center services.


| Item | Accountabilities |
|---|---|
| **Overarching Services** | Enterprise consulting, secure-by-design advisory, and proactive engagement with agency leadership and technical teams. |
| **Governance and Risk Management** | Business cybersecurity advisory, third-party and investment cybersecurity review, awareness and training, policy, and standards. |
| **Solutions Architecture and Identity Services** | Cybersecurity architecture, cloud cybersecurity advisory, identity and access requirements, and privileged access design guidance. |
| **Network Security Operations** | Firewalls, load balancing, proxies, VPNs, Secure Sockets Layer (SSL) services, and web application firewall capabilities. |

| Item | Accountabilities |
| --- | --- |
| **Security Operations Center Services** | Assessments, monitoring, logging, incident response, tabletop exercises, vulnerability management, threat intelligence, and coordinated recovery support. |

# 2. Rules of Engagement and Service Levels

## 2.1 SERVICE DELIVERY EXPECTATIONS

CSS supports many agencies and manages multiple complex engagements at the same time. Because of that, published timelines are service targets rather than guarantees that every request will begin immediately or move at the same pace. CSS acknowledges requests as quickly as possible, then prioritizes work based on enterprise risk, active incidents, legal or policy requirements, operational urgency, and overall complexity.

For most services, the first step is acknowledgment, intake, and scoping. This allows CSS to confirm the nature of the request, identify dependencies, determine whether other teams or service verticals must be involved, and establish realistic next steps. Final delivery timelines depend on the quality and completeness of information provided, technical complexity, the number of dependent teams, change windows, and competing enterprise priorities already in progress.

Some services include specific onboarding, reporting, or delivery targets based on the nature of the work. In all cases, CSS uses a tiered prioritization model so the highest-risk and most time-sensitive work receives attention first. This helps CSS balance responsiveness to individual agency needs with its broader responsibility to protect the enterprise.

## 2.2 TIERED PRIORITIZATION MODEL

This model ensures that the most critical cybersecurity and operational needs receive attention first, while lower-risk work is planned and scheduled in a way that supports sustainable service delivery.

The priority structure separates work into Group A and Group B categories. Group A priorities represent work that is immediate, urgent, or time-sensitive and may require rapid coordination across teams. Group B priorities represent important work that still supports business outcomes, reduces risk, or addresses service needs, yet does not require the same immediate response as Group A items.

Within each group, work is further organized by tier, ranging from critical items to lower-risk discretionary or maintenance activities. This approach helps CSS set clear expectations, reduce competing priorities, focus resources where they are needed most, and maintain a consistent method for scheduling Cyber Security Services, operational support, and enterprise initiatives.

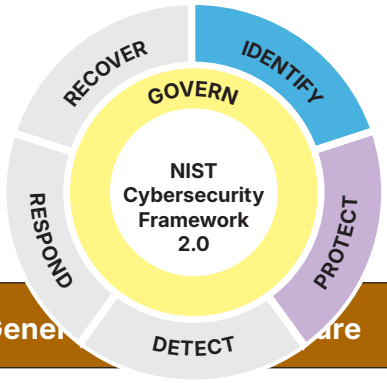
| Group | Tier | Priority Level | Summary |
|---|---|---|---|
| Group A | Tier A-1 | Critical/ Immediate | Issues or initiatives that support a major business outcome pose an immediate cyber or operational risk if not completed or represent a significant security gap that must be addressed. Requires an immediate, all-hands-on-deck response. |
| | Tier A-2 | High / Urgent | Issues that may cause significant disruption to operations or involve high-risk vulnerabilities that have not yet been exploited. Addressed as soon as Tier A-1 issues are completed and stabilized. |
| | Tier A-3 | Medium / Urgent | Initiatives or tasks designed to address minor service or cybersecurity issues that affect a small number of users and have available workarounds. |
| | Tier A-4 | Low / Discretionary | Service optimization changes, long-term initiatives, or work with no significant immediate risk. |
| Group B | Tier B-1 | Critical / Non-Immediate | Issues or initiatives that support a major business outcome pose a non-immediate cyber or operational risk if not completed or represent a security gap that must be addressed. May be done in conjunction with Group A priorities or scheduled immediately after Group A Tier A-1 tasks. |
| | Tier B-2 | High / Non-Urgent | Issues that may cause significant disruption to operations or involve high-risk vulnerabilities that have not yet been exploited. Addressed as soon as Group B Tier B-1 issues are completed and stabilized. |
| | Tier B-3 | Medium | Initiatives or tasks designed to address minor service or cybersecurity issues that affect a small number of users and have available workarounds. Scheduled in conjunction with Group A Tier A-3 initiatives when resources are available. |
| | Tier B-4 | Low | Minor maintenance tasks scheduled as time permits. |

## 2.3 SERVICE DISRUPTION SEVERITY LEVELS

For applicable Network Security Operations services, CSS uses severity (SEV) levels to classify and respond to active service disruptions that affect the availability of supported services. This includes outages, degraded service, failed connectivity, or other disruptions involving CSS-supported firewall, load balancing, proxy, VPN, SSL, Internet Protocol Security Virtual Private Network (IPsec), web application firewall, and related network security capabilities.

SEV levels apply when an active disruption requires response urgency to be determined based on impact, affected services, business criticality, operational scope, and restoration needs. They do not replace the tiered prioritization model used for general service requests, planned work, consulting, onboarding, or routine operational support.

CSS applies SEV levels consistent with the EIS Incident Management process. A lower SEV number represents a higher-priority incident. CSS uses the applicable SEV level to guide response urgency, escalation, communications, restoration coordination, and customer engagement. Agencies are expected to provide timely technical contacts, business impact information, validation support, and decision-makers when needed.




| SEV Level | Availability Impact | Response Anchor | Gener…ure |
|---|---|---|---|
| **SEV-1 Critical** | Highest-impact disruption affecting mission-critical services, public safety services, significant regional or common-cause outages, or conditions that significantly affect critical business services or operations. | 15-minute initial communication; 24x7 response posture where declared. | Immediate incident coordination, elevated communications, assigned incident leadership where required, focused restoration activity, and post-incident reporting when applicable. |
| **SEV-2 High** | Significant production service impact, business-essential service disruption, or failed service that materially affects operations. | Target response within 1 hour for confirmed incidents. | Prompt technical response, customer coordination, escalation as needed, and active restoration work based on business impact and operational urgency. |
| **SEV-3 Medium** | Degraded service, lower-impact network service failure, or disruption where impact is limited and may not materially stop business operations. | Target response within 1 business day. | Standard incident handling with technical troubleshooting, customer updates, and restoration work prioritized based on impact and available resources. |
| **SEV-4 Low** | Limited impact, single-user impact, inconvenience, or a condition where a known workaround exists. | Target response within 2 business days. | Routine incident handling, documented updates, and resolution through normal operational processes. |

Note: The tiered prioritization model applies broadly to CSS service requests, planned work, onboarding, consulting, and operational support. SEV levels apply primarily to active service disruptions where availability of an applicable service is impaired and incident response, restoration, escalation, and communication expectations must be established.

## 2.4 REQUESTING SERVICES

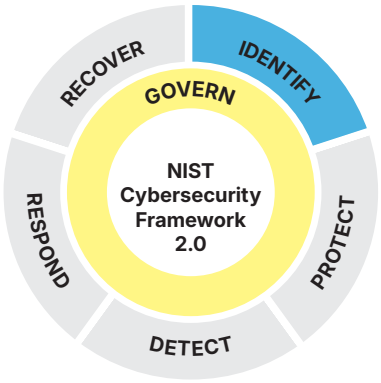
To request a service or ask for agency-specific guidance, agencies will use the standard EIS intake process or email ESO.INFO@eis.oregon.gov. Agencies are encouraged to engage CSS as early as possible when planning new technology, major changes, procurements, architectural decisions, or other security-sensitive implementations. Early engagement helps reduce rework, clarify requirements, and improve the ability to deliver secure and practical outcomes.

**!**

### HIGH IMPORTANCE - Cyber Incident Notification Requirement

If an issue may constitute a cyber incident under an agency's Incident Response Plan, the agency must immediately notify the Security Incident Hotline or contact the Security Operations Center at **eso.soc@eis.oregon.gov**.

# 3. Required Agency Participation and Enterprise Disclosures




## 3.1 STATEWIDE CYBERSECURITY GOVERNANCE AUTHORITY

ORS 276A.300 establishes State Chief Information Officer authority over information systems security in the executive department, including measures needed to protect the availability, integrity, and confidentiality of state information systems. Under that authority, EIS Cyber Security Services provides unified Cyber Security Services for executive department agencies, boards, and commissions within scope. Unless approved by the State CISO through an exception, waiver, or alternate operating model, covered cybersecurity staff, technology, services, and enterprise capabilities are coordinated through CSS.

Agency participation is required where cataloged services support statewide policy, enterprise visibility, coordinated response, and minimum cybersecurity controls. Agencies must also maintain baseline capabilities needed for enterprise services to operate effectively.

This section is intended to make those expectations clear. It does not replace statewide policy, the Statewide IT Control Standards, or agency-specific legal, regulatory, or business obligations.

## 3.2 ENTERPRISE TECHNOLOGY AND SERVICE

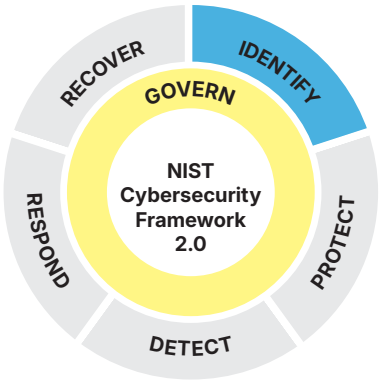
CSS provides and coordinates enterprise capabilities identified in this catalog, including security monitoring and Security Information and Event Management (SIEM), device and identity monitoring, mobile device monitoring, firewall services, virtual private network (VPN) services, vulnerability management coordination, risk management and advisory support, awareness training, and incident response coordination.

When CSS provides, manages, or designates an enterprise cybersecurity service for a cataloged service area or statewide cybersecurity capability, agencies are expected to use the CSS-managed service within the approved scope unless an exception, waiver, or alternate operating model has been formally authorized by the State CISO or designee.

## 3.3 CSS RESPONSIBILITIES

CSS maintains enterprise Cyber Security Services that improve statewide consistency, visibility, response coordination, and compliance with minimum control expectations. This includes operating or coordinating centralized services within CSS scope and providing standards, training, guidance, coordination, and advisory support aligned to statewide requirements and enterprise risk priorities.

## 3.4 AGENCY RESPONSIBILITIES




Agencies, boards, and commissions are responsible for participating in required enterprise Cyber Security Services, complying with statewide cybersecurity policies, plans, standards, and State CISO directives, and operating agency-owned applications within those requirements.

