



**ENTERPRISE**  
information services

# Statewide Information Security Report

Ben Gherezgiher  
State Chief Information Security Officer

Joint Committee on Information  
Management and Technology

May 23, 2025





## Agenda

- ▶ Global Cybersecurity Industry Overview
- ▶ CSS Cyber Services Areas
- ▶ CSS Statewide Cyber Standards
- ▶ CSS Cyber Assessments
- ▶ CSS Projects and Initiatives
- ▶ CSS Cyber Awareness and Partnerships
- ▶ State and Local Cybersecurity Grant Program





## Global Cybersecurity Industry Overview

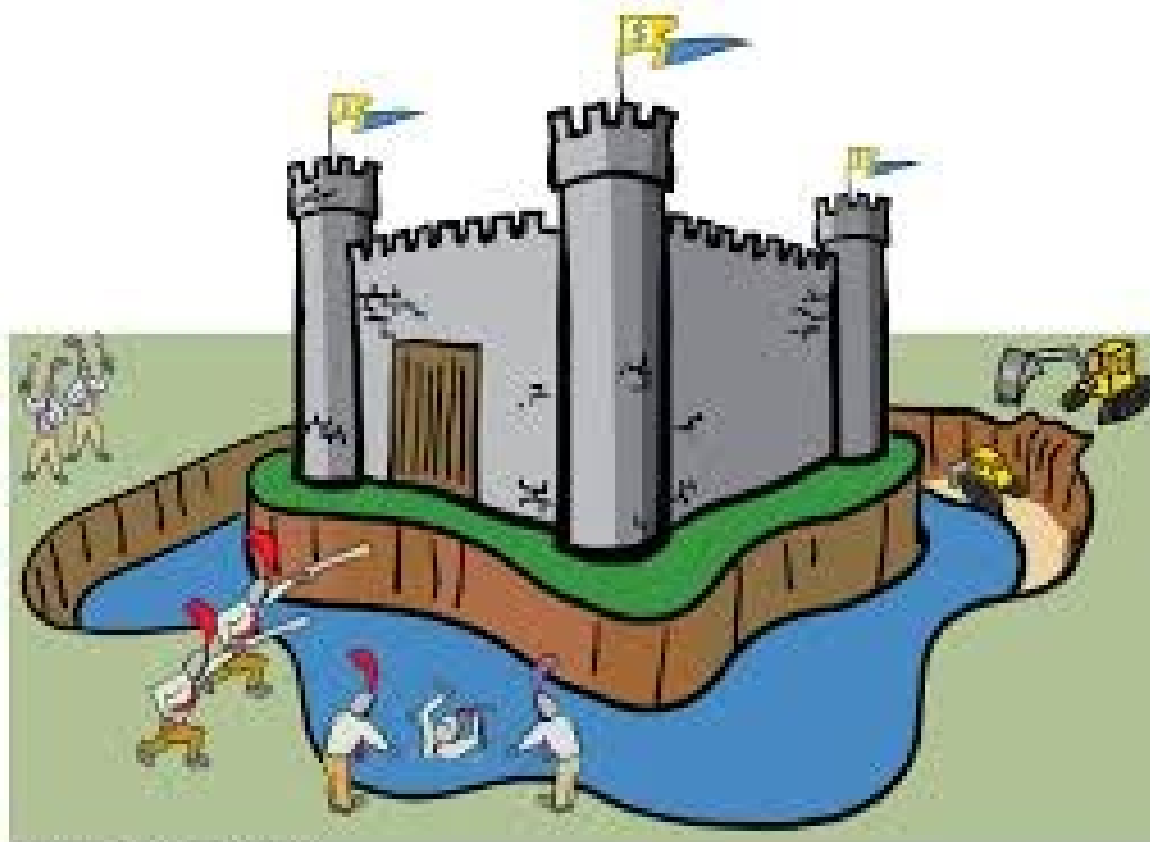


Illustration by Selma Corporation

- ▶ The days of castle-and-moat cybersecurity strategies are gone.
- ▶ Hackers are becoming too advanced, and threats exist both inside and outside of an organization's network.
- ▶ Zero Trust security model recognizes that these threats are vulnerabilities and must be addressed.
- ▶ Whether users are internal employees or external third parties, trust must be eliminated, and verification must become the new standard.



