State of Oregon

Cyber Security Services

Service Catalog

2022

ENTERPRISE
information services

TARGET
TARGET
TARGET
TARGET

TABLE OF CONTENTS

Introduction.......... 2

About this Service Catalog 2

Format of Service Descriptions 2

Icons 2

Requesting Services 2

Overarching Services 2

Vulnerability Management 3

Agency Vulnerability Management Plan Creation Assistance 3

Internal Vulnerability Management Scanning 4

Internal Web Application Scanning (Dynamic) 5

External Vulnerability Management Scanning 6

External (CISA) Web Application Scanning 7

Cyber Threat Intelligence Feeds 8

Monitoring and Detection 9

Security Information and Event Management 9

Network Security Monitoring and Analysis Service (Albert) 10

Phishing E-Mail Analysis 11

DNS Filtering: Malicious Domain Blocking and Reporting (MDBR) 12

Incident Response 13

Agency Incident Response (IR) Plan Creation Assistance 13

Incident Response Coordination and Management 14

Coordination of Tabletop Exercises 15

Enterprise Log Collection and Retention 16

Awareness and Training 17

Annual Security Training 17

Monthly Phishing Campaigns 18

Quarterly Security Awareness 19

October CYBERSecurity Month 20

Cyber Security Risk Assessment 21

Security Risk Assessment 21

Penetration Testing 22

External Vulnerability Scanning and Validation testing 23

Security Standards 24

Business Enablement and Advisory 24

Vendor Contract Review 24

Vendor Security Evaluation and Advisory 25

Business Case Security Consulting 25

Configuration Security Review 26

Network Security 27

Firewall CONFIGURATION 27

Load Balancing 28

Secure socket Layer (SSL) Termination 28

Proxy 29

SSL Virtual Private Network (VPN) 29

Internet Protocol Security (IPSec) VPN 30

Appendix 1 31

Appendix 2 37

INTRODUCTION

About this Service Catalog

This service catalog describes the services currently available to agencies through Enterprise Information Services (EIS), Cyber Security Services (CSS). The services are grouped by service category with each individual service summarized separately within that category.

Some of these services are provided on an enterprise-wide basis, as noted in their descriptions, and thus do not normally require a specific request from an agency. Many services will be tailored to an individual agency's situation and requirements. In that case, CSS will work with the requesting agency to define specific agency and CSS responsibilities.

Format of Service Descriptions

Each service catalog entry contains:

- **Service Description**
    - A brief description of the service and what purpose it serves
    - A list of objectives for the service
- **Engagement Model**
    - CSS' responsibilities associated with the execution of the service
    - The requesting agency's responsibilities regarding execution of the service
    - Service level objectives

Icons

M	Mandatory Service
R	Requested Service

Note that services that are identified as “Requested Service” may identify a service that agencies are required to have but are not required to get through CSS. Services identified as “Mandatory Service” are required to go through CSS.

Requesting Services

To receive more information specific to your agency about any of these services, send a request for the service to ESOINFO@das.oregon.gov.

Overarching Services

Policy and Standards

M

Enterprise Information Services (EIS) has responsibility for statewide information and cybersecurity standards, and policies on information security, under the authority of Oregon Revised Statute 276A.300. As part of EIS, Cyber Security Services (CSS) is responsible for creation and maintenance of the Statewide Information and Cyber Security Standards.

CSS sets the statewide direction for cybersecurity and follows guidance from National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) as well as other cybersecurity organizations such as the Cloud Security Alliance (CSA) where appropriate.

Statewide Information and Cyber Security Standards V1.0

Consulting

R

CSS provides consulting assistance on a voluntary basis to state agencies, boards and commissions. The purpose of these services is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities in state government through stakeholder partnerships and direct assistance activities. CSS maintains central and embedded security resources. CSS security resources:

- Cultivate partnerships with participating organizations and initiate information sharing.
- Introduce organizations to various cybersecurity products and services, along with other resources, and act as liaisons to the organization’s leadership.
- Provide working group support and offer leadership at existing forums and working groups, engaging stakeholders with in-place cybersecurity initiatives and information sharing groups.

Agency Vulnerability Management Plan Creation Assistance

R

Service Description

The Agency Vulnerability Management (VM) Plan Creation Assistance service helps agencies create a plan that defines and documents the planning and operational aspects of the agency vulnerability management program. The agency VM plan is a fundamental source of information that defines the overall agency VM program components and provides auditors with a roadmap for agency VM program operations.

CSS has created a VM plan template that provides an outline and example content for an agency VM plan. The template was created based on input from several sources, including Gartner Consulting, CSS, state agencies, and other consultants.

Service objectives include:

- Reduce cybersecurity risk by enabling the establishment of state agency VM programs.
- Define actions required by ORS 276A.300(3)(a) concerning review and verification of the security of agency information systems.
- Comply with the directive of ORS 276A.300(5) to develop and implement policies for responding to events that damage or threaten the security, availability, and integrity of Oregon information or information systems.
- Provide a common framework for creation of agency VM programs that provides consistency throughout state agencies and leverages EIS CSS resources.
- Provide a detailed template that agencies can use for creation of an agency VM plan.

Engagement Model

CSS RESPONSIBILITIES

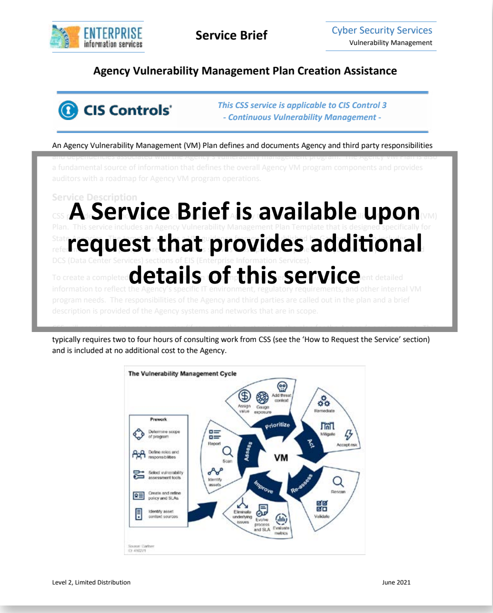
- Provide advice on plan implementation and the template for creation of the agency VM plan.
- Assist agencies on how to construct a customized VM plan specific to their needs.

AGENCY RESPONSIBILITIES

- Submit a request to CSS for assistance with agency VM plan creation.
- Edit and adopt the CSS template based on the agency environment.
- Submit the completed plan to CSS for review and incorporation into the VM plan registry maintained by CSS.

SERVICE LEVEL OBJECTIVES

- New VM plan engagement: 14 days



ENTERPRISE information services

Service Brief

Cyber Security Services
Vulnerability Management

Agency Vulnerability Management Plan Creation Assistance

CIS Controls

This CSS service is applicable to CIS Control 3
- Continuous Vulnerability Management -

An Agency Vulnerability Management (VM) Plan defines and documents Agency and third party responsibilities

a fundamental source of information that defines the overall Agency VM program components and provides auditors with a roadmap for Agency VM program operations.

Service Description

A Service Brief is available upon request that provides additional details of this service

DCS (Data Center Services) sections of EIS (Enterprise Information Services).

information to reflect the Agency's specific IT environment, regulatory requirements, and other internal VM program needs. The responsibilities of the Agency and third parties are called out in the plan and a brief description is provided of the Agency systems and networks that are in scope.

typically requires two to four hours of consulting work from CSS (see the 'How to Request the Service' section) and is included at no additional cost to the Agency.

The Vulnerability Management Cycle

Level 2, Limited Distribution

June 2021

VULNERABILITY MANAGEMENT

Internal Vulnerability Management Scanning

M

Service Description

The Internal Vulnerability Management Scanning service provides dedicated operational infrastructure and technical support to agencies in support of active scanning of specific hosts and/or IP network ranges in their environment. The service includes prioritization of vulnerabilities to be addressed using a risk-based rating approach and monthly reports for agency leadership.

Service objectives include:

- Reduce cybersecurity risk by providing comprehensive vulnerability scanning facilities that can be used for protection of systems within the state network.
- Provide infrastructure and services in support of ORS 276A.300(3)(a) concerning review and verification of the security of agency information systems.
- Provide the VM scanning services to all agencies, including reports and remediation consulting.

Engagement Model

CSS RESPONSIBILITIES

- Establish and maintain the VM infrastructure.
- Maintain and manage VM licensing.
- Prioritize discovered vulnerabilities for remediation.

AGENCY RESPONSIBILITIES

- Provide a technical contact at the agency familiar with the IP address ranges to be scanned.
- Identify specific assets to be scanned.
- Define automated scan schedule and initiate manual scans as required.
- Remediate vulnerabilities as recommended by CSS.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days
- Infrastructure Break-Fix: 2 days
- Custom Requests: Based on Priority/Complexity

Internal Web Application Scanning (Dynamic)

R

Service Description

The Internal Web Application Scanning (Dynamic) service analyzes web-based applications and can be utilized throughout the system development lifecycle, including scanning of production web servers. The service is provided by the CSS Security Operations Center (SOC) and covers devices on state of Oregon government networks, including enterprise-wide and agency-specific networks.