Agency responsibilities include, but are not limited to, the following:

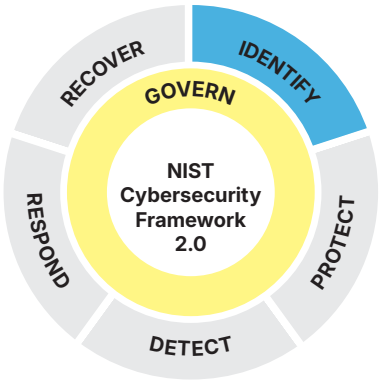
- **Required enterprise services and directives:** Participate in required enterprise Cyber Security Services, onboard to required tools or services, comply with statewide cybersecurity policies, plans, standards, and State CISO directives, and support required remediation and follow-up actions.
- **Assessment remediation:** Collaborate with CSS teams to review identified cybersecurity assessment gaps, support remediation planning, and improve cybersecurity assessment scores. This collaboration is required across agencies, boards, and commissions to help the State collectively meet established cybersecurity posture thresholds and standards.
- **Incident readiness and exercises:** Participate in annual cyber incident exercises and coordinated tabletop exercises, maintain current incident response plans, and coordinate with CSS during cybersecurity incidents, assessments, and response activities.
- **Cybersecurity infrastructure coordination:** Involve CSS before materially changing cybersecurity infrastructure, internet-facing controls, firewall rules or architecture, secure remote access patterns, or identity-related control patterns.
- **Penetration testing and results sharing:** Coordinate penetration testing with CSS and share applicable results with CSS to support enterprise visibility, risk awareness, and coordinated remediation planning.
- **Backup and recovery readiness:** Maintain secure backup and recovery processes that support substantial recovery following a cyber incident. Immutable backups of critical state data are required and must be demonstrated by each agency. CSS resources will be available to validate, advise, and support agencies in strengthening backup and recovery practices.
- **Production environment and system documentation:** Maintain current and complete documentation of agency-owned production network environments, critical applications, services, dependencies, business systems, data inventories, and agency-owned application logs.
- **Vulnerability remediation and recovery expectations:** Remain responsible for vulnerability remediation activities, backup strategies, restoration procedures, backup and recovery compliance, and documentation of the business expectation for substantial operational capability recovery after a cyber incident, unless otherwise documented through an approved enterprise service model.

Agencies remain responsible for agency-owned applications, data, documentation, and operational decisions unless those responsibilities are otherwise assigned through an approved enterprise service model

# 4. Service Catalog

## 4.1 OVERARCHING SERVICES

### 4.1.1 Enterprise Cybersecurity Consulting and Secure-By-Design Advisory




- **Service type:** Requested Service
- **How to engage:** Requested by agency or initiated proactively by CSS through leadership, architecture, project, or operational discussions.
- **Related standards:** PL-8, SA-3, SA-8, SA-9, RA-3, RA-7

#### SERVICE DESCRIPTION

CSS provides broad cybersecurity consulting to help agencies make sound cybersecurity decisions before risk becomes operational debt. This includes secure-by-design advisory, architecture input, cloud cybersecurity consulting, risks and mitigations, IT controls, third-party cybersecurity, and practical guidance for both new initiatives and ongoing operations. This service also includes proactive consultation through recurring leadership touchpoints, including monthly ASCIO meetings, CIO consultations, and other agency leadership engagements where early cybersecurity input can improve planning, sequencing, and risk decisions.

#### SERVICE OBJECTIVES

- Promote early cybersecurity engagement so agencies can build security into projects instead of adding it after the fact.
- Provide consistent statewide guidance that aligns agency decisions with security standards, enterprise capabilities, and realistic operating constraints.
- Help agencies understand tradeoffs, shared responsibilities, and the right sequence for implementation.

#### CSS RESPONSIBILITIES

- Provide cybersecurity architecture input, control recommendations, and practical implementation guidance.
- Advise on cloud cybersecurity, baseline configurations, vendor cybersecurity, and risk mitigation options.
- Participate in recurring leadership and technical meetings, including monthly ASCIO meetings and CIO consultations, to influence architecture, priorities, and cybersecurity decisions early.

#### AGENCY RESPONSIBILITIES

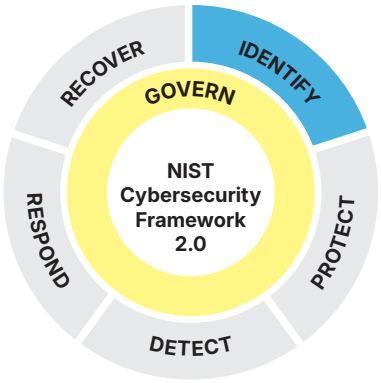
- Engage CSS early for new technology, major design changes, or cybersecurity-sensitive decisions.
- Provide enough business and technical context for CSS to give practical guidance.
- Incorporate agreed controls and follow-up actions into agency planning and execution.

#### SERVICE LEVEL OBJECTIVES

- Acknowledgment and routing follow the tiered service model..

# 4.2 GOVERNANCE AND RISK MANAGEMENT

## 4.2.1 Business Security Enablement and Advisory




- **Service type:** Requested Service
- **How to engage:** Requested by agencies or initiated as follow-up to assessments, risks, or enterprise priorities.
- **Related standards:** RA-3, RA-7, CA-5, CA-7, SR-6

### SERVICE DESCRIPTION

Business Cybersecurity Advisors help agencies understand cyber risk in business terms and translate findings into practical next steps. This service is used to review cybersecurity program maturity, discuss remediation priorities, connect agencies to the right CSS services, and improve posture over time rather than treating cybersecurity as a one-time exercise.

### SERVICE OBJECTIVES

- Communicate cyber risk, options, and tradeoffs in language agency leaders can act on.
- Assist agencies in prioritizing remediation work, plans of action and milestones, and long-term cybersecurity improvements.
- Create measurable follow-up so assessment findings are translated into sequenced remediation work and posture improves over time.

### CSS RESPONSIBILITIES

- Provide aid and guidance to agencies to reduce and mitigate cybersecurity risks.
- Facilitate agency connections across CSS verticals and other EIS programs where assistance or training is needed.

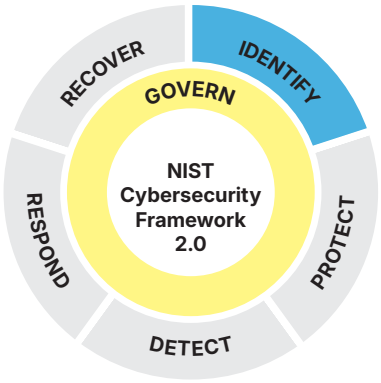
### AGENCY RESPONSIBILITIES

- Provide requested documentation, context, and follow-up status updates.
- Use advisory output to drive prioritization, remediation, and continuous improvement.
- Share progress, blockers, and changed priorities when follow-up work is underway.

### SERVICE LEVEL OBJECTIVES

- Initial scoping target: within 30 calendar days, depending on complexity and enterprise workload.
- Follow-up touchpoints and target dates are established during scoping based on risk and readiness.

## 4.2.2 System Cybersecurity Evaluation




- **Service type:** Mandatory Engagement
- **How to engage:** Agencies must involve CSS when cybersecurity requirements or vendor cybersecurity terms need review, or when major IT investments trigger a review.
- **Related standards:** SA-4, SA-9, SR-5, SR-6, RA-3

### SERVICE DESCRIPTION

CSS evaluates cybersecurity requirements, third-party risk, and solution alignment during procurement, contracting, project gating, and major technology decisions. The review identifies material risks, strengthens cybersecurity language in business and technical artifacts, clarifies required controls and service expectations, and supports decision-making without replacing procurement, legal, or approval authorities.

### SERVICE OBJECTIVES

- Improve cybersecurity requirements in solicitations, contracts, amendments, and technology investments.
- Reduce the risk of onboarding services or solutions that do not meet State cybersecurity expectations.
- Provide a documented cybersecurity view of third-party, solution, service, and control risks before execution or implementation.

### CSS RESPONSIBILITIES

- Review artifacts such as solicitations, contracts, amendments, and technical cybersecurity documentation.
- Ensure cybersecurity requirements, terms, and minimum controls are addressed.
- Coordinate with procurement, oversight, legal, and agency stakeholders as needed.
- Document decisions and identified risks.

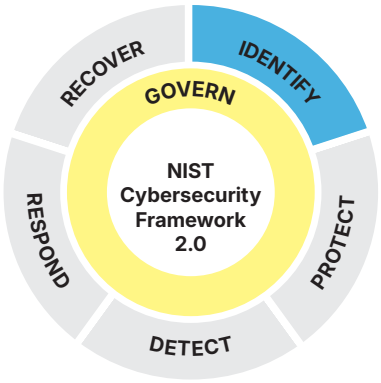
### AGENCY RESPONSIBILITIES

- Bring CSS in early enough for meaningful review.
- Provide complete procurement or project documentation and expected timelines.
- Incorporate required cybersecurity controls and language.

### SERVICE LEVEL OBJECTIVES

- Initial scoping target: within 30 calendar days depending on request volume and transaction complexity.

### 4.2.3 Vendor Cybersecurity Evaluation and Advisory




- **Service type:** Mandatory Engagement
- **How to engage:** Requested or triggered by procurement, architecture, or risk review activity.
- **Related standards:** SA-9, SA-9(1), SA-9(2), SA-9(5), SR-6

#### SERVICE DESCRIPTION

CSS reviews potential vendors and external service providers against internal cybersecurity requirements and maintains awareness of completed evaluations. The service helps agencies make informed risk decisions about whether a vendor appears capable of meeting the state's cybersecurity expectations, but it is not procurement approval, legal approval, or placement on a permanent approved-vendor list.

#### SERVICE OBJECTIVES

- Help agencies understand third-party cybersecurity risk and promote consistent expectations for external service controls, evidence, and follow-up.
- Identify material cybersecurity gaps, unclear ownership of controls, and contract issues before services are adopted.

#### CSS RESPONSIBILITIES

- Evaluate third-party cybersecurity artifacts, assessments, questionnaires, and published attestations.
- Advise on cybersecurity risks, gaps, and required business and technical controls.
- Coordinate with agencies on follow-up questions or compensating controls.

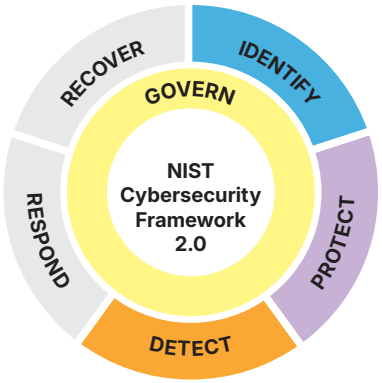
#### AGENCY RESPONSIBILITIES

- Provide vendor documentation and business context.
- Participate in follow-up conversations and decision-making.
- Use the evaluation to inform procurement and risk decisions.

#### SERVICE LEVEL OBJECTIVES

- Target review initiation: within 30 calendar days depending on scope.

## 4.2.4 Cybersecurity Awareness and Training




- **Service type:** Mandatory Service
- **How to engage:** Delivered as part of the statewide program and supported by agencies locally.
- **Related standards:** AT-2, AT-3, AT-4

### SERVICE DESCRIPTION

CSS manages the statewide cybersecurity awareness program to help the workforce build safer habits at work, at home, and while mobile. This service supports the annual awareness training requirement and reinforces key behaviors throughout the year using recurring training, targeted communications, reminders, and other awareness activities. The program is intended to strengthen day-to-day cybersecurity decision-making by helping users recognize common threats, understand their role in protecting state information and systems, and apply practical cybersecurity habits in routine work.

### SERVICE OBJECTIVES

- Improve cybersecurity culture across the enterprise.
- Reduce human risk by providing foundational awareness content and role-based reinforcement where needed.
- Support agency compliance with statewide requirements for cybersecurity awareness.