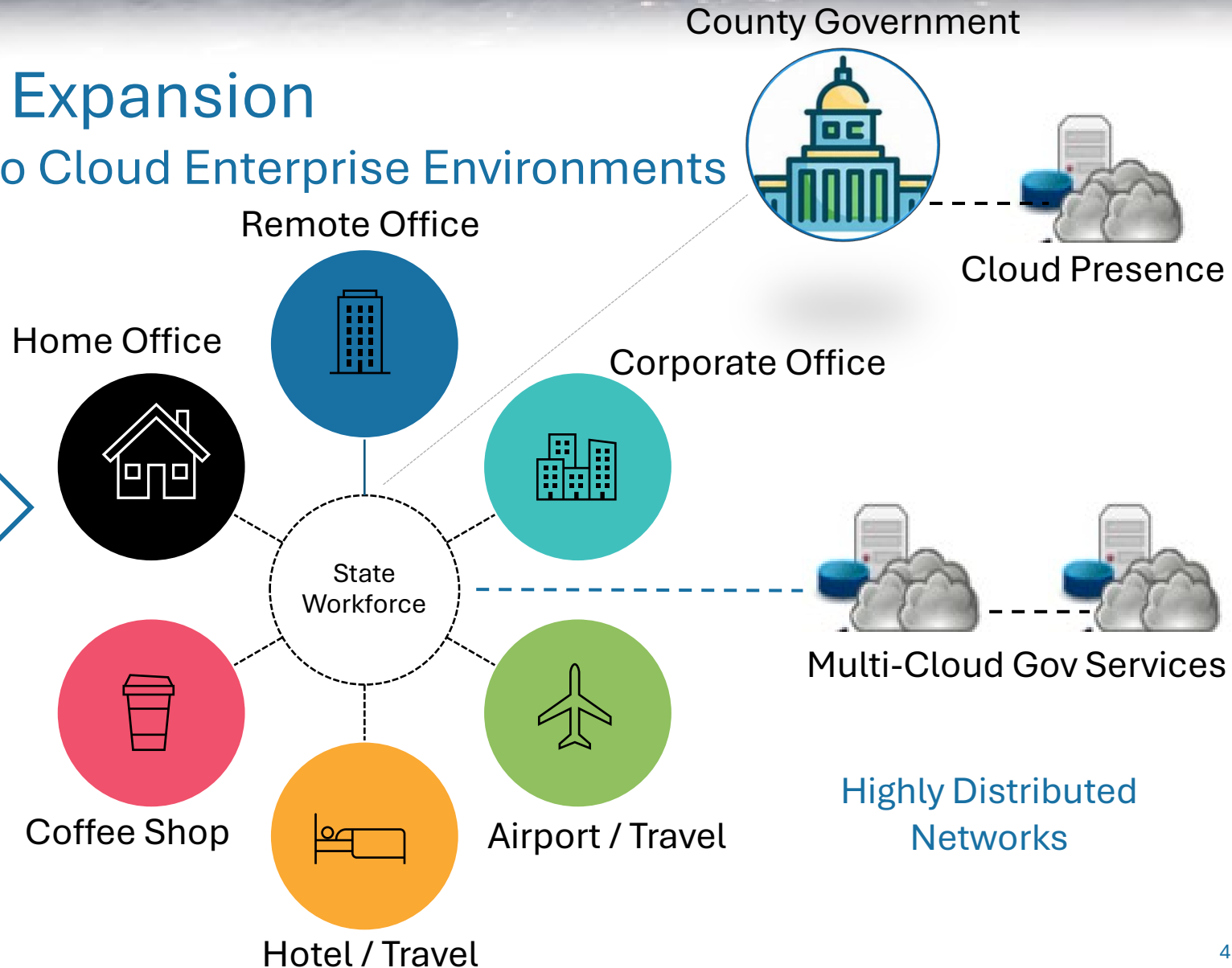


# Threat Landscape Expansion

## Multi-Cloud and Cloud to Cloud Enterprise Environments



Office Workers  