Service features include web application vulnerability scanning, scan automation, and website mapping.

Service objectives include:

- Reduce cybersecurity risk by proactively identifying threats to state-hosted web servers.
- Utilize up-to-date tools to enable detailed analysis of web infrastructure.
- Provide detailed, concise information that can be used to remediate web server vulnerabilities.
- Fulfill the requirement in ORS 276A.300(3)(c) to conduct vulnerability assessments of state agency information systems for the purpose of responding to security vulnerabilities in information systems.

Engagement Model

CSS RESPONSIBILITIES

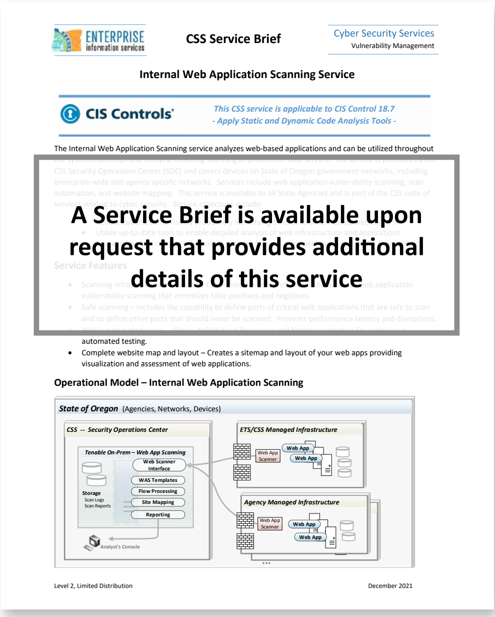
- Establish and maintain infrastructure.
- Maintain and manage licensing.
- Prioritize discovered vulnerabilities for remediation.

AGENCY RESPONSIBILITIES

- Submit a request for this service to CSS.
- Provide a technical contact at the agency familiar with the web applications to be scanned.
- Define automated scan schedule and initiate manual scans as required.
- Remediate vulnerabilities according to degree of risk determined by CSS.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days



ENTERPRISE information services

CSS Service Brief

Cyber Security Services
Vulnerability Management

Internal Web Application Scanning Service

CIS Controls

This CSS service is applicable to CIS Control 18.7
- Apply Static and Dynamic Code Analysis Tools -

The Internal Web Application Scanning service analyzes web-based applications and can be utilized throughout

A Service Brief is available upon request that provides additional details of this service

automated testing.

- Complete website map and layout – Creates a sitemap and layout of your web apps providing visualization and assessment of web applications.

Operational Model – Internal Web Application Scanning

Level 2, Limited Distribution

December 2021

External Vulnerability Management Scanning

M

Service Description

The External Vulnerability Management Scanning service scans internet-accessible assets and checks for known vulnerabilities and weak configurations. The service can scan all external-facing IP address space for the state of Oregon. To the extent that external IP addresses are assigned by agency, individual reports can be generated for each agency. Features include network mapping, vulnerability and configuration scanning, and detailed scan reporting.

This service provides unauthenticated external scanning of state assets utilizing the CISA Cyber Hygiene program using services contracted by EIS CSS and implemented by the Cybersecurity & Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security.

Service objectives include:

- Reduce cybersecurity risk by assessing the security posture of agency and state internet-accessible systems.
- Provide insight into how systems and infrastructure appear to potential attackers.
- Drive proactive mitigation of vulnerable system software.

Engagement Model

CSS RESPONSIBILITIES

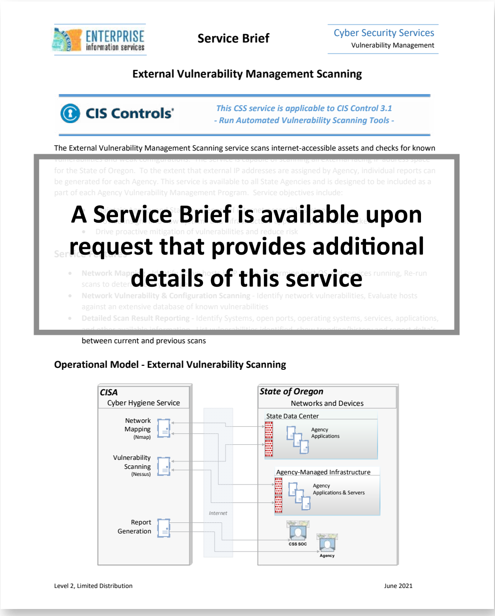
- Maintain coordinated scheduling of all state scans to avoid network saturation.
- Ensure all state external IP address space is being scanned.

AGENCY RESPONSIBILITIES

- Provide CSS SOC with an updated list of agency IP address space that is routable on the public Internet.
- Maintain a distribution list (DL) for receipt of the weekly assessment report.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days


ENTERPRISE information services

Service Brief

Cyber Security Services
Vulnerability Management

External Vulnerability Management Scanning

CIS Controls

This CSS service is applicable to CIS Control 3.1
- Run Automated Vulnerability Scanning Tools -

The External Vulnerability Management Scanning service scans internet-accessible assets and checks for known

A Service Brief is available upon request that provides additional details of this service

between current and previous scans

Operational Model - External Vulnerability Scanning

Level 2, Limited Distribution

June 2021

External (CISA) Web Application Scanning

R

Service Description

The External Web Application Scanning (WAS) service is coordinated and contracted by EIS CSS and implemented by the Cybersecurity & Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security. The service assesses the health of publicly accessible web applications, checking for known vulnerabilities and weak configurations specific to web site implementation. The service can scan any external-facing web application for the state of Oregon. This service is available to all state agencies and is designed to be included as a part of each agency Vulnerability Management program.

Service objectives include:

- Reduce cybersecurity risk by assessing the security posture of agency and state internet-accessible web sites.
- Provide insight into how systems and infrastructure appear to potential attackers.
- Drive proactive mitigation of vulnerable web sites.

Engagement Model

CSS RESPONSIBILITIES

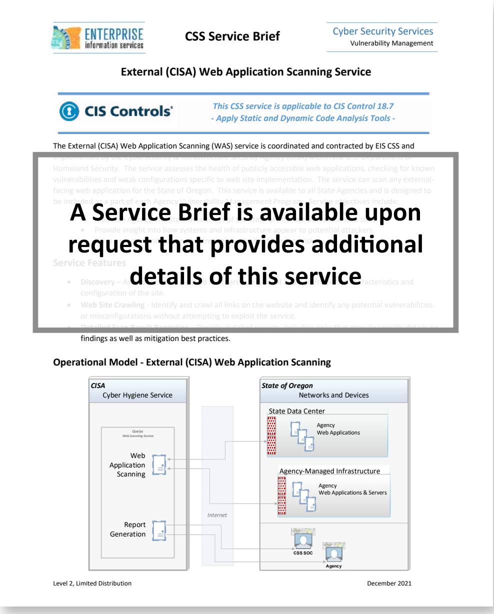
- Maintain coordinated scheduling of all state scans to avoid network saturation.
- Provide contractual interface with CISA for the service.

AGENCY RESPONSIBILITIES

- Submit a request to CSS for assistance with external web application scanning.
- Specify the external (Internet-facing) website(s) to be scanned.
- Maintain a distribution list (DL) for receipt of the weekly assessment report.
- Provide a technical contact at the agency familiar with the website(s) to be scanned.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days



ENTERPRISE information services

CSS Service Brief

Cyber Security Services
Vulnerability Management

External (CISA) Web Application Scanning Service

CIS Controls

This CSS service is applicable to CIS Control 18.7
- Apply Static and Dynamic Code Analysis Tools -

The External (CISA) Web Application Scanning (WAS) service is coordinated and contracted by EIS CSS and

A Service Brief is available upon request that provides additional details of this service

findings as well as mitigation best practices.

Operational Model - External (CISA) Web Application Scanning

Level 2, Limited Distribution

December 2021

Cyber Threat Intelligence Feeds

R

Service Description

The Cyber Threat Intelligence (CTI) Feeds service coordinates threat intelligence information from several commercial and open-source distributions. The CTI collection systems disseminate that information as appropriate for consumption and analysis by CSS and as appropriate to agencies.

This allows agencies to subscribe to, receive, and review feeds from: Multi-State-Information Sharing and Analysis Center (MS-ISAC) - Cybersecurity Advisories, Cyber Alerts, Cyber Intel Advisories, Situational Awareness Reports (SARs); Weekly Attacking IPs and Domains. Other threat information is received from the U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency (CISA), the U.S. Department of Justice, and additional commercial sources.

Activities resulting from the intelligence gathering and creation process may include partner/agency notifications and threat event correlation within the SOC Security Information and Event Management System (SIEM).

Service objectives include:

- Reduce cybersecurity risk by collecting and qualifying a wide base of current threat intelligence from many reputable sources.
- Coordinate activities to better understand and address security incidents and critical cybersecurity threats to the state.
- Disseminate qualified cyber threat intelligence to all involved agencies.
- Meet requirements under statewide policy (107-004-120 – Cyber and Information Security Incident Response).