### CSS RESPONSIBILITIES

- Provide awareness content through the approved learning platform and supporting campaign materials.
- Update content based on emerging threats, lessons learned, and statewide needs.
- Provide program-level communications, guidance, and metrics where available.

### AGENCY RESPONSIBILITIES

- Ensure the covered workforce completes required training.
- Support local communications, follow-up, and accountability for completion and repeat risk behaviors.
- Provide workforce access to the approved learning platform and related program materials.

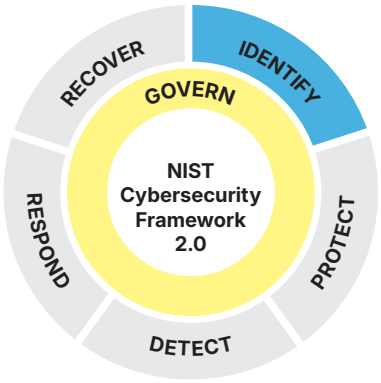
### SERVICE LEVEL OBJECTIVES

- Annual training cycle established each year.
- Supplemental awareness materials and follow-up campaigns are delivered throughout the year.

### ADDITIONAL NOTE

- ORS 276A.323 requires annual information cybersecurity awareness training for covered executive department personnel.

### 4.2.5 Phishing Campaigns




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agency coordination.
- **Related standards:** AT-2, AT-3, SI-8

#### SERVICE DESCRIPTION

CSS conducts recurring phishing simulations to help users recognize suspicious email, reduce click risk, and identify groups that may need additional awareness, coaching, or communication support. The service is designed to build practical awareness through repeated exposure to realistic phishing scenarios and to help agencies better understand human-risk trends over time. Results are intended to support improvement, not one-time testing, and to inform targeted follow-up where patterns of risk persist.

#### SERVICE OBJECTIVES

- Reinforce phishing awareness through realistic practice and repeated exposure.
- Identify repeat risk areas, user groups, or patterns that need targeted follow-up.
- Provide leaders with insight into human-risk trends, phish susceptibility, and targeted follow-up needs.

#### CSS RESPONSIBILITIES

- Plan and operate the phishing simulation program.
- Provide metrics and communications guidance where available.
- Coordinate campaign scheduling and targeted awareness follow-up.

#### AGENCY RESPONSIBILITIES

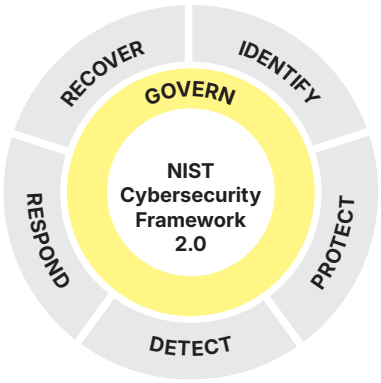
- Support required communications, workforce participation, local coordination, and stakeholder awareness of campaign timing, scope, and follow-up expectations.
- Use results to drive coaching, awareness efforts, accountability, and local follow-up for repeated phishing risk.
- Reinforce reporting expectations and encourage improvement over time.

#### SERVICE LEVEL OBJECTIVES

- Recurring monthly campaign cadence with periodic metrics and communications support.
- Campaign scheduling and targeting may vary based on enterprise priorities, agency readiness, and program capacity.
- Follow-up communications and improvement discussions are provided based on results, trends, and available support capacity.

## 4.2.6 Cybersecurity Awareness Month

- **Service type:** Mandatory Service
- **How to engage:** Annual enterprise campaign supported by agency communications.
- **Related standards:** AT-2, AT-3




### SERVICE DESCRIPTION

CSS coordinates statewide Cybersecurity Awareness Month activities each October to reinforce good cybersecurity habits, highlight current threats, and keep cybersecurity visible for the workforce and agency leadership. The campaign is intended to supplement, not replace, required training by providing a concentrated annual awareness effort built around practical behaviors users can apply in daily work. It also helps agencies reinforce year-round cybersecurity messaging through shared themes, statewide materials, and coordinated outreach.

### SERVICE OBJECTIVES

- Keep cybersecurity visible for the workforce and agency leadership through accessible, timely, and relevant messaging.
- Promote practical habits that reduce avoidable user-driven incidents.
- Support year-round awareness with a concentrated annual campaign.
- Encourage broader participation in cybersecurity awareness activities across the enterprise.

### CSS RESPONSIBILITIES

- Provide statewide campaign themes, resources, and awareness materials.
- Develop or coordinate messaging that aligns with current risks, common user behaviors, and enterprise priorities.
- Share approved content, communication ideas, and supporting materials agencies can use locally.
- Promote consistency in campaign messaging across participating agencies.

### AGENCY RESPONSIBILITIES

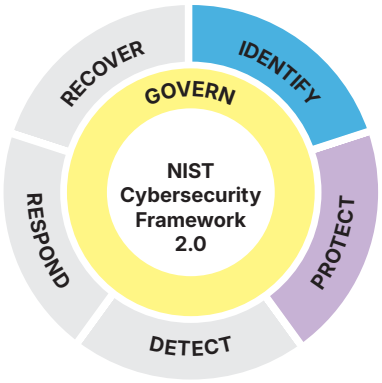
- Promote the campaign internally and give staff time to participate.
- Distribute approved materials and integrate them into local awareness efforts.
- Coordinate internal communications, leadership support, and local participation activities.

### SERVICE LEVEL OBJECTIVES

- Annual campaign delivered during October.
- Campaign materials and communications support are provided in advance of and during the awareness month cycle.
- Agency participation levels and implementation may vary based on agency size, capacity, and internal priorities.

## 4.2.7 Policy and Standards

- **Service type:** Mandatory Service
- **How to engage:** Provided centrally; agencies engage CSS for interpretation, questions, and collaboration.
- **Related standards:** All statewide cybersecurity policies, plans, and standards as applicable




### SERVICE DESCRIPTION

CSS develops, maintains, and interprets statewide cybersecurity policy, the statewide information cybersecurity program plan, and the Statewide IT Control Standards. This service establishes the minimum statewide cybersecurity expectations agencies are required to meet and provides a common governance baseline across the enterprise. It helps ensure agencies have clear direction for implementing controls, aligning cybersecurity programs, and making risk-informed decisions in a consistent way. In addition to publishing and maintaining these governing documents, the service helps agencies understand control intent, apply requirements in practice, and navigate situations where implementation questions or exceptions arise.

### SERVICE OBJECTIVES

- Set clear minimum requirements and promote consistent controls, governance, and risk management practices across agencies.
- Provide interpretation and implementation guidance so agencies can align their local programs to statewide policy and control requirements.

### CSS RESPONSIBILITIES

- Develop and maintain policy, plans, and standards.
- Engage agencies during updates and provide implementation guidance.
- Respond to questions and clarify control intent where needed.

### AGENCY RESPONSIBILITIES

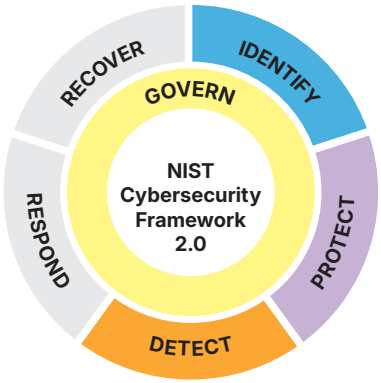
- Incorporate statewide requirements into agency programs, processes, and technology decisions.
- Collaborate with CSS on implementation questions and feedback.
- Request and document deviations and compensating controls when exceptions are necessary.

### SERVICE LEVEL OBJECTIVES

- Responses to questions are typically provided by the end of the next business day.
- Formal policy and standards updates follow the applicable review and approval process.

# 4.3 SOLUTIONS ARCHITECTURE AND IDENTITY SERVICES

## 4.3.1 Cybersecurity Architecture and Secure-By-Design Consulting




- **Service type:** Requested Service
- **How to engage:** Requested by agencies or initiated as part of project, architecture, or modernization discussions.
- **Related standards:** PL-8, SA-3, SA-8, SA-11, CM-6

### SERVICE DESCRIPTION

CSS works with agencies to design cybersecurity into systems, platforms, and implementations from the start. This service includes security architecture reviews, control pattern guidance, secure baseline recommendations, design validation, and consultation on how agency solutions connect to enterprise Cyber Security Services. The goal is to reduce avoidable redesign, clarify required, shared, and inherited controls, and identify dependencies before implementation is too far along.

### SERVICE OBJECTIVES

- Reduce redesign and rework by addressing cybersecurity early in solution planning and design.
- Improve security architecture consistency across the enterprise.
- Make sure agencies understand which controls are required, shared, inherited, or locally implemented.
- Support secure design decisions that align with statewide standards and enterprise capabilities.
- Identify security architectural risks, gaps, and dependencies before they become delivery or operational issues.

### CSS RESPONSIBILITIES

- Provide security architecture consultation and cybersecurity design input.
- Review proposed patterns for alignment with statewide controls and enterprise capabilities.
- Identify gaps, dependencies, and recommended next steps.

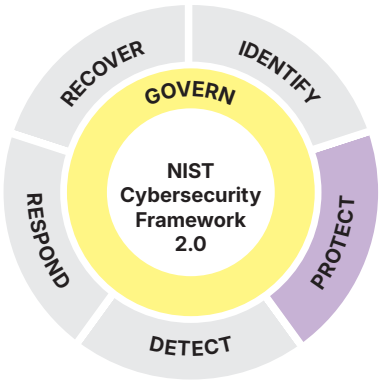
### AGENCY RESPONSIBILITIES

- Bring CSS into the design process early.
- Provide diagrams, data flows, business context, and implementation assumptions.
- Incorporate required controls and follow up on identified gaps.

### SERVICE LEVEL OBJECTIVES

- Target scoping and scheduling follow the tiered service model.
- Review timelines vary based on complexity, documentation readiness, and enterprise workload.

## 4.3.2 Cloud Cybersecurity Consulting




- **Service type:** Requested Service
- **How to engage:** Requested during cloud planning, implementation, review, or remediation work.
- **Related standards:** SA-9, CM-6, RA-5, SI-4, SC-13

### SERVICE DESCRIPTION

CSS advises agencies on cloud cybersecurity architecture, baseline controls, logging, identity dependencies, monitoring expectations, and risk treatment for cloud-hosted systems and services. The service helps agencies align cloud use with statewide control requirements, enterprise cybersecurity expectations, and shared capabilities while clarifying control ownership and required integrations with identity, monitoring, vulnerability management, and incident response processes.

### SERVICE OBJECTIVES

- Improve consistency in cloud cybersecurity control implementation across agencies and environments.
- Reduce common cloud misconfigurations, control gaps, and visibility issues.
- Help agencies understand shared responsibility between cloud providers, agencies, and CSS.
- Improve clarity around required logging, identity, monitoring, and risk treatment expectations for cloud-hosted systems.

### CSS RESPONSIBILITIES

- Review proposed cloud patterns, control expectations, and monitoring needs.
- Advise on identity, logging, cybersecurity architecture, and required enterprise integrations.
- Coordinate with other CSS verticals when monitoring, vulnerability, or incident response services are affected.