Localized Networks

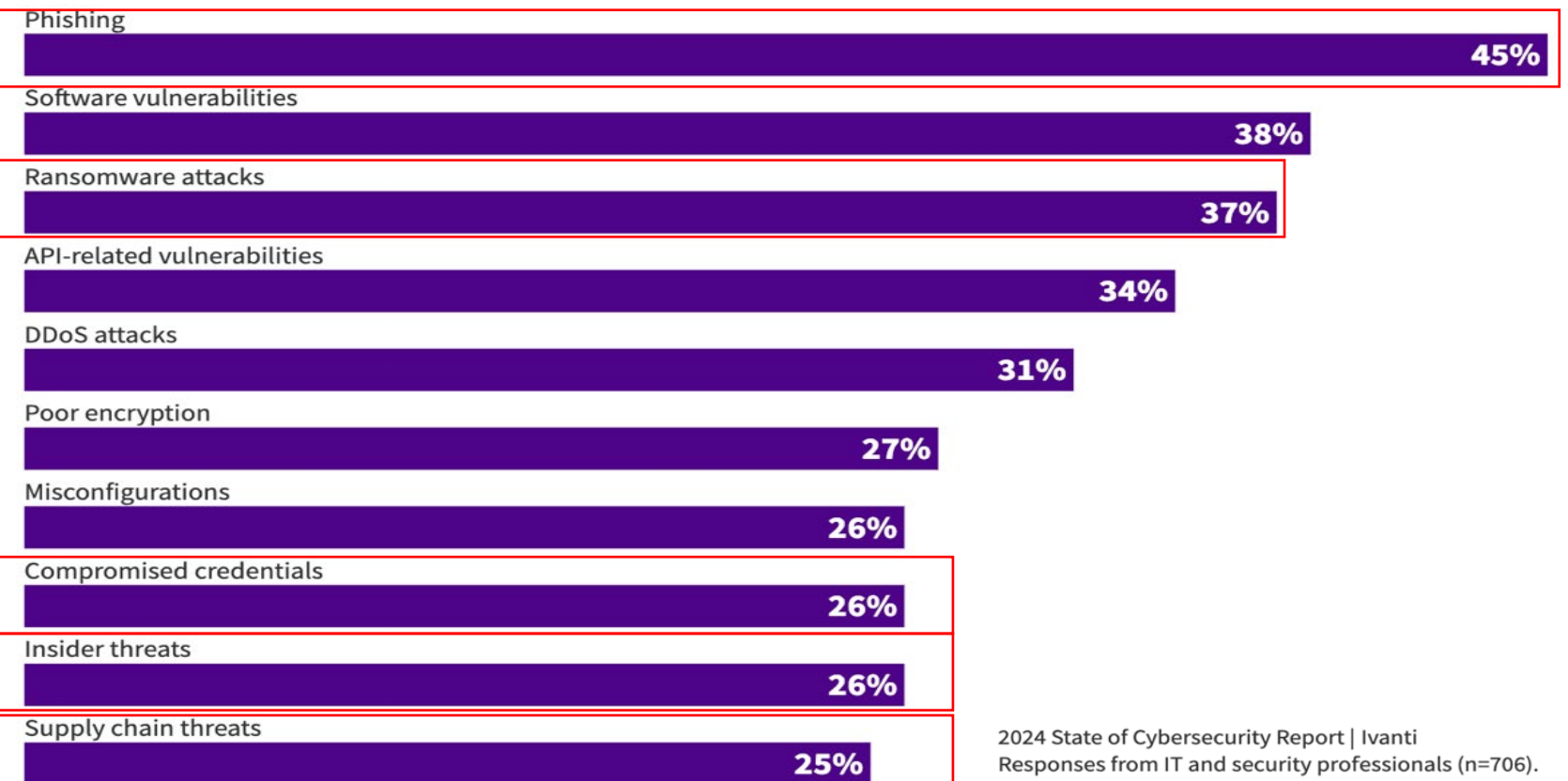




## Global Cybersecurity Industry Overview

- ▶ AI-powered threats loom large