Engagement Model

CSS RESPONSIBILITIES

- Collect, store and aggregate cyber threat data.
- Review and qualify cyber threat into intelligence from threat data sources.

AGENCY RESPONSIBILITIES

- Review if the CTI is pertinent to the agency.
- Determine if the CTI is fully qualified and in a useful form.

SERVICE LEVEL OBJECTIVES

- Incorporation of new CTI feeds: 30 days

Security Information and Event Management

R

Service Description

The Security Information and Event Management (SIEM) service provides tactical security log monitoring and rapid detection of security events. The service is provided by the CSS Security Operations Center (SOC) and covers devices on state of Oregon government networks, including enterprise-wide and agency-specific networks. Services include enterprise-level log analysis, threat detection, and alerting.

This service is available to all state Agencies and is part of the CSS suite of services related to cybersecurity. Features of this service include:

- Correlation of data from multiple sources - Logs are collected from multiple sources across the enterprise.
- Threat Intelligence and Analytics - Threat feeds from third-party sources augment internal threat data to help prioritize security events requiring proactive action by the SOC.
- Threat Hunting - SOC Analysts use pre-defined and ad-hoc queries, based on the latest threat intelligence, to scan for anomalous events to help proactively thwart threat actors.

Service objectives include:

- Reduce cybersecurity risk by proactively identifying threats to state networks and systems.
- Utilize modern software to correlate events using rules and user behavior analytics.
- Provide detailed, concise information that can be used during Incident Response.

Engagement Model

CSS RESPONSIBILITIES

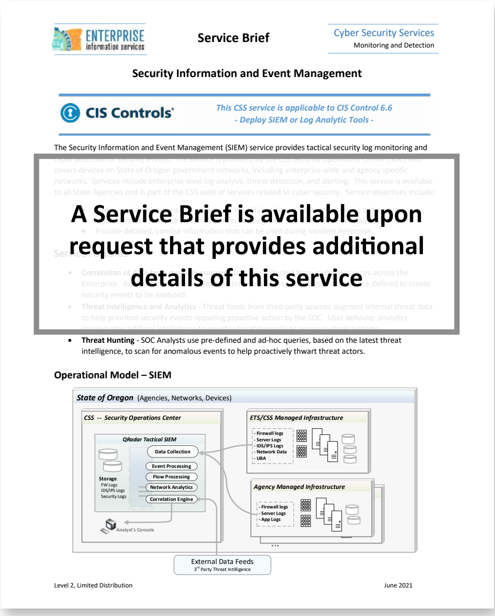
- CSS provides this service without a specific agency request.

AGENCY RESPONSIBILITIES

- Supply a distribution list (DL) that defines where agency-specific alerts are sent.
- Provide specific agency network configuration information when requested from CSS.

SERVICE LEVEL OBJECTIVES

- Agencies notified of detection of potential threats: 24 hours.
- New cyber threat intelligence is incorporated into the SIEM: 24 hours



ENTERPRISE information services

Service Brief

Cyber Security Services
Monitoring and Detection

Security Information and Event Management

CIS Controls

This CSS service is applicable to CIS Control 6.6
- Deploy SIEM or Log Analytic Tools -

The Security Information and Event Management (SIEM) service provides tactical security log monitoring and

A Service Brief is available upon request that provides additional details of this service

- **Threat Hunting** - SOC Analysts use pre-defined and ad-hoc queries, based on the latest threat intelligence, to scan for anomalous events to help proactively thwart threat actors.

Operational Model – SIEM

Level 2, Limited Distribution

June 2021

MONITORING AND DETECTION

Network Security Monitoring and Analysis Service (Albert)

M

Service Description

The Network Security Monitoring and Analysis (Albert) service is a third-party service provided in cooperation with MS-ISAC. The MS-ISAC Albert Network Monitoring Service is implemented at the state government network perimeter and provides network security alerts for both traditional and advanced network threats. The MS-ISAC 24×7 Security Operations Center provides enhanced monitoring capabilities and notifications of malicious activity to EIS CCS SOC.

The service uses a high-performance Intrusion Detection System (IDS) engine and sensors that identify and report on malicious events. It also monitors raw network packets and converts data into an industry standard (netflow) format for efficient storage and analysis of historical data.

Service objectives include:

- Reduce cybersecurity risk by identifying known threats to state networks and systems.
- Identify malicious activity in near-real time.

Utilize high-reliability sources of threat signatures including:

- Commercial signatures optimized for detecting malware and crimeware
- Advanced Persistent Threat (APT) indicators
- Center for Internet Security (CIS) repositories of malicious signature sets

Engagement Model

CSS RESPONSIBILITIES

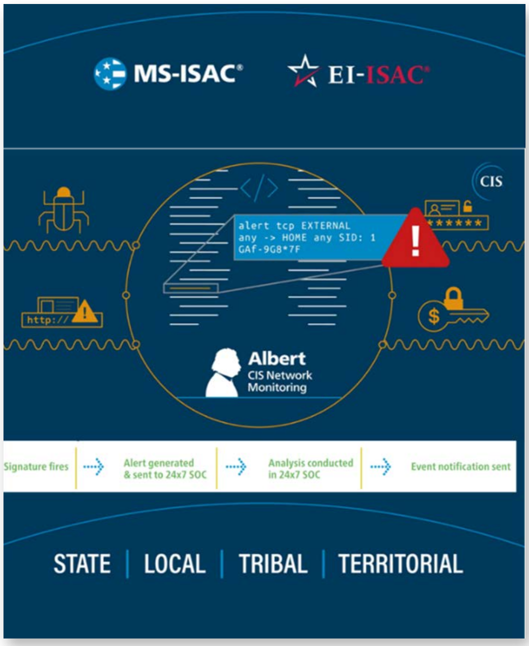
- Engage MS-ISAC and CIS to provide the service within the state network.
- Receive alerts and check the data against internal systems using the SOC Security Information and Event Management System (SIEM).
- Forward event information to agencies for those events needing remediation or information.
- Provide event status and ticket closure information back to MS-ISAC.

AGENCY RESPONSIBILITIES

- Respond to events by providing information to CSS regarding status and corrective action.

SERVICE LEVEL OBJECTIVES

- Forward alerts to agencies: 24 hours
- Respond to MS-ISAC: 24 hours from receipt of agency response



Phishing E-Mail Analysis

M

Service Description

The Phishing E-Mail Analysis service provides for review and possible action on reported phishing e-mails as part of the ReportAPhish program. Suspicious or potentially harmful e-mails are forwarded to the CSS SOC from agency e-mail users by e-mailing directly to ReportAPhish@das.oregon.gov or using the Outlook PhishAlert button.

The PhishAlert button is provided by the EIS Phishing Awareness Program as an Outlook toolbar add-on to agencies. The Phish Alert Button (PAB):

- Forwards the e-mails to an agency-determined e-mail address retaining all header information for analysis.
- Provides automatic feedback to staff informing them the e-mail they are reporting is an EIS simulated phishing attack. If it is not a simulation, further analysis will be done to determine if the email was a phishing attack.
- Moves the e-mail from their mailbox to their deleted folder.

Service objectives include:

- Reduce cybersecurity risk by providing a mechanism to report on and inspect suspicious e-mails.
- Capture data for metrics related to suspicious e-mails and organize by type (Valid, Spam, Phishing, No Info).
- Provide a consistent and convenient method to report suspicious e-mails across agencies.

Engagement Model

CSS RESPONSIBILITIES

- Include PAB as part of the EIS Phishing Awareness Program.
- Send out simulation phishing e-mails to agencies.

AGENCY RESPONSIBILITIES

- Adopt a process for reporting suspicious e-mails, including the use of PAB or alternate method.
- Determine agency training requirements for the agency phishing reporting process.
- Use resources provided by the Information Security Awareness and Training (ISAT) program for any communication and training needed.

SERVICE LEVEL OBJECTIVES

- Review the ReportAPhish mailbox: Daily
- Create an M365 ticket if requested: Same Day
- Create metrics based on suspicious e-mail type: Weekly and Monthly

DNS Filtering: Malicious Domain Blocking and Reporting (MDBR)

M

Service Description

The DNS Filtering service proactively blocks network traffic from the state to known harmful web domains. All external domain name system (DNS) requests sent to the Data Center Services (DCS) DNS Server are sent to the Secure DNS provider. Every DNS lookup is compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, are blocked and logged.

The DNS Filtering service utilizes the Malicious Domain Blocking and Reporting (MDBR) service funded by the U.S. Department of Homeland Security and provided by the Center for Internet Security (CIS). This MDBR service has been made available to all U.S. State, Local, Tribal, and Territorial (SLTT) governments in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Service objectives include:

- Reduce cybersecurity risk by proactively blocking access to malicious domains.
- Utilize up-to-date tools and malicious domain lists to limit access to malicious sites.
- Provide detailed reporting to CSS.