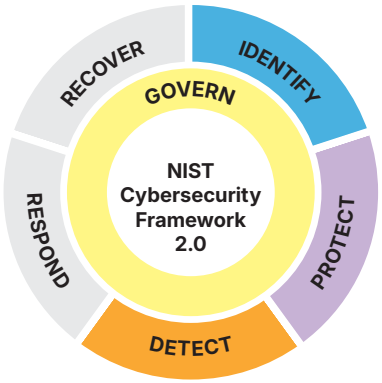
### AGENCY RESPONSIBILITIES

- Provide proposed cybersecurity architecture, hosting model, and operational ownership details.
- Implement agency-owned controls and support enterprise integrations.
- Maintain system documentation, data inventory, and restoration planning for agency-owned services.

### SERVICE LEVEL OBJECTIVES

- Target schedules are established during scoping based on the service tier and complexity.

### 4.3.3 Identity and Access Requirements




- **Service type:** Mandatory Engagement
- **How to engage:** Agencies must involve CSS when identity, access control, or privileged access design materially affects cybersecurity posture or statewide requirements.
- **Related standards:** AC-2, AC-6, IA-2, IA-5, IA-12

#### SERVICE DESCRIPTION

CSS provides statewide identity and access control standards and clarifies the minimum cybersecurity requirements agencies must meet for authentication, authorization, privileged access, and identity proofing. This service gives agencies a path for advisory review today while future managed identity capabilities continue to evolve.

#### SERVICE OBJECTIVES

- Clarify agency responsibility to meet published identity standards.
- Improve consistency for strong authentication, least privilege, and privileged access patterns.
- Identify advisory review needs and future managed capability opportunities where approved.

#### CSS RESPONSIBILITIES

- Provide cybersecurity architectural review and standards interpretation for identity and privileged access topics.
- Document current state requirements and identify future-state managed opportunities where applicable.
- Coordinate with agencies when identity decisions affect enterprise Cyber Security Services or access models.

#### AGENCY RESPONSIBILITIES

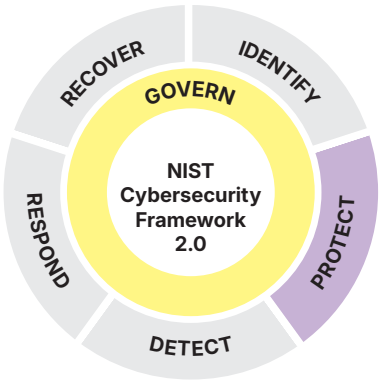
- Comply with published identity and access standards.
- Bring identity and privileged access designs to CSS when cybersecurity review is required.
- Until enterprise-managed identity services are formally established for a given function, agencies remain responsible for implementing and operating identity lifecycle, privileged access governance, and related access controls in accordance with statewide standards.

#### SERVICE LEVEL OBJECTIVES

- Target response and scheduling follow the tiered service model.

# 4.4 NETWORK SECURITY OPERATIONS

## 4.4.1 Firewall




- **Service type:** Mandatory Service
- **How to engage:** Agencies must submit requests through the standard change process and involve CSS for design, rule, or policy changes.
- **Related standards:** SC-5, SC-7, SC-7(5), SC-8, CM-3

### SERVICE DESCRIPTION

CSS designs, reviews, implements, and manages firewall changes for state network perimeter, agency border, and remote-office firewall services that are within CSS scope. The service includes rule review, standards-based configuration guidance, implementation support, testing coordination, and consultation on how firewall policy will be structured to support secure access while limiting unnecessary exposure. It is intended to ensure firewall changes are risk-informed, documented, and implemented consistently across supported environments. The service also helps agencies understand how policy design, segmentation, routing dependencies, and rule lifecycle management affect both cybersecurity posture and operational outcomes.

### SERVICE OBJECTIVES

- Reduce risk through controlled, reviewed, and documented firewall changes.
- Maintain consistent design patterns and deny-by-default control practices.
- Provide practical consultation on rule design, segmentation, and configuration approach.

### CSS RESPONSIBILITIES

- Review requests, analyze cybersecurity impact, and approve or deny changes.
- Implement approved changes and coordinate testing or validation.
- Provide consultation on policy design, standards, and configuration approach.

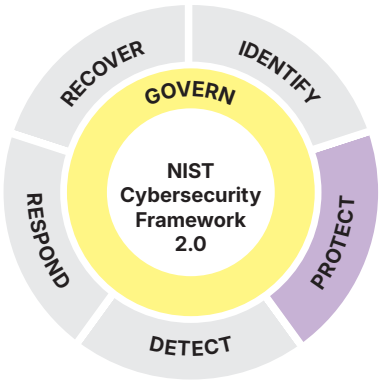
### AGENCY RESPONSIBILITIES

- Obtain agency approval and submit complete requests with business justification.
- Provide the information CSS needs to design and validate the rule set.
- Participate in testing and confirm that implemented access behaves as expected.

### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.2 Load Balancing




- **Service type:** Mandatory Service
- **How to engage:** Requested through standard intake and coordinated with CSS.
- **Related standards:** SC-7, SC-8, CM-3

#### SERVICE DESCRIPTION

CSS provides load-balancing design and change support for covered enterprise services. The service helps distribute traffic, improve application availability, and apply secure front-end patterns consistently across supported environments. It includes review and implementation of configuration changes, support for application delivery design considerations, coordination of testing and validation, and consultation on how traffic management will be structured to support resilience, maintainability, and secure service delivery.

#### SERVICE OBJECTIVES

- Improve application availability and resilience.
- Apply consistent configuration and change control to shared load-balancing services.
- Provide predictable and resilient operational patterns for shared application delivery services.

#### CSS RESPONSIBILITIES

- Review requests, implement approved changes, and coordinate validation.
- Provide implementation guidance for supported cybersecurity architecture, dependencies, and change sequencing.
- Coordinate with adjacent platform or network teams when service dependencies affect delivery.

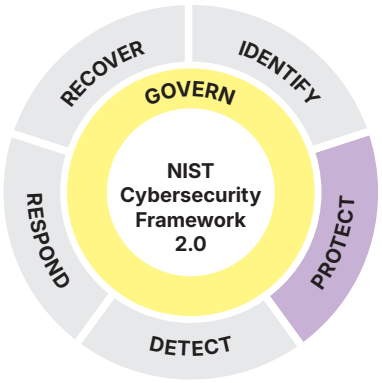
#### AGENCY RESPONSIBILITIES

- Submit the request, provide needed details, and test the resulting configuration.
- Provide application context, expected traffic behavior, and testing contacts.
- Validate the service after implementation and notify CSS of future application changes that affect the configuration.

#### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.3 Secure Sockets Layer (SSL) Termination




- **Service type:** Mandatory Service
- **How to engage:** Requested through standard intake and coordinated with CSS.
- **Related standards:** SC-8, SC-13, CM-3

#### SERVICE DESCRIPTION

CSS provides SSL termination support where covered enterprise designs use centralized cryptographic offload or front-end encryption services. The service helps agencies apply secure transport patterns consistently, reduce operational variation at the edge, and simplify how certificates, encrypted sessions, and front-end traffic handling are managed within supported enterprise architectures. It is intended to support secure application delivery by centralizing approved encryption patterns where appropriate, improving consistency in how inbound encrypted traffic is handled, and helping agencies align with enterprise operational and cybersecurity practices for front-end services.

#### SERVICE OBJECTIVES

- Provide secure, consistent SSL termination and transport patterns for supported services.
- Reduce variation in how external-facing encryption is handled for supported services.

#### CSS RESPONSIBILITIES

- Review, implement, and coordinate validation for approved changes.
- Review certificate, connectivity, and dependency requirements for supported implementations.
- Coordinate implementation sequencing where shared enterprise platforms are involved.

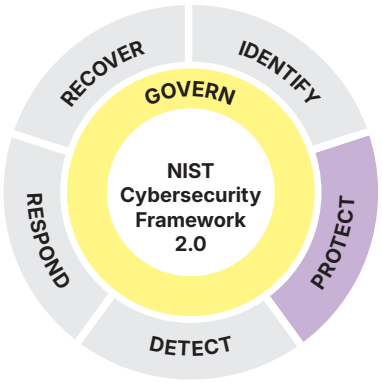
#### AGENCY RESPONSIBILITIES

- Submit the request with accurate application, certificate, cutover, and validation information.
- Validate that application behavior and cybersecurity expectations are met after implementation.

#### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.4 Proxy




- **Service type:** Mandatory Service
- **How to engage:** Agencies must coordinate with CSS for covered proxy designs or changes.
- **Related standards:** SC-7(8), SC-8, CM-3

#### SERVICE DESCRIPTION

Proxy services provide controlled intermediation between users, applications, and external networks where enterprise architecture, cybersecurity requirements, or access patterns call for it. The service reduces direct exposure, improves policy enforcement, and provides a predictable method for handling approved traffic flows between internal users, hosted services, and external destinations.

#### SERVICE OBJECTIVES

- Promote secure traffic routing and inspection patterns where required.
- Reduce design inconsistency, unmanaged exposure, and unnecessary direct internet access.
- Support consistent enterprise mediation patterns for approved use cases.

#### CSS RESPONSIBILITIES

- Review proxy design requests, advise on supported patterns and dependencies, implement approved changes, and coordinate validation.

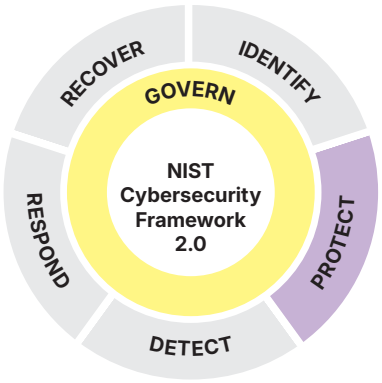
#### AGENCY RESPONSIBILITIES

- Provide business purpose, source and destination patterns, affected systems, traffic patterns, and testing support.
- Describe the business purpose, source and destination patterns, and affected systems.
- Support validation and future updates when application behavior changes.

#### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.5 Secure Sockets Layer Virtual Private Network (SSL VPN)




- **Service type:** Mandatory Service
- **How to engage:** Requested through standard intake with CSS coordination.
- **Related standards:** AC-17, AC-17(2), AC-17(3), SC-8

#### SERVICE DESCRIPTION

CSS supports secure remote access patterns that use encrypted SSL VPN connectivity to provide authorized users with access to state resources from external locations. The service focuses on approved enterprise connectivity patterns, secure authentication, session handling, and reliable operation of remote-access services within CSS scope.

#### SERVICE OBJECTIVES

- Provide secure, centrally governed remote access using approved enterprise patterns.
- Maintain consistent control and review for changes to remote access services.
- Reduce risk associated with inconsistent remote access implementations.

#### CSS RESPONSIBILITIES

- Review requests and access patterns, implement approved changes, and coordinate testing and validation.

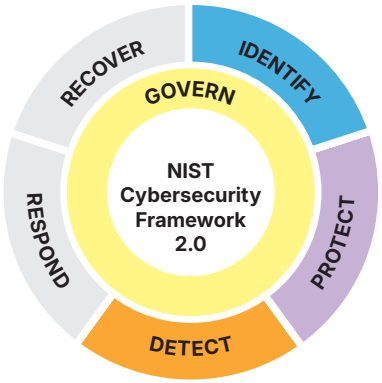
#### AGENCY RESPONSIBILITIES

- Provide user populations, business need, technical details, and validation support.
- Work within approved remote access standards and exception processes.

#### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.6 Internet Protocol Security Virtual Private Network (IPsec)




- **Service type:** Mandatory Service
- **How to engage:** Requested through standard intake with CSS coordination.
- **Related standards:** SC-8, SC-13, AC-17

#### SERVICE DESCRIPTION

CSS provides support for approved site-to-site IPsec connectivity patterns used to securely connect state networks, agency environments, data centers, cloud environments, and other authorized partner networks. The service focuses on strong encryption, controlled change management, and practical coordination with agencies and connected partners to ensure tunnels are secure, supportable, and consistent.

#### SERVICE OBJECTIVES

- Provide secure, supportable site-to-site connectivity using approved patterns and controlled implementation.
- Reduce risk by ensuring encryption, governance, and documented ownership for each connection.

#### CSS RESPONSIBILITIES

- Review requests and peer requirements, implement approved configuration changes, and coordinate cutover validation with connected parties.

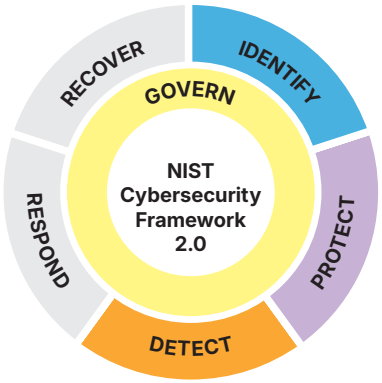
#### AGENCY RESPONSIBILITIES

- Provide peer configuration details, ownership contacts, business justification, and test participation.
- Maintain awareness of connected partner changes that may affect the tunnel.

#### SERVICE LEVEL OBJECTIVES

- Timelines vary based on request completeness, complexity, risk, dependency analysis, and scheduling constraints.
- Target response and scheduling follow the tiered service model.

### 4.4.7 Web Application Firewall (WAF)




- **Service type:** Mandatory Service for High-Value Protections
- **How to engage:** Agencies request onboarding and coordinate validation with CSS.
- **Related standards:** SC-5, SC-7, AU-2, SA-9

#### SERVICE DESCRIPTION

CSS designs, deploys, and maintains web application firewall protections for covered applications. The service is intended to provide a standardized layer of protection for high-value and internet-facing applications by detecting and blocking common web-based attacks, reducing unnecessary exposure, and improving consistency in front-end cybersecurity controls. WAF onboarding begins in monitoring or learning mode so agencies can validate application behavior, identify false positives, and tune rules in coordination with CSS before the service moves into active prevention mode. This approach helps balance strong cybersecurity protections with application stability and gives agencies a controlled path to enforcement.

#### SERVICE OBJECTIVES

- Provide a standardized WAF capability for high-value and internet-facing applications where required.
- Reduce exposure to common web attacks such as Structured Query Language (SQL) injections, cross-site scripting, and automated abuse.
- Balance strong protection with controlled tuning and agency validation.

#### CSS RESPONSIBILITIES

- Review onboarding requests, design the initial policy, and deploy the WAF in monitoring mode first.
- Coordinate tuning, review outcomes with the agency, and move to active prevention once validation is complete.
- Maintain the enterprise WAF service and related platform governance.

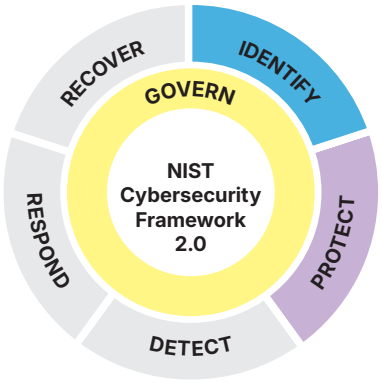
#### AGENCY RESPONSIBILITIES

- Provide application information, expected traffic patterns, and testing support.
- Coordinate cutover windows and validate the tuning outcome.
- Participate in ongoing tuning where application changes affect expected behavior.

#### SERVICE LEVEL OBJECTIVES

- Typical onboarding target: approximately 2 to 4 weeks after scope is confirmed, depending on application complexity and readiness.
- Onboarding and tuning timelines vary based on application architecture, traffic patterns, stakeholder availability, and validation needs.
- Ongoing policy adjustments and support are scheduled based on operational priority, risk, and the nature of the requested change.

## 4.4.8 Enterprise Security Guardrails




- **Service type:** Mandatory Service
- **How to engage:** Provided centrally; agencies engage CSS for interpretation, questions, and collaboration.
- **Related standards:** All statewide cybersecurity policies, plans, and standards as applicable

### SERVICE DESCRIPTION

CSS develops, maintains, and coordinates enterprise security guardrails that help agencies configure cloud environments in alignment with statewide security expectations, approved baselines, and control requirements. Guardrails provide a controlled path from planning to audit, enforcement, and adherence. Existing environments are measured before enforcement, while new cloud environments may begin in enforcement mode to support secure-by-design operations. After enforcement, guardrails prevent non-adherent changes and reduce configuration drift while agencies remediate existing resources.

### SERVICE OBJECTIVES

- Translate standards and approved baselines into practical cloud controls.
- Improve consistency across agency cloud environments.
- Measure configuration gaps before enforcement begins.
- Prevent non-compliant changes once guardrails are enforced.
- Support remediation, deferrals, training, and ongoing adherence.

### CSS RESPONSIBILITIES

- Define, maintain, and update guardrail control sets.
- Build, test, and stage policy-as-code before rollout.
- Communicate timing, impacts, training, and transition expectations.
- Monitor dashboards, adherence, drift, and remediation trends.
- Review and track temporary deferrals when justified.
- Keep temporary deferrals documented, time-bound, and tracked to closure.

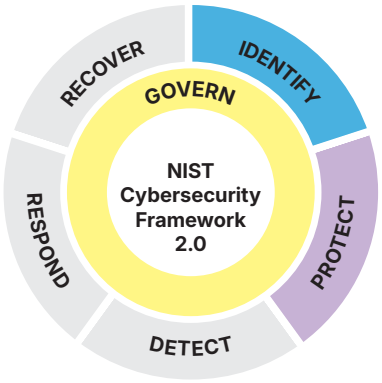
### AGENCY RESPONSIBILITIES

- Review guardrail control sets, training, and dashboard results.
- Assess existing configurations and plan remediation before enforcement.
- Make manual configuration changes or run approved remediation tasks.
- Coordinate with CSS when temporary deferrals are needed.
- Maintain adherence after enforcement and address drift over time.

### SERVICE LEVEL OBJECTIVES

- Onboarding or major changes are scheduled through the tiered service model.
- Provide advance communication before new or updated guardrails enter audit mode.
- Use audit mode for existing subscriptions before scheduled enforcement when practical.
- Coordinate transition to enforcement after review, remediation, and owner engagement.

# 4.5 SECURITY OPERATIONS CENTER SERVICES




## 4.5.1 Cybersecurity Assessment

- **Service type:** Mandatory Service
- **How to engage:** CSS schedules and coordinates the enterprise assessment program with each covered agency.
- **Related standards:** CA-2, CA-7, CA-5, CM-6, RA-5

### SERVICE DESCRIPTION

CSS conducts cybersecurity assessments to evaluate the fundamental security posture of executive department agencies, boards, and commissions. These assessments are intended to provide a structured view of how well an agency is positioned to manage cybersecurity risk, meet statewide expectations, and sustain core cybersecurity practices over time. Assessments identify strengths, weaknesses, and prioritized recommendations, and they can include validation of required plans, governance practices, operational processes, and baseline hardening expectations such as CIS benchmark alignment. CSS may scale assessment depth or level based on agency complexity, risk, mission criticality, and the maturity of the environment being reviewed.

### SERVICE OBJECTIVES

- Identify critical gaps and priority improvements that will materially improve posture.
- Track aggregate findings so enterprise services can be improved over time.
- Validate the presence and quality of key agency plans, including incident response planning.
- Monitor year-over-year posture improvement where scoring or maturity measures are available.

### CSS RESPONSIBILITIES

- Lead assessment planning, interviews, technical validation, and reporting.
- Coordinate with agency staff on rules of engagement and required artifacts.
- Provide prioritized recommendations and support follow-up improvement planning.

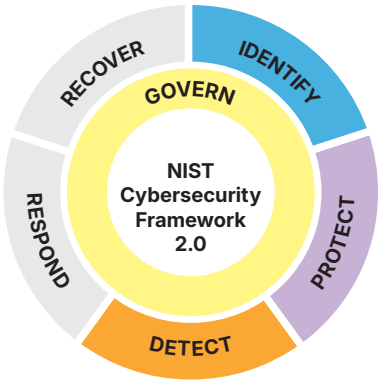
### AGENCY RESPONSIBILITIES

- Provide an executive sponsor, single point of contact, requested artifacts, and staff participation.
- Support technical validation and provide access as agreed.
- Use assessment results to drive remediation and posture improvement.
- Coordinate agency leadership entrance and exit meetings.

### SERVICE LEVEL OBJECTIVES

- Typical end-to-end assessment target: up to 90 days, depending on scope, complexity, and agency readiness.

## 4.5.2 Penetration Testing




- **Service type:** Mandatory Engagement
- **How to engage:** Agencies must coordinate penetration testing through CSS whether the effort is agency-initiated or coordinated by another party.
- **Related standards:** CA-8, CA-8(1), CA-8(2)

### SERVICE DESCRIPTION

Penetration testing evaluates how well security controls withstand targeted attack methods in practice. Unlike assessments or design reviews, this service is intended to test whether real-world exploitation is possible against agreed scope and objectives. CSS coordinates the engagement, helps define rules of engagement, and makes sure results are shared back into the statewide cybersecurity program so validated findings can inform both agency remediation and broader enterprise risk awareness. The service helps agencies understand exploitable risk, likely business impact, and where technical or procedural controls may not perform as intended under realistic attack conditions. It also supports situations where penetration testing is needed to satisfy regulatory, contractual, audit, or high-risk deployment expectations.

### SERVICE OBJECTIVES

- Help agencies understand exploitable risk and business impact.
- Test whether controls work in practice, not just on paper.
- Support regulatory or contractual penetration-testing requirements while maintaining enterprise awareness.

### CSS RESPONSIBILITIES

- Coordinate the engagement and ensure enterprise awareness of scope and results.
- Help establish rules of engagement, scheduling assumptions, and enterprise coordination needs.
- Capture results and themes that will inform broader statewide risk management where appropriate.

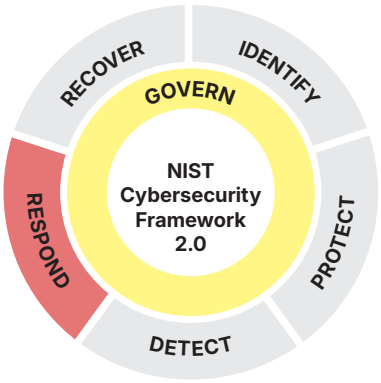
### AGENCY RESPONSIBILITIES

- Request or coordinate the engagement through CSS.
- Provide scope, approvals, contacts, and required participation.
- Share final results with CSS, track remediation, and report status where requested.

### SERVICE LEVEL OBJECTIVES

- Initial coordination target: within 2 weeks after complete intake information is received.
- Execution timing depends on tester availability, scope, and readiness of the target environment.

