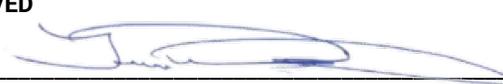


STATEWIDE PROCEDURE

	NUMBER 107-004-052_PR	SUPERSEDES New
	EFFECTIVE DATE February 17, 2026	PAGE NUMBER Pages 1 of 3
	REVIEWED DATE December 2, 2025	
DIVISION Enterprise Information Services	REFERENCE <ul style="list-style-type: none"> • ORS 276A.300, 276A.303, 276A.306, 276A.323, 276A.326, 276A.329, 276A.332, 276A.335 • OAR 125-800 • Cyber and Information Security Policy 107-004-052 	
POLICY OWNER Cyber Security Services		
SUBJECT Cyber and Information Security	APPROVED  <hr/> Terrence Woods, State Chief Information Officer	

PURPOSE

This procedure describes Enterprise Information Services (EIS) and agency responsibilities and actions that must be followed to comply with Statewide Policy 107-004-052, Cyber and Information Security.

APPLICABILITY

Refer to Statewide Policy 107-004-052, Cyber and Information Security, for applicability of this procedure.

EXHIBITS

- Cyber Security Services (CSS) [Assessment Schedule](#)
- Attachment A: CSS assessment finding and recommendations template
- Attachment B: Plan of Action and Milestones template
- Attachment C: Request to use offshore or foreign services

DEFINITIONS

Refer to Statewide Policy 107-004-052, Cyber and Information Security, for definitions.

PROCEDURE

ASSESSMENTS

<u>RESPONSIBILITY</u>	<u>STEP</u>	<u>ACTION</u>
Cyber Security Services (CSS)	1	Biennially, publish the CSS Assessment Schedule for two calendar years.
CSS	2	Send assessment engagement letter to agency head and agency IT leader for agency assessments in the upcoming quarter.
Agency head and agency IT leader	3	Attend CSS assessment engagement kickoff meeting with CSS.
CSS	4	Conduct assessment of agency security program.
Agency	5	Participate in CSS assessment of agency security program.
Agency head and agency IT leader	6	Attend CSS assessment exit briefing where CSS will deliver and discuss findings and recommendations with the agency.
CSS	7	Deliver final report to agency head and agency IT leader. (Attachments A)
Agency	8	Document plans of actions and milestones (POAM) and review at least monthly. Quarterly, deliver updated status of identifying and implementing remediations of findings and recommendations for outstanding critical and severe findings. Required POAM elements are defined in Attachment B.

Note: CSS may meet with the agency quarterly or as needed to provide consultation for remediation of findings.

ANNUAL TRAINING

<u>RESPONSIBILITY</u>	<u>STEP</u>	<u>ACTION</u>
CSS	1	Update and upload annual cybersecurity training in Workday.
Agency	2	Coordinate with CSS for scheduling training for users.
Chief Human Resource Office and agencies as applicable	3	Schedule training in Workday for all users.
Users	4	Complete annual cybersecurity training by December 31 of each year.

OFFSHORE AND FOREIGN SERVICES

<u>RESPONSIBILITY</u>	<u>STEP</u>	<u>ACTION</u>
Agency	1	Identifies need for services that can only be completed via offshore or foreign means.
Agency	2	Submit request to use offshore or foreign services to ESO.INFO@das.oregon.gov . (Attachment C)
CSS	3	Review request and make recommendations to State Chief Information Officer.
State CIO	4	Make determination on request.
CSS	5	Respond to agency request.

Attachment A: CSS assessment findings and recommendations template

Findings and Recommendations

Finding 1:

Finding Title		Finding Severity
FINDING TITLE		
CIS v8.0 Control		
CIS v8.0 Safeguard		
Artifact(s)		
References		

Finding Detail: Content.

Impact: Content.

Recommendation: Content.

Finding Title		Finding Severity
FINDING TITLE		
CIS v8.0 Control		
CIS v8.0 Safeguard		
Artifact(s)		
References		

Finding Detail: Content.

Impact: Content.

Recommendation: Content.

Attachment B: Plan of Action and Milestones (POAM) template

Plan Element	Plan Element Description	Input by	Input Example
POAM ID	Unique identifier for each POAM item	Agency	AGCY-0101
Safeguard	Applicable control	EIS	01.01
Finding	Brief description of finding	EIS	Agency’s consolidated asset inventory contained 2000 deployed items with nearly all expected attributes enumerated. Comparison of Defender and Tenable data with inventory found 350 assets not listed by agency.
Recommended remediation	Proposed remediation action	EIS	Agency should leverage its existing hardware asset management tools to develop and maintain an authoritative inventory of all authorized devices with the potential to receive, store, or process data. The inventory should include end-use devices (including mobile devices), network devices that the organization manages, IoT devices that the organization manages, and servers. For each device, the inventory should document the network address (if static), hardware (MAC) address, machine name, data asset owner, department, and whether the asset has been approved to connect to the network. The inventory should be reviewed for accuracy and updated, at a minimum, bi-annually. Once agency has documented its authorized hardware asset inventory, it should periodically compare output from its asset inventory tools to its authorized hardware asset inventory to review for unauthorized devices.
Criticality	Assigned criticality	EIS	Critical
Assessed score	Safeguard score at the time of assessment	EIS	59.6%
Issue Date	Date finding was issued	EIS	12/31/2024
Recommended remediation date	Calculated based on criticality	EIS	1/30/2025
Agency internal point of contact	Agency personnel assigned to POAM	Agency	Butch Cassidy
Remediation Plan	Overall plan to remediate deficiency	Agency	Create asset inventory

Plan Element	Plan Element Description	Input by	Input Example
Planned milestones	Planned milestones with project completion dates	Agency	(01) 2025-01-10: Extract full inventory of all systems. (COMPLETE) (02) 2025-01-15: Evaluate assets for approval. (COMPLETE) (03) 2025-01-31: Develop procedure to update inventory. (COMPLETE)
Internal comments	Internal agency comments	Agency	Working with BSA and ASCIO-supplied template.
Dependency	Description of any dependencies	Agency	
Support documents	List any supporting documents	Agency	AssetInventory.xlsx
Date closed	Date remediation actions completed	Agency	1/31/2025

Attachment C: Agency request to use offshore or foreign services

Date:

To: ESO.INFO@das.oregon.gov

From:

Re: Request to use offshore or foreign services

Agency:

Vendor name:

Vendor system:

Needed service(s):

Location of services(s):

Vendor explanation:

Agency director emergency declaration attached: Y / N