Engagement Model

CSS RESPONSIBILITIES

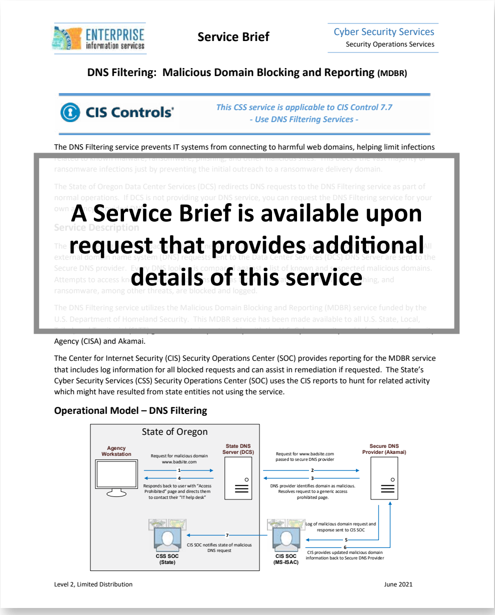
- Contract with CIS to supply the MDBR service to agencies.
- SOC analysts review blocked sites that may require unblocking.
- Interface with CIS for changes in the service.
- Review reports provided by CIS.

AGENCY RESPONSIBILITIES

- Report sites blocked by MDBR to CSS for review and potential remediation.

SERVICE LEVEL OBJECTIVES

- New service implementation: 7 days
- Review requests to unblock sites: Same Day



ENTERPRISE information services

Service Brief

Cyber Security Services
Security Operations Services

DNS Filtering: Malicious Domain Blocking and Reporting (MDBR)

CIS Controls

This CSS service is applicable to CIS Control 7.7
- Use DNS Filtering Services -

The DNS Filtering service prevents IT systems from connecting to harmful web domains, helping limit infections

A Service Brief is available upon request that provides additional details of this service

Agency (CISA) and Akamai.

The Center for Internet Security (CIS) Security Operations Center (SOC) provides reporting for the MDBR service that includes log information for all blocked requests and can assist in remediation if requested. The State's Cyber Security Services (CSS) Security Operations Center (SOC) uses the CIS reports to hunt for related activity which might have resulted from state entities not using the service.

Operational Model – DNS Filtering

State of Oregon
Agency Workstation
Request for malicious domain www.badsite.com
1
4
Responds back to user with "Access Prohibited" page and directs them to contact their "IT help desk"
State DNS Server (DCS)
Request for www.badsite.com passed to secure DNS provider
2
3
DNS provider identifies domain as malicious. Resolves request to a generic access prohibited page.
Secure DNS Provider (Akamai)
Log of malicious domain request and response sent to CIS SOC
5
6
CIS provides updated malicious domain information back to Secure DNS Provider
7
CIS SOC notifies state of malicious DNS request
CSS SOC (State)
CIS SOC (MS-ISAC)

Level 2, Limited Distribution

June 2021

Agency Incident Response (IR) Plan Creation Assistance

R

Service Description

The Agency Incident Response (IR) Plan Creation Assistance service assists agencies with creation of an agency-specific Information Security Incident Response Plan. CSS provides consultation to agency management and staff and provides a customizable template that agencies can use to establish an IR plan.

All agencies are required to have an incident response plan and to perform regular tabletop exercises against the plan. The IR plan identifies the resources and defines the processes for responding to any event that harms or threatens the security of agency information assets and identifies where the agency will take advantage of CSS capabilities.

Service objectives include:

- Reduce cybersecurity risk by enabling the establishment of agency incident response programs.
- Collaborate with agencies as required by ORS 276A.300(5) to develop and implement policies and procedures for incident response.
- Meet the requirements under the Statewide Information Security Incident Response Plan.
- Document processes that facilitate quick and efficient response to incidents to limit incident impact.
- Provide a common framework for creation of agency IR programs that provides consistency throughout state agencies and leverages EIS CSS resources.

Engagement Model

CSS RESPONSIBILITIES

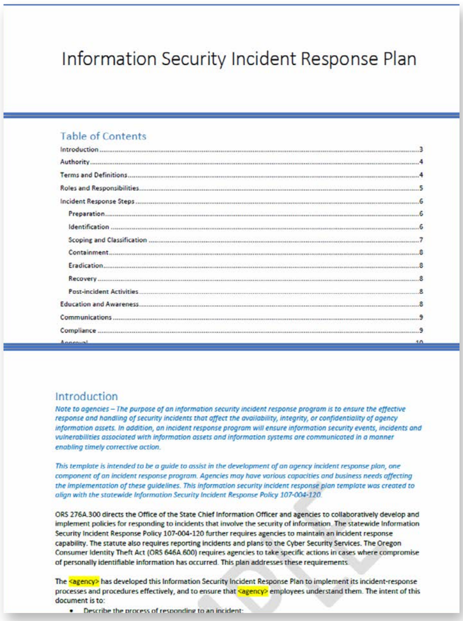
- Create and provide an IR template for creation of the agency IR plan.
- Assist agencies on how to construct a customized IR plan specific to agency needs.

AGENCY RESPONSIBILITIES

- Submit a request to CSS for assistance with agency IR plan creation.
- Edit and adopt the CSS IR template based on the agency environment.
- Submit the completed plan to CSS for review and incorporation into the IR plan registry maintained by CSS.

SERVICE LEVEL OBJECTIVES

- New IR plan engagement: 14 days



Information Security Incident Response Plan

Table of Contents

Introduction 3
Authority 4
Terms and Definitions 4
Roles and Responsibilities 5
Incident Response Steps 6
Preparation 6
Identification 6
Scoping and Classification 7
Containment 8
Eradication 8
Recovery 8
Post-incident Activities 8
Education and Awareness 8
Communications 9
Compliance 9
Approval 10

Introduction

Note to agencies – The purpose of an information security incident response program is to ensure the effective response and handling of security incidents that affect the availability, integrity, or confidentiality of agency information assets. In addition, an incident response program will ensure information security events, incidents and vulnerabilities associated with information assets and information systems are communicated in a manner enabling timely corrective action.

This template is intended to be a guide to assist in the development of an agency incident response plan, one component of an incident response program. Agencies may have various capacities and business needs affecting the implementation of these guidelines. This information security incident response plan template was created to align with the statewide Information Security Incident Response Policy 107-004-120.

ORS 276A.300 directs the Office of the State Chief Information Officer and agencies to collaboratively develop and implement policies for responding to incidents that involve the security of information. The statewide Information Security Incident Response Policy 107-004-120 further requires agencies to maintain an incident response capability. The statute also requires reporting incidents and plans to the Cyber Security Services. The Oregon Consumer Identity Theft Act (ORS 646A.600) requires agencies to take specific actions in cases where compromise of personally identifiable information has occurred. This plan addresses these requirements.

The <agency> has developed this Information Security Incident Response Plan to implement its incident-response processes and procedures effectively, and to ensure that <agency> employees understand them. The intent of this document is to:

- Describe the process of responding to an incident;

INCIDENT RESPONSE

Incident Response Coordination and Management

M

Service Description

The Incident Response Coordination and Management service provides enterprise-level incident response services to all agencies. CSS provides consultation to agency management and staff at any stage of the security incident response process, from initial triage to appropriate actions in response to the final closeout report.

CSS is prepared to assist or lead incident response based on the scope and scale of the incident. This service includes basic forensic capabilities and CSS will also coordinate with third party vendors that may be engaged to supply software or services associated with the incident.

CSS SOC response activities generally follow the incident response handling stages as described in NIST Special Publication 800-61. The State of Oregon Information Security Incident Response Plan contains considerable details of the IR process.

Service objectives include:

- Reduce cybersecurity risk and minimize loss of data and service disruptions by providing agencies with timely coordination and expert knowledge related to incidents, including post-incident analysis and incorporation of lessons learned.
- Coordinate and enter into agreements for third-party services as permitted by ORS 276A.332(1) related to incident response.
- Fully understand and address security incidents and critical cybersecurity threats to the state.

Engagement Model

CSS RESPONSIBILITIES

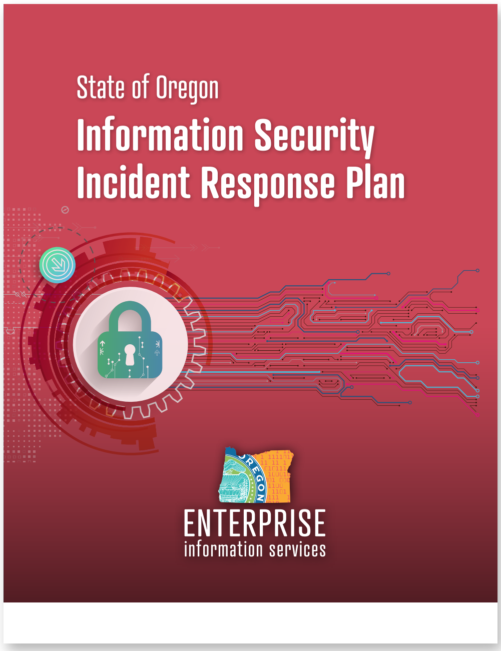
- Assist or lead all levels of incident response as needed.
- Provide consulting/coordination on public-facing communications.
- State Chief Information Security Officer notify Legislative Fiscal Office as appropriate.