### 4.5.3 External Vulnerability Scanning and Validation Testing




- **Service type:** Mandatory Engagement
- **How to engage:** Requested through standard intake and coordinated with CSS.
- **Related standards:** RA-5, CA-2, SI-2

#### SERVICE DESCRIPTION

This service scans targeted internet-accessible systems for known vulnerabilities and weak configurations and then validates findings to distinguish true positives from false positives. It is intended for focused assessment work where agencies need deeper validation than standard recurring scanning alone, particularly when a system is high-value, internet-facing, newly deployed, materially changed, or of specific concern. The service helps agencies understand how externally exposed systems may appear to likely attackers, identify weaknesses that are actionable, and prioritize remediation based on validated risk rather than raw scan output alone.

#### SERVICE OBJECTIVES

- Show agencies how exposed systems appear to likely attackers.
- Validate findings so remediation is focused on confirmed, actionable risk rather than false positives or noise.
- Support remediation and retesting of externally visible weaknesses.
- Identify high-priority vulnerabilities and weak configurations affecting public-facing systems.

#### CSS RESPONSIBILITIES

- Coordinate the engagement and execute or oversee focused external scanning and validation work.
- Define scope, timing, and approach in coordination with the agency and any supporting parties.
- Validate identified findings to distinguish confirmed issues from false positives, duplicate results, or conditions that are not exploitable as reported.

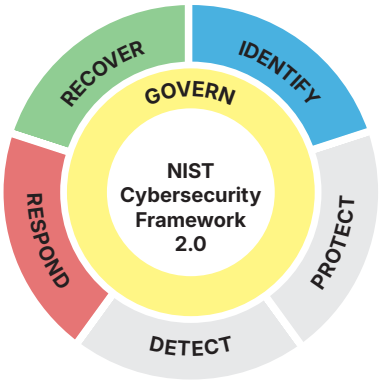
#### AGENCY RESPONSIBILITIES

- Provide scope, technical contacts, and rules of engagement.
- Remediate confirmed vulnerabilities and share final reporting back to CSS as needed.
- Support clarification of findings, technical questions, and validation activities as needed during the engagement.

#### SERVICE LEVEL OBJECTIVES

- Start and completion targets are defined during scoping based on size and complexity.
- Timelines vary based on the number of systems in scope, the depth of validation required, and agency responsiveness during the engagement.

### 4.5.4 Agency Incident Response Plan Creation Assistance




- **Service type:** Required Agency Capability with CSS Support
- **How to engage:** Agencies request CSS assistance through standard intake; agency ownership of the final plan remains required.
- **Related standards:** IR-3, IR-6, IR-8, CP-2

#### SERVICE DESCRIPTION

Each agency is expected to maintain an agency-specific incident response plan. CSS provides templates, consultation, and review support so agencies can document how they will identify, escalate, coordinate, communicate, and manage cybersecurity incidents within their own environment while aligning to the statewide response structure. The service helps agencies establish a practical and repeatable framework for incident handling that reflects agency-specific roles, systems, dependencies, and decision-making needs.

#### SERVICE OBJECTIVES

- Help every agency maintain a practical, current, and usable incident response plan with consistent structure and agency-specific roles, workflows, and escalation paths.
- Make sure the plan identifies where CSS support is expected and where agency ownership remains.
- Improve readiness to detect, escalate, coordinate, communicate, and manage cybersecurity incidents.

#### CSS RESPONSIBILITIES

- Provide the baseline template and consultation.
- Assist agencies in tailoring the plan to their environment.
- Review the resulting plan and maintain awareness of agency plan status.

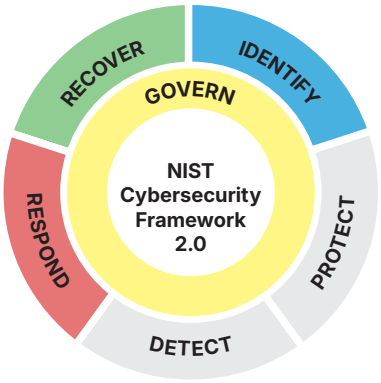
#### AGENCY RESPONSIBILITIES

- Own, approve, submit, and maintain the final agency plan.
- Define agency-specific roles, decision authorities, communications paths, and operational procedures needed to support response.
- Use the plan in tabletop exercises, preparedness activities, and actual incidents.

#### SERVICE LEVEL OBJECTIVES

- Typical plan-assistance target: initial support within 14 calendar days after intake.
- Review and consultation timelines vary based on plan maturity, agency complexity, and enterprise workload.
- Follow-up discussions, revisions, and target dates are established during scoping based on readiness and identified gaps.

### 4.5.5 Incident Response Coordination and Management




- **Service type:** Mandatory Service
- **How to engage:** Engaged for suspected or confirmed incidents and may be initiated by CSS or requested by the agency.
- **Related standards:** IR-4, IR-5, IR-6, IR-7

#### SERVICE DESCRIPTION

CSS provides enterprise-level coordination and management for cybersecurity incidents. CSS will lead or coordinate response based on incident scope, severity, and enterprise impact, including active compromise, high-impact operational disruption, confirmed or suspected malicious activity, and larger-scale incidents requiring multi-team response. When CSS Cyber Command is activated, it serves as the lead coordinating authority for enterprise response priorities, resource coordination, agency alignment, communications support, and recovery coordination. The Cyber Command structure is intended to reduce confusion during fast-moving incidents by clarifying roles, directing activities, and establishing escalation paths and response expectations. Agencies remain responsible for agency-owned operational and business decisions while coordinating those decisions through the Cyber Command framework and leadership.

#### SERVICE OBJECTIVES

- Coordinate timely, effective, and unified cyber incident response and direction from a central command.
- Provide a clear Cyber Command structure for escalation and coordination.
- Establish a clear Cyber Command structure that reduces confusion and provides agencies with a defined escalation and coordination path during high-stress events.
- Support technical investigation, operational decision-making, communications coordination, and post-incident improvement activities.
- Ensure enterprise resources, subject matter experts, and external partners are effectively mobilized to support incident response and recovery efforts.

#### CSS RESPONSIBILITIES

- Stand up a Cyber Command team to lead and coordinate incident response based on scope, severity, and impact.
- Activate and manage state Cyber Command resources when required.
- Coordinate enterprise resources, vendors, partners, notifications, briefings, and after-action reviews as appropriate.
- Manage defensive and recovery activities and direct tasks across all dedicated resources.

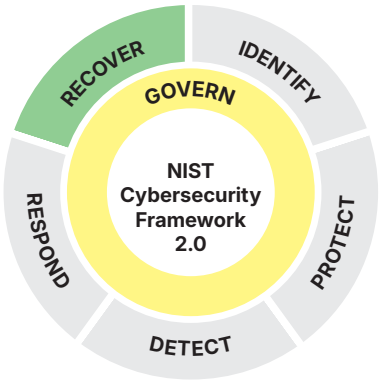
#### AGENCY RESPONSIBILITIES

- Notify CSS of suspected or confirmed cyber incidents according to state incident response plan requirements.
- Provide leadership, technical contacts, decision-makers, system access, and complete tasks assigned by the Cyber Command on a timely basis.
- Participate in Cyber Command activities and carry out agency-owned containment, recovery, and business decisions effectively as directed by the Cyber Command.

#### SERVICE LEVEL OBJECTIVES

- Target response and scheduling follow the tiered service model.

## 4.5.6 Coordination of Tabletop Exercises




- **Service type:** Mandatory Engagement
- **How to engage:** CSS coordinates with agencies on tabletop planning, scheduling, and facilitation.
- **Related standards:** IR-3, IR-3(2), CP-4

### SERVICE DESCRIPTION

CSS coordinates tabletop exercises to test agency response plans, communications, decision-making, and escalation paths. Tabletop participation is expected for executive department agencies as part of maintaining readiness and validating that documented plans can be used during an incident. These exercises are intended to help agencies practice how they would respond to realistic cybersecurity scenarios, clarify roles and decision authorities, identify gaps in plans or coordination, and strengthen familiarity with statewide escalation and support processes before a real event occurs.

### SERVICE OBJECTIVES

- Keep agency teams familiar with their roles and escalation paths.
- Validate incident response plans and identify needed updates.
- Strengthen enterprise coordination and agency decision-making before a real event occurs.
- Identify procedural, organizational, or coordination gaps that should be addressed through planning or follow-up actions.

### CSS RESPONSIBILITIES

- Coordinate planning, scheduling, facilitation, and follow-up.
- Work with agencies to define exercise scope, objectives, scenario assumptions, and participant needs.
- Develop or tailor exercise scenarios that reflect agency risk, mission, dependencies, and likely incident conditions.
- Help agencies turn exercise findings into plan or process improvements.

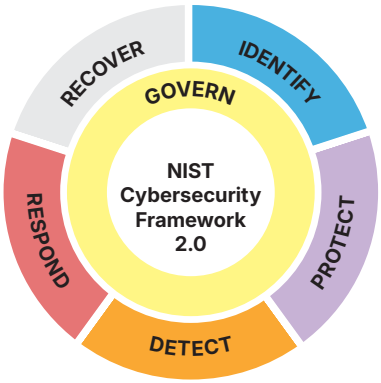
### AGENCY RESPONSIBILITIES

- Participate with the right business and technical stakeholders.
- Use exercise results to update plans, contacts, and procedures.
- Coordinate periodic exercises with CSS and track follow-up actions.

### SERVICE LEVEL OBJECTIVES

- Tabletop planning and execution are coordinated on an annual or otherwise agreed schedule.
- Scheduling, scenario development, and follow-up timing vary based on agency readiness, complexity, and enterprise workload.
- After-action discussions, observations, and improvement follow-up are provided after the exercise based on scope and outcomes.

## 4.5.7 Recovery and Restoration Support




- **Service type:** Requested Service
- **How to engage:** Triggered during significant cyber incidents where enterprise-managed infrastructure, shared platforms, or coordinated restoration support are required.
- **Related standards:** CP-2, CP-7, CP-9, CP-10, IR-4

### SERVICE DESCRIPTION

CSS may provide hands-on or coordinated recovery support during a major cyber incident, especially where enterprise-managed infrastructure, shared cybersecurity platforms, or cross-agency restoration needs are involved. Agencies continue to own their applications, business restoration decisions, data, backups, and recovery priorities unless a managed service explicitly says otherwise. CSS support may include coordination, technical guidance, enterprise service restoration, and assistance in evaluating whether conditions are appropriate to bring systems back online.

### SERVICE OBJECTIVES

- Support safe and coordinated restoration of services after a major cyber incident.
- Clarify where CSS can directly assist and where agency ownership remains.
- Reduce recovery confusion by connecting incident response, contingency planning, and practical restoration work.

### CSS RESPONSIBILITIES

- Coordinate recovery support for enterprise-managed cybersecurity and infrastructure elements within CSS scope.
- Help agencies align restoration sequence with cybersecurity conditions and lessons learned.
- Provide consultation on recovery dependencies, restoration risk, and readiness gaps identified during an event.

### AGENCY RESPONSIBILITIES

- Maintain application inventories, backup strategies, immutable backups where applicable, and restoration procedures.
- Own agency business restoration decisions and testing for agency-managed systems.
- Work with CSS during a major incident to sequence safe restoration activities.

### SERVICE LEVEL OBJECTIVES

- Response and support timing depend on incident severity, enterprise impact, and the scope of CSS-managed technology involved.