for security professionals

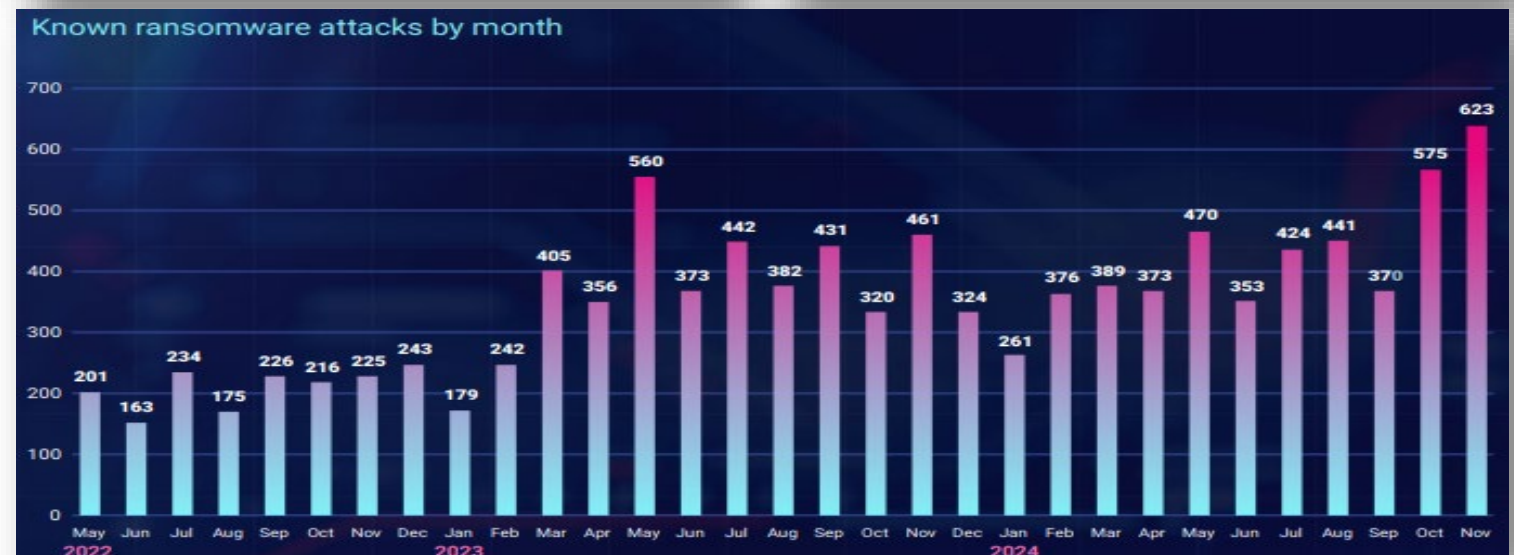
Q: Which of these threats will become more dangerous due to generative AI?