AGENCY RESPONSIBILITIES

- Request help from the CSS SOC team at any time during incident response.
- Notify CSS of all incidents and provide regular updates on status and progress.

SERVICE LEVEL OBJECTIVES

- CSS engagement upon request: Same Day



State of Oregon

Information Security Incident Response Plan

ENTERPRISE
information services

Coordination of Tabletop Exercises

R

Service Description

The Coordination of Tabletop Exercises service provides planning and coordination of incident response exercises and scenarios for the workforce involved in incident response. The tabletop exercises test communications channels, decision-making, and incident responders' technical capabilities using available tools and data.

Tabletop exercises are designed to maintain familiarization with the statewide and agency information security incident response plans, while also testing the agency’s ability to execute the plan and identify areas of improvement or updates to plans.

Service objectives include:

- Reduce cybersecurity risk by ensuring timely response to security incidents through preparation and simulation of cyber incidents.
- Coordinate activities as required by ORS 276A.323(2)(e) to better understand and address security incidents and critical cybersecurity threats to the state.
- Meet requirements under statewide policy (107-004-120 – Cyber and Information Security Incident Response).
- Meet requirements under the State of Oregon Information Security Incident Response Plan.

Engagement Model

CSS RESPONSIBILITIES

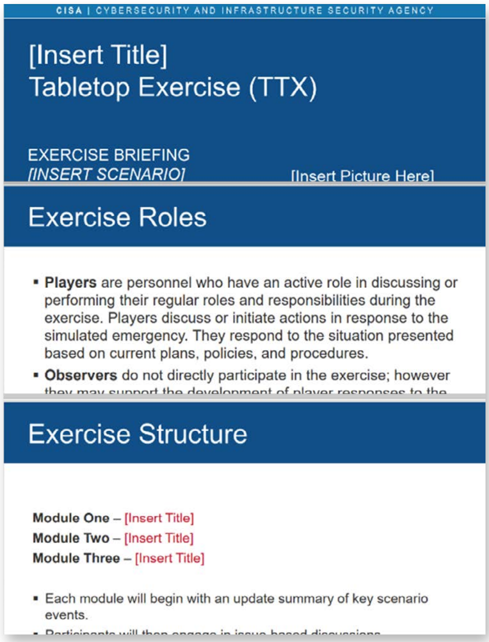
- Coordinate contracts and scheduling with third-party vendors.
- Facilitate exercise implementation.
- Assist in remediation of findings associated with the exercise.

AGENCY RESPONSIBILITIES

- Schedule periodic exercises and review related to IR plan.
- Coordinate with CSS in support of exercises and findings.

SERVICE LEVEL OBJECTIVES

- Testing and review of IR plans: Annually



CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

[Insert Title]
Tabletop Exercise (TTX)

EXERCISE BRIEFING
[INSERT SCENARIO]

[Insert Picture Here]

Exercise Roles

- **Players** are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency. They respond to the situation presented based on current plans, policies, and procedures.
- **Observers** do not directly participate in the exercise; however they may support the development of player responses to the

Exercise Structure

Module One – [Insert Title]
Module Two – [Insert Title]
Module Three – [Insert Title]

- Each module will begin with an update summary of key scenario events.
- Participants will then engage in issue based discussions

Enterprise Log Collection and Retention

R

Service Description

The Enterprise Log Collection and Retention service collects and retains select enterprise logs for compliance and cyber incident response. This is limited to Data Center Services systems. It is focused on firewall and network logs originating from infrastructure supported by the State Data Center and CSS.

All logs are separated into different retention buckets based on type of data and agency or other requirements.

Service objectives include:

- Reduce cybersecurity risk by storing and maintaining logs that are valuable for incident response activities and cyber threat determination.
- Ingest and manage logs required for state and federal regulatory compliance.
- Provide log search capabilities to aide in troubleshooting and threat analysis.
- Provide stable and secure log storage and management infrastructure for the state.

Engagement Model

CSS RESPONSIBILITIES

- Maintain infrastructure for storage and work with DCS.
- Maintain connectivity from log sources.
- Provide adequate storage for retention needs.
- Add new sources as needed.
- Review log sources and provide audit information to agencies and DCS.

AGENCY RESPONSIBILITIES

- Review information as needed.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Annual Security Training

M

Service Description

The Annual Security Training service is a continuous effort to educate and empower the state's workforce to adopt good security habits at work, at home and while mobile with awareness and targeted training to address specific roles and risks.

ORS 276A.323 requires annual information security awareness training for all employees, board and commission members, temporary employees, contractors, and volunteers and applies to all Executive Branch agencies. This statutory requirement is limited to Executive Branch agencies as defined in ORS 174.112 but is not limited to those with state system access. It includes all information assets; written, verbal, and electronic information related to the state of Oregon.

Per the Department of Administrative Services (DAS) Statewide Employee Training policy 10.040.01 – State Employee Training, all users who have access to state information assets are required to complete annual computer-based training through the state's Learning Management System. EIS provides the annual information security awareness training for the Executive Branch only.

Service objectives include:

- Improve the security culture of the enterprise.
- Reduce cybersecurity risk by providing foundational information security training for the state's workforce.
- Ensure compliance with the aforementioned policy.
- Reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

Engagement Model

CSS RESPONSIBILITIES

- Provide annual security training through the state's Learning Management System.

AGENCY RESPONSIBILITIES

- Incorporate the awareness and training content into their training program.
- Provide access to the state's Learning Management System to all staff.

SERVICE LEVEL OBJECTIVES

- Service implementation: Annually

Monthly Phishing Campaigns

M

Service Description

The Monthly Phishing Campaigns service is a continuous effort to educate and empower the state's workforce to adopt good security habits at work, at home and while mobile with awareness and targeted training to address specific roles and risks.

A phishing awareness program, also known as a phishing simulation program, phishing assessment program or self-phishing, is a customizable training and awareness program used by security awareness professionals in various industries.

This program allows EIS CSS to simulate phishing emails that can be sent to end users. Conducting these types of phishing attack simulations helps empower end users to make better decisions around email and can also help identify which end users or programs are responsive in order to provide the opportunity for more focused training opportunities to help reduce organizational risk.

Service objectives include:

- Improve the security culture of the enterprise.
- Reduce cybersecurity risk by empowering users to make better decisions around email.
- Reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

Engagement Model

CSS RESPONSIBILITIES

- Oversee the implementation of the Phishing Awareness Program.
- Provide communication updates and metrics to participating agencies.

AGENCY RESPONSIBILITIES

- Provide communication about the Phishing Awareness Program to all staff prior to implementation.
- Provide all supporting documentation to staff prior to and during participation in the Phishing Awareness Program.
- Prevent all spam filtering of emails related to the Phishing Awareness Program.
- Implementation of the Phish Alert Button.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Quarterly Security Awareness

M

Service Description

The Quarterly Security Awareness service is a continuous effort to educate and empower the state's workforce to adopt good security habits at work, at home and while mobile with awareness and targeted training to address specific roles and risks.

We understand and recognize that training people annually is not enough to change human behavior and reduce organizational risk. As a result, the awareness program continuously reinforces key behaviors by utilizing various methods throughout the year.

Service objectives include:

- Improve the security culture of the enterprise.
- Reduce cybersecurity risk by providing reinforcement training.
- Reduce cybersecurity risk by providing agencies access to additional security training resources through the state's Learning Management System.
- Reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

Engagement Model

CSS RESPONSIBILITIES

- Provide Security Awareness material: short videos, e-mail templates, and printed material through the state's Learning Management System.
- Provide agencies access to additional security training resources through the state's Learning Management System.

AGENCY RESPONSIBILITIES

- Incorporate the awareness and training content into their training program.
- Provide access to the state's Learning Management System to all staff.
- Support, disseminate, and publish the awareness materials.
- Provide time for staff to participate.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

October CYBERSecurity Month

M

Service Description

October Cybersecurity Month service is an annual effort to educate and empower the state's workforce to adopt good security habits at work, at home and while mobile with awareness and targeted training to address specific roles and risks.

We understand and recognize that training people annually is not enough to change human behavior and reduce organizational risk. As a result, the awareness program continuously reinforces key behaviors by utilizing various methods throughout the year.

Cybersecurity Awareness Month—previously known as National Cybersecurity Awareness Month—continues to raise awareness about the importance of cybersecurity across our Nation, ensuring that all Americans have the resources they need to be safer and more secure online.

Service objectives include:

- Improve the security culture of the enterprise.
- Reduce cybersecurity risk by increasing awareness of cybersecurity.
- Reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

Engagement Model

CSS RESPONSIBILITIES

- Provide resources related to Cybersecurity Awareness Month.

AGENCY RESPONSIBILITIES

- Incorporate the awareness and training content into their training program.
- Provide access to the state's Learning Management System to all staff.
- Support, disseminate, and publish the materials.
- Provide time for staff to participate.