## 4.5.8 Cyber Threat Intelligence Collection


- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agency consumption and follow-up where applicable.
- **Related standards:** SI-4, SI-5

### SERVICE DESCRIPTION

CSS collects threat intelligence from commercial, open-source, government, and partner sources and uses that information to enrich cybersecurity monitoring, correlation, analysis, and notifications across the statewide cybersecurity program. The service is intended to help agencies receive timely, actionable information rather than raw threat data by translating external intelligence into practical awareness, detection context, and response value. This includes identifying relevant indicators, tactics, trends, and emerging threats that may affect state systems, services, users, or agency operations.

### SERVICE OBJECTIVES

- Maintain a current picture of relevant threat activity.
- Improve enterprise detection and response through correlated intelligence.
- Provide actionable notifications, including Common Vulnerabilities and Exposures (CVE) and recommended next steps, when agency action is needed.

### CSS RESPONSIBILITIES

- Collect, qualify, correlate, and use threat data within enterprise monitoring and response processes.
- Notify agencies with actionable detail when threat information materially affects them or requires action.

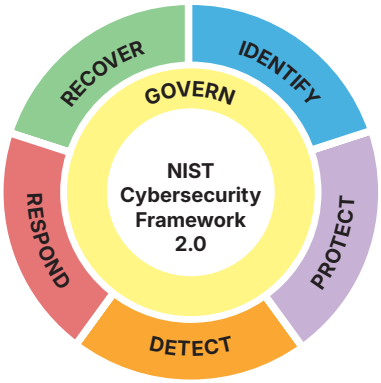
### AGENCY RESPONSIBILITIES

- Review notifications, route them to the right operational owners, and act on agency-owned remediation or follow-up tasks.
- Coordinate with CSS when additional context or agency-side action is needed.

### SERVICE LEVEL OBJECTIVES

- Threat intelligence is integrated continuously; agency notifications are prioritized by urgency, exploitability, relevance, and enterprise impact.

### 4.5.9 Cybersecurity Event Log Collection and Retention




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally by CSS for logs within CSS scope; agency coordination required for onboarding and use.
- **Related standards:** AU-2, AU-6, AU-11, AU-12, SI-4

#### SERVICE DESCRIPTION

CSS collects and retains enterprise security event logs for covered platforms and services. This includes cybersecurity logs that support detection, response, investigation, compliance, and enterprise visibility across shared cybersecurity capabilities and CSS-managed technologies. The service is intended to provide a usable source of cybersecurity-relevant event data so CSS can monitor activity, investigate incidents, correlate events across systems, and maintain broader situational awareness of enterprise risk. It also helps agencies understand the distinction between enterprise cybersecurity logging and application- or business-system-specific logging that remains under agency ownership unless a managed service explicitly includes it.

#### SERVICE OBJECTIVES

- Maintain reliable cybersecurity logs for investigations, detection, response, threat analysis, and enterprise visibility.
- Clarify the boundary between enterprise cybersecurity logs and agency application logs.

#### CSS RESPONSIBILITIES

- Operate the infrastructure used to ingest, retain, and manage covered cybersecurity logs.
- Monitor log health and availability within CSS scope.
- Support use of retained cybersecurity logs for investigations and analysis.

#### AGENCY RESPONSIBILITIES

- Maintain application and business-system logs that are outside CSS-managed scope.
- Provide context when log interpretation requires agency knowledge.
- Coordinate onboarding information and operational changes that affect log sources.

#### SERVICE LEVEL OBJECTIVES

- Onboarding or major changes are scheduled through the tiered service model.
- Timing varies based on source complexity, readiness, dependency coordination, and enterprise workload.
- Target response and scheduling follow the tiered service model.

## 4.5.10 Security Information and Event Management (SIEM) and Security Orchestration


- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally; agencies provide routing, context, and follow-up support.
- **Related standards:** AU-6, AU-7, SI-4, SI-5

### SERVICE DESCRIPTION

CSS operates the enterprise SIEM and related orchestration capabilities to monitor cybersecurity events, analyze alerts, enrich detections, and support response workflows. This is the core enterprise platform used to bring together cybersecurity telemetry from multiple sources and turn it into actionable cybersecurity operations. The service is intended to improve statewide visibility by centralizing covered cybersecurity event data, correlating activity across systems and services, and applying detection logic that helps identify suspicious, malicious, or policy-relevant behavior. It also supports operational response by providing analysts with the context, enrichment, and workflow tooling needed to investigate alerts, prioritize risk, and coordinate follow-up with agencies and other CSS functions.

### SERVICE OBJECTIVES

- Detect cybersecurity events quickly and consistently across covered services.
- Correlate data from multiple sources so analysts can prioritize real risk.
- Support investigations and response with actionable event context.
- Improve enterprise visibility into suspicious activity, control failures, and emerging threats.
- Enable more efficient cybersecurity operations through centralized monitoring, enrichment, and workflow support.

### CSS RESPONSIBILITIES

- Operate the SIEM and related cybersecurity orchestration processes.
- Incorporate new threat intelligence and detection logic into the platform.
- Notify agencies of events that require agency awareness or action.

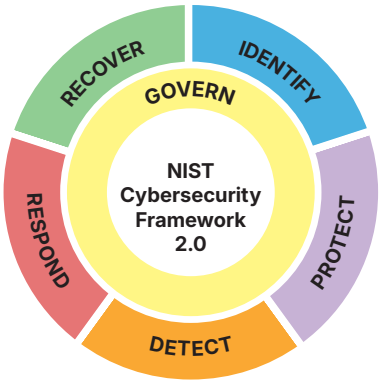
### AGENCY RESPONSIBILITIES

- Provide distribution lists, contacts, and requested environment context.
- Respond to agency-specific alerts and support investigation or remediation as needed.

### SERVICE LEVEL OBJECTIVES

- Potential threats detected by the enterprise platform are generally routed or escalated within 24 hours based on severity.
- New threat intelligence is typically incorporated into the SIEM within 24 hours when operationally appropriate.
- Response timing for specific alerts varies based on severity, confidence, operational priority, and the need for additional analysis or agency context.

## 4.5.11 Network Cybersecurity Monitoring and Analysis




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agency follow-up where alerts require action.
- **Related standards:** SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(16), SI-4(18), SI-4(23)

### SERVICE DESCRIPTION

CSS continuously monitors covered network, identity, cloud, and Software as a Service (SaaS)-related telemetry to identify suspicious behavior, attacker tactics, and indicators of compromise across supported environments. The service combines platform analytics, threat intelligence, correlation logic, and analyst review to prioritize events and generate actionable alerts rather than raw technical data. It is intended to improve enterprise visibility into malicious or potentially harmful activity by detecting patterns that may indicate account compromise, unauthorized access, lateral movement, misuse of cloud services, suspicious network activity, or other signs of cyber risk. The service also helps agencies understand when observed activity may require investigation, containment, remediation, or additional coordination with CSS.

### SERVICE OBJECTIVES

- Detect malicious or suspicious activity and potential compromise across covered attack surfaces.
- Provide agencies with alerts that are prioritized and actionable rather than raw telemetry.
- Improve enterprise awareness of attacker behavior and emerging risk.
- Strengthen statewide detection capability through centralized monitoring and analyst-driven review.

### CSS RESPONSIBILITIES

- Operate and tune the monitoring platform.
- Triage alerts, enrich findings, and coordinate event tracking.
- Notify agencies when remediation or investigation is needed.

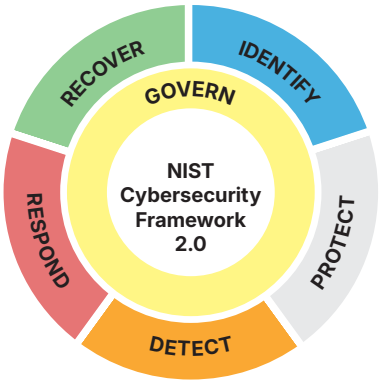
### AGENCY RESPONSIBILITIES

- Respond promptly to alerts and provide status updates when requested.
- Maintain accurate records of agency IP space, boundaries, and major environment changes that affect monitoring coverage.

### SERVICE LEVEL OBJECTIVES

- Alerts are generally forwarded to agencies within 24 hours during normal business operations unless urgency requires faster escalation.
- Agency updates and inquiries are normally answered within 24 hours during standard business operations.
- Escalation timing may be faster for higher-severity events, suspected compromise, or activity requiring immediate coordination.

## 4.5.12 Phishing Email Analysis




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally through the state phishing reporting workflow.
- **Related standards:** SI-4, SI-8, IR-6

### SERVICE DESCRIPTION

CSS reviews suspicious emails reported by users through the approved reporting process. The service helps determine whether reported messages are phishing, spam, benign, or part of a broader malicious campaign, and it supports statewide metrics, awareness, and follow-up action. It is intended to give the workforce a clear and consistent path for escalating questionable messages so potential phishing activity can be reviewed quickly and patterns can be identified across agencies. In addition to classifying individual reports, the service helps CSS detect coordinated campaigns, reduce the time between user reporting and response, and improve enterprise understanding of phishing-related risk trends over time.

### SERVICE OBJECTIVES

- Give the workforce an easy, consistent way to report suspicious emails and help identify broader phishing campaigns.
- Reduce response time for likely phishing events.
- Improve metrics, trend visibility, awareness, and response capabilities related to phishing risk.

### CSS RESPONSIBILITIES

- Review, classify, and take appropriate follow-up action on reported emails, including broader coordination when campaigns are detected.
- Track results to support enterprise metrics and awareness improvements.

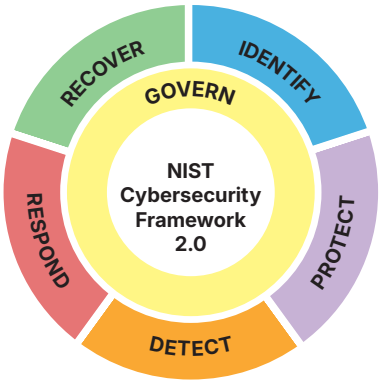
### AGENCY RESPONSIBILITIES

- Promote the approved phishing reporting process and encourage users to report suspicious messages promptly.
- Use CSS awareness materials to support local training where needed.
- Support local communication when agency-specific follow-up is needed.

### SERVICE LEVEL OBJECTIVES

- Report mailboxes are reviewed daily.
- Follow-up actions or ticket creation occur on the same day when requested and appropriate.
- Trend reporting is typically produced on a weekly or monthly cadence, depending on the metrics available to agencies.

## 4.5.13 Domain Name System (DNS) Filtering - Malicious Domain Blocking and Reporting (MDBR)




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agencies reporting exceptions or unblock requests.
- **Related standards:** SC-7, SI-4, SI-5

### SERVICE DESCRIPTION

DNS filtering blocks known malicious, suspicious, or high-risk domains to reduce exposure to malware, phishing, ransomware, command-and-control activity, and other common internet-based threats. The service adds preventive value before a connection is established by stopping many unsafe destinations at the DNS layer, helping reduce risk across participating environments with minimal operational friction. It also provides reporting and visibility that support awareness, tuning, and follow-up when blocked activity may indicate user risk, malicious activity, or a business need that requires review.