SERVICE LEVEL OBJECTIVES

- Annual service implementation: October

CYBER SECURITY RISK ASSESSMENT

Security Risk Assessment

M

Service Description

The Security Risk Assessment service provides biennial information security assessments against the Center for Internet Security (CIS) Controls to assess the fundamental security posture of Executive Branch agencies, boards, and commissions. The assessment provides a list of strengths and weaknesses and suggests recommendations the agency can use to develop a roadmap and plans to improve their security posture.

- ORS 276A.203, ORS 276A.300 and 276A.306 require agencies and EIS CSS collaboratively work together to perform biennial security assessments. CSS' Security Assessment and Risk Management section has developed the CIS Control Assessment service to satisfy this statutory responsibility and align with the State Chief Information Security Officer's strategic commitment to the CIS controls.

Security Assessment Tasks include:

- Kickoff Meeting: Provide a high-level overview of the assessment process.
- Interview Session: Review controls implementation status.
- Technical Assessment: Perform discovery, inventory, vulnerability scans, and other technical checks.
- Draft Report: Provide draft report to agency for review.
- Agency Feedback: Opportunity to make corrections prior to report finalization
- Out Brief: CSS will conduct a briefing of the assessment with agency stakeholders, answering any questions that may arise.
- Final Report: Generate and deliver final reports to agency and enterprise stakeholders.

Service objectives include:

- Help agencies identify and remediate critical security gaps and provide priority recommendations for the implementation of the CIS controls.
- EIS identify common weak points in enterprise defenses to help inform enterprise service development.
- Track aggregated results to monitor enterprise risk posture.
- Report aggregated results to the Governor's Office and Legislature.

Engagement Model

CSS RESPONSIBILITIES

- Lead Assessment.
- Coordinate testing with agency staff per rules of engagement.
- Facilitate interviews, meetings, and check-ins.
- Notify agency (and State Incident Response Team if needed) if a critical issue is found.
- Provide prioritized recommendations.
- Continue remediation support through CSS.

AGENCY RESPONSIBILITIES

- Respond to CSS survey and artifact requests.
- Provide agency executive sponsor.
- Provide agency single point of contact for assessment coordination.
- Ensure appropriate staff participate in kick-off, interviews, technical sessions and exit briefings.
- Provide network access and assist CSS assessors performing technical tests.
- Review draft CSS report and provide feedback if needed.
- Collaborate with CSS to address findings.

SERVICE LEVEL OBJECTIVES

- New service implementation: 60 days

Penetration Testing

R

Service Description

More complex than the External Vulnerability Scanning Service, the Penetration Testing service involves testing the protection, detection, and response capabilities of the organization by finding and exploiting vulnerabilities in a targeted computer system, the organizations user community, and its network. Assessors perform either Black-Box or Gray-Box assessments to simulate the cyberattack.

Service objectives include:

- Help agencies understand and manage risk.
- Test cyber-defense capabilities.
- Measure and characterize potential impact from data breaches.
- Measure business resilience.
- Support penetration testing compliance requirements on regulated systems.

Engagement Model

CSS RESPONSIBILITIES

- Lead the assessment.
- Provide in-depth testing as required.
- Facilitate interviews, meetings, and check-ins.

AGENCY RESPONSIBILITIES

- Request penetration testing from CSS.
- Respond to questionnaire and artifact requests.
- Provide scope of assessment.
- Agree to rules of engagement.
- Provide agency executive sponsor.
- Provide agency single point of contact for assessment coordination.
- Assign appropriate staff to participate in kick-off, interviews, technical sessions and exit briefings.
- Provide network access and assist CSS assessors performing technical tests.
- Review draft CSS report and provide feedback if needed.

SERVICE LEVEL OBJECTIVES

- New service implementation: 2 weeks.

External Vulnerability Scanning and Validation testing

R

Service Description

The External Vulnerability Scanning and Validation Testing service provides scanning of targeted internet-accessible assets and checks for known vulnerabilities and weak configurations. The External Vulnerability Scanning and Validation Testing service uses unauthenticated and authenticated scanning on targeted external-facing agency systems to identify potential vulnerabilities. Additionally, the Assessment Team conducts validation testing of identified vulnerabilities using different tools and methods to determine validity.

Service objectives include:

- Reduce cybersecurity risk by assessing the security posture of internet-accessible systems.
- Provide insight into how systems and infrastructure appear to potential attackers.
- Validate vulnerabilities as positive, false-positive, negative, or false-negative.
- Validate remediation of vulnerabilities.
- Drive proactive mitigation of vulnerable system software.
- Assist agencies with integrating security testing into the development lifecycle.

Engagement Model

CSS RESPONSIBILITIES

- Provide assessment questionnaire and rules of engagement to agency.
- Perform technical testing per the rules of engagement.
- Deliver report to agency.
- Perform follow-up scanning to validate vulnerability remediation, if requested by agency.

AGENCY RESPONSIBILITIES

- Request External Vulnerability Scanning and Validation Testing from CSS.
- Respond to questionnaire.
- Provide scope of assessment.
- Agree to rules of engagement.
- Provide agency executive sponsor.
- Provide agency single point of contact for assessment coordination.
- Remediate any vulnerabilities identified by the scan.

SERVICE LEVEL OBJECTIVES

- New service implementation: As defined between agency and CSS.

Business Enablement and Advisory

R

Service Description

Business Enablement and Advisory service provides expert cybersecurity policy, consulting, and advocacy services with a priority to reduce security risks.

Service objectives include:

- Communicate security risks and benefits of the organization's cybersecurity initiatives with state leadership and agency executive management in business and operational terms.
- Provide enterprise cybersecurity standardization.
- Research, plan, document and maintain current knowledge for IT security frameworks and standards for network, software, and data.

Engagement

CSS RESPONSIBILITIES

- Provide CSS resource for agencies to utilize for guidance on security standards and best practices while advocating to reduce or mitigate security risks.

AGENCY RESPONSIBILITIES

- Agencies contact CSS to ask for security assistance.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Vendor Contract Review

R

Service Description

Vendor Contract Review service provides the determination of the security risk associated with the vendor contract and provides standard security terms and conditions for inclusion.

Service objectives include:

- Work in partnership with stakeholders and follow contracting guidelines to review, assist or provide highly technical input on security requirements in solicitations, contracts and amendments.
- Provide recommendations in partnership with Senior IT Portfolio Managers, EIS Oversight Analysts and others regarding information security requirements and recommend improvements to minimize security threats.
- Lead agencies in developing or providing informational technical input to security related documents including System Security Plans (SSP).

Engagement Model

CSS RESPONSIBILITIES

- Provide vendor contract reviews with agencies to determine the security risk associated with the vendor contract and provide standard security terms and conditions for inclusion.

AGENCY RESPONSIBILITIES

- Involve CSS in review of their IT investment.

SERVICE LEVEL OBJECTIVES

- TBD

SECURITY STANDARDS

Vendor Security Evaluation and Advisory

R

Service Description

Vendor Security Evaluation and Advisory service provides evaluation of potential vendors and service providers against internal security requirements and controls. CSS maintains an inventory of evaluations of audited vendors. Note: The inventory of evaluations does not constitute a pre-approved list of vendors. This service does not provide approval from a procurement perspective.

Service objectives include:

- Identify and educate agencies on laws, regulations and policies as they relate to cybersecurity.
- Provide expert level technical information, security knowledge and application of vendor tools and services.
- Lead agencies in the development of security system requirements by working with stakeholders, assessing current and future potential security risks.

Engagement Model

CSS RESPONSIBILITIES

- Participate with agencies in statewide price agreements, solicitations including RFPs, contract renewals and other IT investments.

AGENCY RESPONSIBILITIES

- Participate in statewide price agreements, RFPs etc.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Business Case Security Consulting

R

Service Description

Business Case Security Consulting service provides security perspective and guidance for business case development of new technologies, tools, or services.

Service objectives include:

- Assess programs and technical mechanisms to ensure compliance with contractual obligations and security standards.
- Collaborate with agencies and CSS to ensure security improvement actions are evaluated, validated, and implemented as required.
- Provide information technical consultation of hardware, software and data systems to ensure security plans and improvements are implemented correctly.

Engagement Model

CSS RESPONSIBILITIES

- Provide CCS resource for all agency IT investments, advising the agency’s project team.

AGENCY RESPONSIBILITIES

- Involve CSS in review of their IT investment.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Configuration Security Review

R

Service Description

Configuration Security Review service provides configuration reviews upon request to identify potential configuration concerns in operating systems, network equipment, and/or application servers.

Service objectives include:

- Collaborate with agencies in meeting SOC 2 compliance and providing recommendations to improve.
- Coordinate resourcing internal CSS resources for the agencies to better respond to system scan results to help improve security posture.

Engagement Model

CSS RESPONSIBILITIES

- Provide security review of system artifacts (Vulnerability Scans, Configuration Scans, SSP, etc.).

AGENCY RESPONSIBILITIES

- Provide the system artifacts (Vulnerability Scans, Configuration Scans, SSP, etc.) to CSS Governance Risk and Compliance for security configuration review.

SERVICE LEVEL OBJECTIVES

- New service implementation: 30 days

Firewall CONFIGURATION

R

Service Description

Firewall Configuration service provides resources to design, coordinate, test, and implement changes to firewall configurations at the state network perimeter and at agency network boundaries. Proper firewall configuration prevents unauthorized access to computing devices within the state network. This service is available to all state agencies.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for firewall changes.
- Provide a formal set of rules for firewall configurations.
- Ensure consistent firewall design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

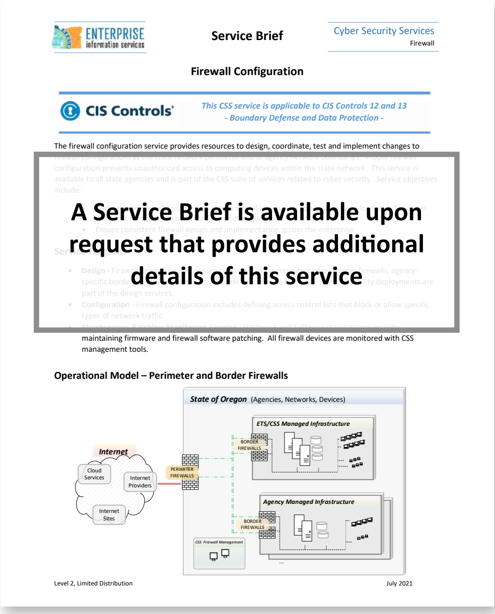
- Review firewall requests sent in by the customer.
- Approve or deny the requests after review and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

- Gain agency approval.
- Submit firewall request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days



ENTERPRISE information services | Service Brief | Cyber Security Services Firewall

Firewall Configuration

CIS Controls® This CSS service is applicable to CIS Controls 12 and 13 - Boundary Defense and Data Protection -

The firewall configuration service provides resources to design, coordinate, test and implement changes to firewall configurations at the state network perimeter and at agency network boundaries. Proper firewall configuration prevents unauthorized access to computing devices within the state network. This service is available to all state agencies and is part of the CSS suite of services related to cyber security. Service objectives include:

A Service Brief is available upon request that provides additional details of this service

- **Configuration -** Firewall configuration includes defining access control lists that block or allow specific types of network traffic.
- maintaining firmware and firewall software patching. All firewall devices are monitored with CSS management tools.

Operational Model – Perimeter and Border Firewalls

Level 2, Limited Distribution July 2021

Load Balancing

R

Service Description

Load Balancing service provides resources to design, coordinate, test, and implement changes to network load balancing configurations. Network load balancers boost the efficiency and implementation of applications through load distribution and application management. Load balancing servers optimize resource use, minimize response time, and reduce the possibility of overloading resources.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for load balancing changes.
- Provide a formal set of rules for load balancing configurations.
- Ensure consistent load balancing design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

- Review load balancing requests sent in by the customer, approve or deny the requests after review, and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

- Gain agency approval.
- Submit request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days

Secure socket Layer (SSL) Termination

R

Service Description

Secure Socket Layer (SSL) Termination service provides resources to design, coordinate, test, and implement changes to SSL termination which is used to reduce the load on the main application servers by offloading cryptographic processing to another machine, to control where the cryptographic processing takes place and to support servers that do not support SSL.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for termination services changes.
- Provide a formal set of rules for termination services configurations.
- Ensure consistent termination services design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

- Review termination requests sent in by the customer, approve or deny the requests after review, and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

- Gain agency approval.
- Submit request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days

Proxy

R

Service Description

Proxy service provides resources to design, coordinate, test, and implement changes to proxy configurations. Proxy servers act as an intermediary server between application users and the application servers. This separation can be used to organize distributed computing systems, implement services, such as load balancing, and browse external networks securely.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for proxy changes.
- Provide a formal set of rules for proxy configurations.
- Ensure consistent proxy design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

- Review proxy requests sent in by the customer, approve or deny the requests after review, and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

- Gain agency approval.
- Submit request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days

SSL Virtual Private Network (VPN)

R

Service Description

SSL Virtual Private Network (VPN) service provides resources to design, coordinate, test, and implement SSL VPN profiles for end-user secure remote access. Secure remote-access VPNs allow secure access to state resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with today’s VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to authorized staff, to any place, at any time.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for SSL VPN changes.
- Provide a formal set of rules for SSL VPN configurations.
- Ensure consistent SSL VPN design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

- Review SSL VPN requests sent in by the customer, approve or deny the requests after review, and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

- Gain agency approval.
- Submit request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days

Internet Protocol Security (IPSec) VPN

R

Service Description

Internet Protocol Security (IPSec) VPN service provides resources to design, coordinate, test, and implement changes to IPSec configurations also known as site-to-site VPN.   An IPSec VPN provides an enhanced layer of security for site-to-site private networking, which authenticates and encrypts the traffic sent between two networks. This allows organizations to cost-effectively and securely extend the reach of their networks to authorized staff.

Service objectives include:

- Reduce cybersecurity risk by providing a formal review and approval process for IPSec VPN changes.
- Provide a formal set of rules for IPSec configurations.
- Ensure consistent IPSec design and implementation across the enterprise.

Engagement Model

CSS RESPONSIBILITIES

- Review VPN requests sent in by the customer, approve or deny the request after review, and implement the approved requests.
- After the request has been implemented, CSS will notify the customer and the agency can test the new configuration to ensure it meets the request.

AGENCY RESPONSIBILITIES

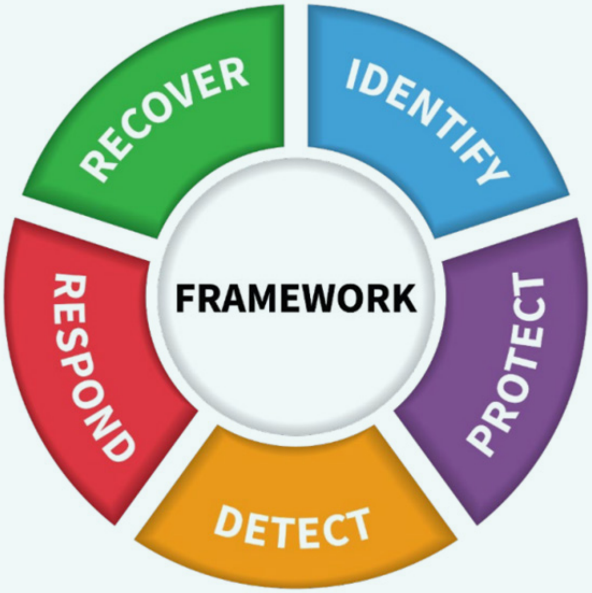
- Gain agency approval.
- Submit request.
- Provide information.
- Test demotion or increase in access as requested.

SERVICE LEVEL OBJECTIVES

- New service implementation: 3-5 days

APPENDIX 1

NIST Cybersecurity Framework



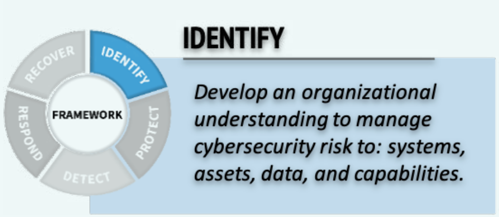
CSS Adopted Cybersecurity Framework

August 3, 2022

APPENDIX 1

NIST Cybersecurity Framework Defined.

The Framework is organized by five key Functions – Identify, Protect, Detect, Respond, Recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity over time. The activities listed under each Function may offer a good starting maturity guide for our organization.



IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

Critical Information Asset List

- **Identify critical enterprise processes and assets** – What are your enterprise's activities that absolutely must continue in order to be viable? For example, this could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information your enterprise collects remains accessible and accurate.
- **Document information flows** – It's important to not only understand what type of information your enterprise collects and uses, but also to understand where the data is located and flows, especially where contracts and external partners are engaged.
- **Maintain hardware and software inventory** – It's important to have an understanding of the computers and software in your enterprise because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.
- **Establish policies for cybersecurity that include roles and responsibilities** – These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).
- **Identify threats, vulnerabilities, and risk to assets** – Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Ensure risk responses are identified and prioritized, executed, and results monitored.

APPENDIX 1

RECOVER
IDENTIFY
FRAMEWORK
PROTECT
RESPOND
DETECT

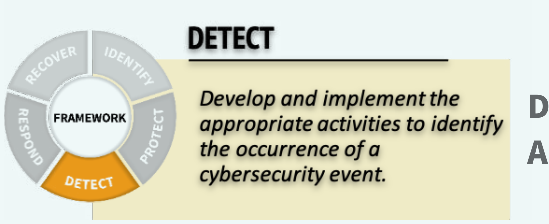
PROTECT

Develop and implement the appropriate safeguards to ensure delivery of services.