### SERVICE OBJECTIVES

- Reduce exposure by blocking known bad destinations, malware, phishing, ransomware, and command-and-control activity before connections are completed.
- Improve visibility into blocked destination trends that may inform awareness, investigation, or tuning.
- Support more consistent protective DNS controls across participating agencies and services.

### CSS RESPONSIBILITIES

- Manage the enterprise relationship and operational coordination for the service.
- Review blocked-site issues and work through appropriate changes or exceptions.
- Maintain awareness of blocked-domain trends, service health, and broader risk patterns that may warrant additional action.

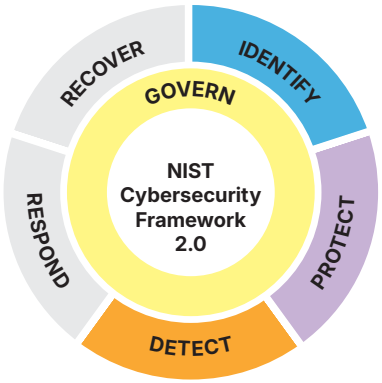
### AGENCY RESPONSIBILITIES

- Report suspected false positives or business-impacting blocks to CSS for review.
- Provide business context, testing support, and technical contacts when blocked destinations require investigation or exception review.
- Notify CSS of major architecture or service changes that may affect DNS filtering coverage or behavior.

### SERVICE LEVEL OBJECTIVES

- Typical onboarding target: 7 calendar days.
- Requests to review blocked sites are generally triaged on the same day.
- Resolution timing for blocked-site reviews depends on the complexity of the request, business impact, and whether additional validation or coordination is required.

## 4.5.14 Agency Vulnerability Management Plan Creation Assistance




- **Service type:** Required Agency Capability with CSS Support
- **How to engage:** Agencies request assistance, but agencies are expected to maintain a documented plan.
- **Related standards:** RA-5, CA-5, SI-2

### SERVICE DESCRIPTION

CSS helps agencies create and maintain a documented vulnerability management plan that defines how scanning, triage, remediation, validation, risk acceptance, escalation, and reporting will work at the agency level. The plan gives agencies a durable operating model rather than treating vulnerability management as an ad hoc activity. It is intended to help agencies establish clear roles, decision points, timelines, and accountability for identifying and reducing vulnerabilities across systems and services in their environment. The service also helps agencies align local vulnerability management practices with statewide expectations, available CSS services, and risk-based remediation approaches so that findings are handled consistently and improvements can be sustained over time.

### SERVICE OBJECTIVES

- Help agencies maintain a documented vulnerability management process.
- Create consistency in how agencies triage, remediate, and track vulnerabilities.
- Provide a practical template that agencies can adapt to their environment.
- Clarify roles, ownership, escalation paths, and decision criteria for vulnerability-related work.

### CSS RESPONSIBILITIES

- Provide the base template and advisory support.
- Review completed plans and connect agencies to related scanning, validation, advisory, or enterprise coordination services where needed.

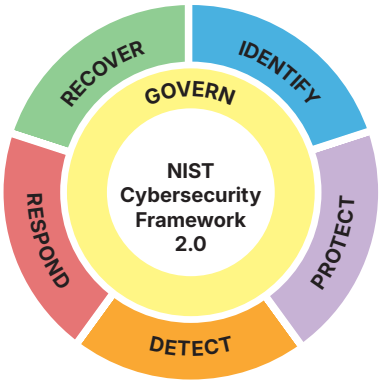
### AGENCY RESPONSIBILITIES

- Own, tailor, approve, and maintain the final agency plan.
- Use the plan to guide remediation, escalation, and reporting.
- Document risk acceptance, exceptions, and compensating controls when remediation cannot be completed as expected.

### SERVICE LEVEL OBJECTIVES

- Typical plan-assistance target: initial support within 14 calendar days after intake.
- Review and consultation timelines vary based on plan maturity, agency complexity, and enterprise workload.
- Follow-up discussions, revisions, and target dates are established during scoping based on readiness and identified gaps.

## 4.5.15 Internal Vulnerability Management Scanning




- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agency onboarding, scheduling, and remediation support.
- **Related standards:** RA-5, RA-5(2), RA-5(3), RA-5(5), SI-2

### SERVICE DESCRIPTION

CSS provides vulnerability scanning for covered internal assets and correlated visibility across servers, workstations, cloud resources, network-connected devices, and other reachable systems within scope. The service helps agencies identify vulnerabilities, misconfigurations, missing patches, and broader exposure patterns so they can prioritize remediation based on risk rather than isolated findings alone. By combining scanning data across covered environments, the service supports more consistent enterprise visibility into internal cybersecurity conditions and helps agencies understand where weaknesses may affect critical systems, sensitive data, or broader operational resilience.

### SERVICE OBJECTIVES

- Identify vulnerabilities and misconfigurations across covered environments.
- Provide consistent enterprise visibility and risk-based prioritization.
- Support agency remediation, reporting, and trend analysis.
- Improve awareness of critical weaknesses that could materially increase agency or enterprise risk.

### CSS RESPONSIBILITIES

- Operate scanning infrastructure and analytics within service scope.
- Provide agencies with access to data, dashboards, and reporting where available.
- Highlight critical or time-sensitive vulnerabilities for action.

### AGENCY RESPONSIBILITIES

- Provide technical contacts, asset scope, and scanning prerequisites.
- Review and remediate vulnerabilities according to statewide standards and risk.
- Notify CSS of major infrastructure changes that affect scanning coverage.

### SERVICE LEVEL OBJECTIVES

- Routine vulnerability reports are generally available within 5 business days after scheduled scan completion.
- Agencies are directly notified of critical, high-risk, or actively exploited issues requiring urgent attention.
- Reporting and notification timing may vary based on scan scope, validation needs, system availability, and enterprise workload.

## 4.5.16 External Vulnerability Management Scanning

- **Service type:** Mandatory Service
- **How to engage:** Delivered centrally with agency coordination of IP space and reporting contacts.
- **Related standards:** RA-5, SI-2

### SERVICE DESCRIPTION

CSS coordinates recurring external vulnerability scanning of state internet-accessible assets to show how public-facing systems appear to external observers and to help agencies reduce exposed weaknesses over time. The service provides a recurring external view of the state's public attack surface by identifying vulnerabilities, weak configurations, exposed services, and other issues that may be visible from the internet. It is intended to help agencies understand and reduce externally observable risk before weaknesses are exploited, while also giving CSS broader visibility into statewide exposure trends. The service supports ongoing risk reduction by providing repeatable scanning, regular reporting, and a common process for tracking externally visible issues across participating agencies.

### SERVICE OBJECTIVES

- Maintain recurring visibility into the state's public attack surface, including public-facing vulnerabilities and weak configurations.
- Drive timely remediation of externally visible weaknesses before they become incidents.

### CSS RESPONSIBILITIES

- Coordinate statewide external scan scheduling, coverage, and delivery of findings to the appropriate agency contacts.
- Ensure known public IP space is included in the scanning process.
- Maintain enterprise awareness of broad external exposure trends.

### AGENCY RESPONSIBILITIES

- Provide current internet-routable IP address information and maintain current report distribution lists.
- Review findings and remediate issues based on risk and required timelines.

### SERVICE LEVEL OBJECTIVES

- Typical onboarding target: 30 calendar days.
- Timing for onboarding and reporting may vary based on scope, asset readiness, completeness of submitted information, and enterprise workload.
- Recurring report delivery follows the established program cadence after onboarding is complete.

# 5. Appendices

## 5.1 APPENDIX A - COORDINATED EXTERNAL PARTNER SERVICES

Some cybersecurity capabilities used by agencies are delivered by external partners or government programs and are coordinated through CSS rather than operated directly by CSS. Examples may include federal or multi-state Cyber Security Services, partner-provided intelligence feeds, and specialized assessment or emergency response support.

CSS may help agencies evaluate, onboard, or coordinate these services where they support statewide objectives. Their inclusion here does not mean they are fully operated by CSS or that they replace agency responsibilities.

- CSS will identify when an external partner service is the best fit for the agency's need.
- Service eligibility, scope, and timelines may depend on the external provider.
- Agencies may still need to provide contacts, scope, approvals, and follow-up actions.

## 5.2 APPENDIX B – CYBER SECURITY SERVICES RACI MATRIX

For purposes of this matrix, the **CSS** column includes Cyber Security Services leadership, enterprise cybersecurity governance, and State CISO decision authority where applicable.

### Responsibility Notes

This matrix does not transfer ownership of agency systems, applications, data, or business processes to CSS. CSS is accountable for the enterprise Cyber Security Services it operates, manages, or coordinates. Agencies remain accountable for agency-owned systems, applications, data, business processes, remediation decisions, backup strategies, restoration procedures, and compliance activities unless otherwise documented through an approved enterprise service model.

Where a cybersecurity service is mandatory or enterprise-managed, agencies are expected to participate in onboarding, follow established standards, provide required system and business context, maintain appropriate agency documentation, and support remediation or follow-up actions.

**RACI Key:**
**R** = Responsible for performing or supporting the work
**A** = Accountable for the outcome, decision, or service
**C** = Consulted before or during the work
**I** = Informed of status, outcomes, or changes

| CSS Vertical | Catalog Service | Service Type | CSS | Agency | State CISO / EIS Leadership | DAS / EIS Communications | Governor's Office | Legislature | Procurement/ Legal/ Oversight | External Partners/ Vendors/Federal Partners |
|---|---|---|---|---|---|---|---|---|---|---|
| **Overarching Services** | Enterprise Cybersecurity Consulting and Secure-By-Design Advisory | Requested Service | R | A | I* | | | | | C* |
| **Governance and Risk Management** | Business Security Enablement and Advisory | Requested Service | R | A | I* | | | | | |
| | System Cybersecurity Evaluation | Mandatory Engagement | R | A | I* | | | | C | C* |
| | Vendor Cybersecurity Evaluation and Advisory | Mandatory Engagement | R | A | I* | | | | C | C |
| | Cybersecurity Awareness and Training | Mandatory Service | A | R | I | C* | | | | C* |
| | Phishing Campaigns | Mandatory Service | A | R | I | C* | | | | C* |
| | Cybersecurity Awareness Month | Mandatory Service with Agency Participation | A | R | I | C | | | | C* |
| | Policy and Standards | Mandatory Service | A | R | C | I* | I* | I* | C | |
| **Solutions Architecture and Identity Services** | Cybersecurity Architecture and Secure-By-Design Consulting | Requested Service | R | A | I* | | | | | C* |
| | Cloud Cybersecurity Consulting | Requested Service | R | A | I* | | | | | C* |
| | Identity and Access Requirements | Mandatory Engagement | R | A | I* | | | | | C* |
| **Network Security Operations** | Firewall Services | Mandatory Service | A | R | I* | | | | | C* |
| | Load Balancing Services | Mandatory Service | A | R | I* | | | | | C* |
| | SSL Termination Services | Mandatory Service | A | R | I* | | | | | C* |
| | Proxy Services | Mandatory Service | A | R | I* | | | | | C* |
| | SSL VPN Services | Mandatory Service | A | R | I* | | | | | C* |
| | IPsec VPN Services | Mandatory Service | A | R | I* | | | | | C |
| | Web Application Firewall Services | Mandatory Service for High-Value Protections | A | R | I* | | | | | C* |
| | Enterprise Security Guardrails | Mandatory Service | A | R | C | I* | | | | C* |


# ENTERPRISE
information services