Protect Critical Information Assets

- **Manage access to assets and information** – Create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs. Authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications. Tightly manage and track physical access to devices.
- **Protect sensitive data** – If your enterprise stores or transmits sensitive data, make sure that this data is protected by encryption both while it's stored on computers as well as when it's transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it's no longer needed or required for compliance purposes.
- **Conduct regular backups** – Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware.
- **Securely protect your devices** – Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of.
- **Manage device vulnerabilities** – Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.
- **Train users** – Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.

APPENDIX 1



DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Detect Threats to Critical Information Assets

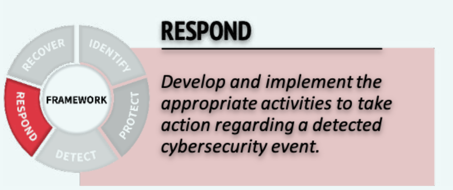
- **Test and update detection processes –** Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your organization and to external governance and legal authorities.

- **Maintain and monitor logs** – Logs are crucial in order to identify anomalies in your enterprise's computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.

- **Know the expected data flows for your enterprise** – If you know what and how data is expected to flow for your enterprise, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include customer information being exported from an internal database and exiting the network. If you have contracted work to a cloud or managed service provider, discuss with them how they track data flows and report, including unexpected events.

- **Understand the impact of cybersecurity events** – If a cybersecurity event is detected, your enterprise should work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicating information on the event with appropriate stakeholders will help keep you in good stead in terms of partners, oversight bodies, and others (potentially including investors) and improve policies and processes.

APPENDIX 1



RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Respond & Mitigate Detected Threats to Critical Information Assets

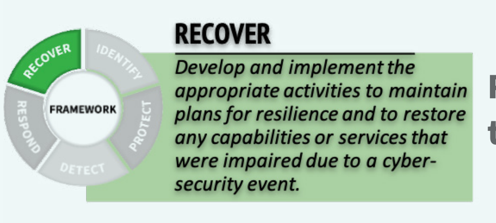
- **Ensure response plans are tested** – It's even more important to test response plans to make sure each person knows their responsibilities in executing the plan. The better prepared your organization is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.

- **Execute planned exercises to ensure expectations are met** – It's important to execute planned exercises with realistic scenarios to test and validate response plans meet expectations.

- **Ensure response plans are updated** – Testing the plan (and execution during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned.

- **Coordinate with internal and external stakeholders** – It's important to make sure that your enterprise's response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.

APPENDIX 1



RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

Recover & Restore Access to Critical Information Assets

- **Communicate with internal and external stakeholders** – Part of recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need, but no inappropriate information is shared.

- **Ensure Disaster Recovery/Business Continuity plans are prepared for all critical information assets** – As with response plans, disaster recovery plans that address business continuity with predictable mode of operation after recovery are crafted and exercised. Be sure to update Disaster Recovery/Business Continuity plans with lessons learned to ensure expectation of business operations are met.

- **Ensure recovery plans are updated** – As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update recovery plans with lessons learned.

- **Manage public relations and CSS enterprise reputation** – One of the key aspects of recovery is managing the enterprise's reputation. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.

APPENDIX 2

	EIS			
Cyber Security Responsibilities	**CSS**	**CTO**	**DCS**	**Agency**
Vulnerability Management				
Tenable Vulnerability Scanning				
Determine/Assess deployment requirements	AR		C	CI
Provide hardware/software	AR		C	
Implement scanning	R		I	AR
Enterprise reporting	AR			CI
Vulnerability remediation	CI			AR
Public-Facing Vulnerability Scanning (CISA CyHy)				
Ensure all routable IP address space for the state is being scanned	AR		C	
Ensure all routable IP address space for agency is being scanned	A		C	R
Maintain agency distribution list (DL) for reporting, technical contact, and scan window restrictions	CI			AR
Maintain service with CISA	AR			CI
Vulnerability remediation	CI			AR
Tenable Web Application Scanning				
Determine/Assess deployment requirements	AR			CI
Provide hardware/software (where applicable)	AR		C	CI
Implement scanning	R			AR
Enterprise reporting	AR			
Vulnerability remediation	CI			AR
External Web Application Scanning (CISA WAS)				
Ensure all external web applications for the state are being scanned	AR			CI
Ensure all external web applications for agency are being scanned	A			R
Maintain agency distribution list (DL) for reporting, technical contact, and scan window restrictions	CI			AR
Maintain service with CISA	AR			CI
Vulnerability remediation	CI			AR
Penetration Testing				
Request Pen Testing	CI			AR
Define scope of pen testing activities	CI			AR
Provide resource availability (people, technology, documentation)	CI			AR
Conduct penetration testing activities	AR			CI
Reporting results	ARC			I

APPENDIX 2

	EIS			
Cyber Security Responsibilities	**CSS**	**CTO**	**DCS**	**Agency**
External Vulnerability Scanning and Validation Testing				
Request scanning	CI			AR
Provide assessment questionnaire and rules of engagement to agency	AR			CI
Respond & Return questionnaire & agree to rules of engagement to agency	CI			AR
Provide Resource Availability (people, technology, documentation)	CI			AR
Perform technical testing per the rules of engagement	AR			CI
Reporting results	AR			I
Cyber Threat Intelligence (CTI) Feeds				
Receive, store, aggregate, and disseminate information specific to cyber threats	AR		I	I
Apply to security operations where applicable	AR		R	R
Monitoring and Detection				
Security Information and Event Management (SIEM)				
Provide enterprise-level collection of security events for detection and after-the-fact incident response	AR			CI
Collect and apply threat intelligence (MS-ISAC, CISA, IBM X-Force, etc.)	AR			
Ensure SOC has contact information for agency notifications	CI			AR
Notify agencies of anomalous activity for action to be taken by agency	AR			CI
Network Security Monitoring and Analysis (MS-ISAC Albert)				
Maintain enterprise service with MS-ISAC (network threat detection at the perimeter)	AR			
Triage reported events and escalate to agencies where applicable	AR			CI
Provide event status and ticket closure requests to MS-ISAC	AR			CI
Phishing Email Analysis				
Report suspected phishing emails to the CSS SOC	CI			AR
Leverage M365 capabilities to assess/investigate reported email	AR			
DNS Filtering: Malicious Domain Blocking and Reporting				
Maintain service with the MS-ISAC	AR		CI	I
Configure agency DNS recursion for service integration	C		CI	AR
Incident Response				
Incident Response Coordination and Management				
Maintain Agency Incident Response (IR) Plan	CI			AR
Maintain Enterprise Incident Response (IR) Plan	AR			CI
Notify CSS SOC of any incident and provide updates	CI			AR
Handle statutory-required notifications to LFO	AR			CI
Assist and/or lead all levels of incident response as needed	AR			CI

APPENDIX 2

	EIS			
Cyber Security Responsibilities	**CSS**	**CTO**	**DCS**	**Agency**
Cyber Incident Tabletop Exercises (SOC)				
Provide opportunities for agencies to exercise Incident Response Plans and security incident decision-making capabilities	AR			CI
Exercise Agency Incident Response Plan	CI			AR
Enterprise Log Collection and Retention				
Identify security events to be collected (including retention)	CI		AR	I
Manage collection and retention of identified security events	AR		CI	
Awareness and Training				
Annual Security Training				
Provide the Annual Security Training in the LMS	AR			I
Provide access to the LMS and time for staff to take the training	I			AR
Security Awareness				
Provide Security Awareness material (including October Cybersecurity Awareness month)	AR			I
Support, disseminate, and publish the materials	CI			AR
Provide time for staff to participate	I			AR
Phishing Simulation Campaigns				
Onboarding	AR			CI
Deploy requirements	CI			AR
Deploy Phish Alert Button (PAB)	I		C	AR
Prevent spam filtering of simulation emails	I		C	AR
Phishing simulation templates	AR			I
Repeat responder awareness trainings	AR			I
Repeat responder remediation	I			AR
Risk Assessment				
Risk Assessment				
Ensure agencies are scheduled for bi-annual security risk assessments	AR			I
Coordinate and perform bi-annual Security Risk Assessment	AR			CI
Participate in the Security Risk Assessment	CI			AR
Remediate Security Risk Assessment findings	I			AR
Report 3rd party assessments to CSS	I			AR
Security Standards				
Cyber Security Plans (System Security, Agency Vulnerability Management and Incident Response)				
Create and maintain plan template	AR			IC
Develop and maintain plan	CI			AR
Validate plan	R			A

APPENDIX 2

	EIS			
Cyber Security Responsibilities	CSS	CTO	DCS	Agency
Security Standards (e.g. Statewide Standards & CIS Controls)				
IT Procurements/Renewal	RCI			AR
Business Case Security Review	CI			R
Review of 3rd party assessment (e.g. SOC2 Type2)	CI			AR
Audit/Assessment Remediation (e.g. POAMS)	RCI			AR
Network Security				
VPN - SSL and IPSec (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Proxy (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
SSL Termination (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Load Balancing (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I

APPENDIX 2

	EIS			
Cyber Security Responsibilities	**CSS**	**CTO**	**DCS**	**Agency**
Firewall (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Network Intrusion Detection and Prevention Systems (IDS/IPS) - perimeter				
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I

ENTERPRISE
information services