## Global Cybersecurity Industry Overview

### ► Ransomware attacks in 2024



Source: Threat down 2025  
state of malware report





## Global Cybersecurity Industry Overview

### ► Ransomware attacks in 2024

Top 5 ransomware groups by known attacks in 2024



Most ransomware attacks happen at night, between the hours of 1 am and 5 am, while IT staff are asleep



Source: Threat down 2025  
state of malware report





# Cyber Security Services

CSS Cyber Services Areas





## EIS – Cyber Security Services (CSS)



*Ben Gherezgiher*  
Chief Information  
Security Officer

Cyber Security Services brings together a full suite of enterprise cybersecurity services – governance, infrastructure, cloud security, operations, architecture - under a single, accountable enterprise focused program. This allows for end-to-end direction setting and execution for enterprise security. CSS personnel work collaboratively with Data Center Services domain teams to deliver secure solutions to our customers.

-  Cybersecurity Administration
-  Security Architecture
-  Security Governance, Risk and Compliance
-  Network Security Services (Enterprise)
-  Security Assessment
-  Security Operations Center (SOC)





## CSS – Enterprise Security Operations Center (ESOC)

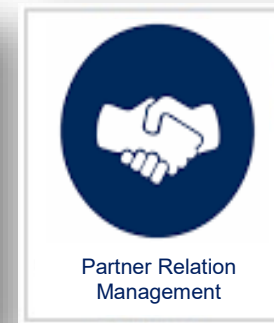




## CSS – Network Security Services (Net-Sec)



## Cybersecurity Governance



## Cybersecurity Assessment



## Cyber Architecture

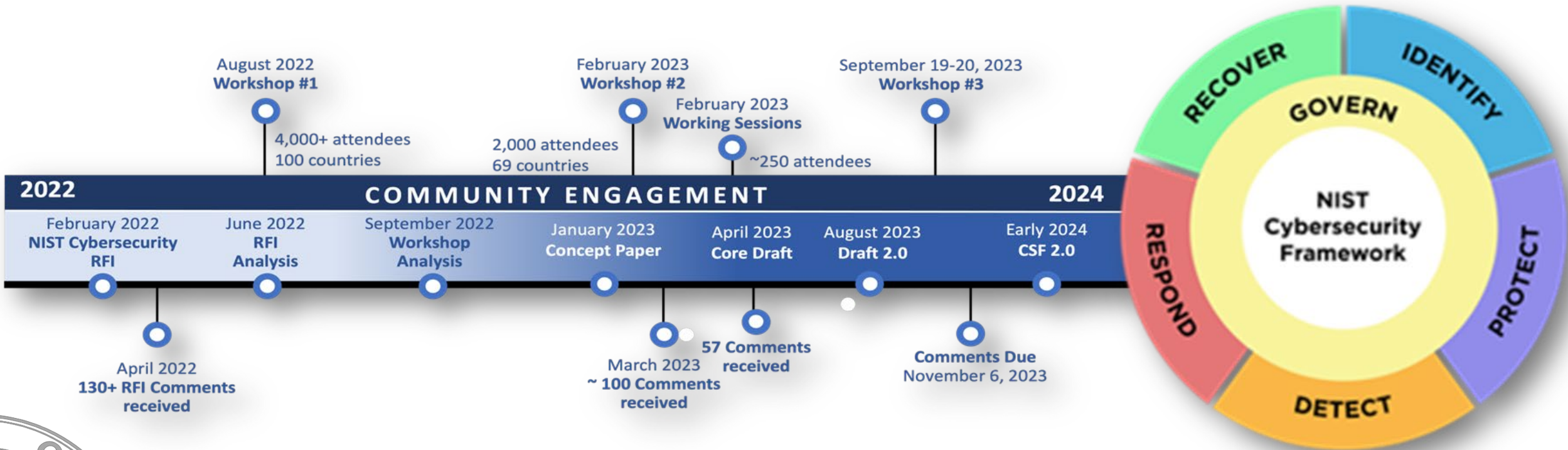


## CSS Statewide Cyber Standards





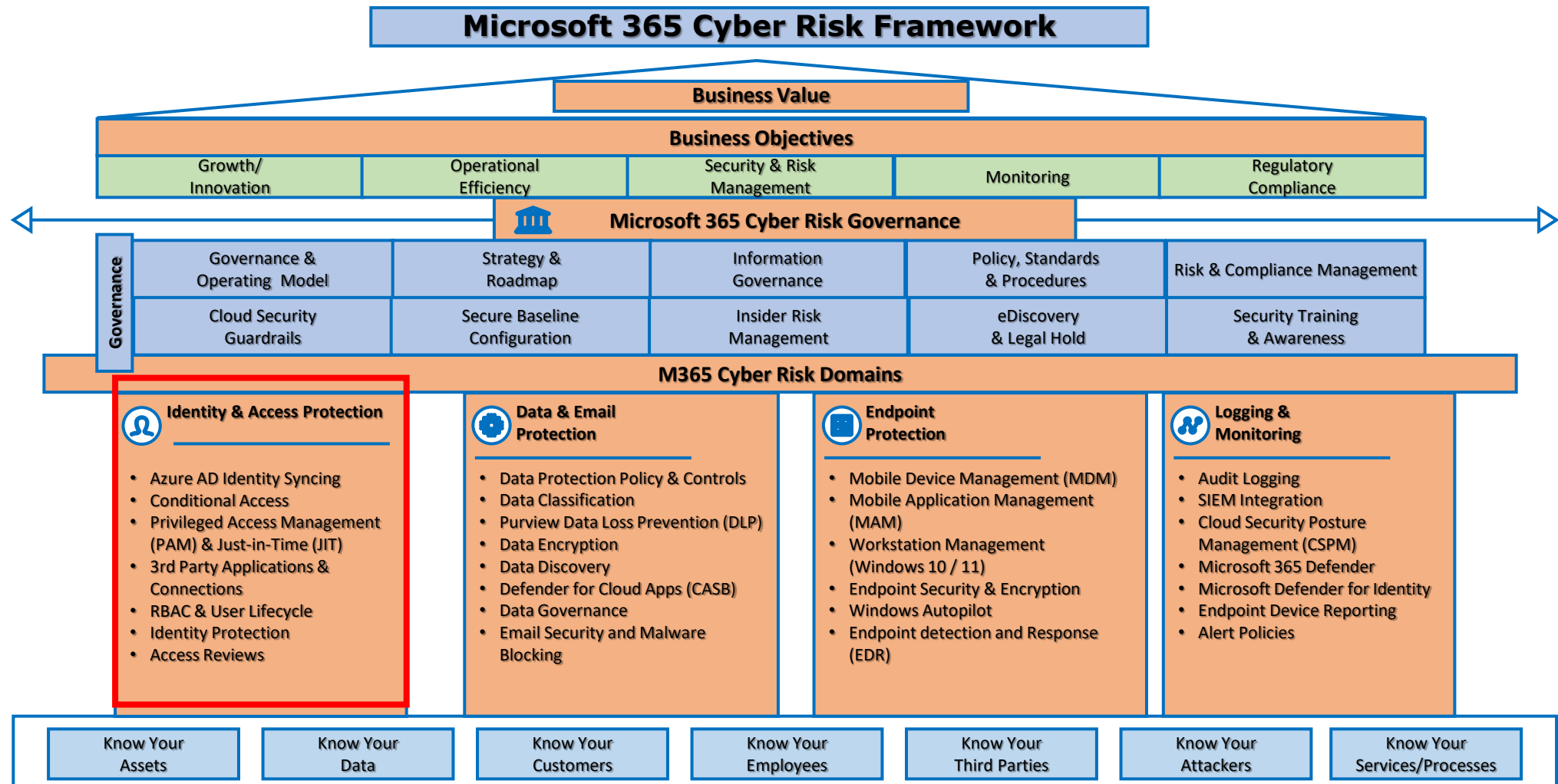
## Adoption of NIST Framework 2.0



NIST: National Institute of Standards and Technology



## Cloud M365 Security Framework





## NIST 800-53 Security Control Families, Release 5

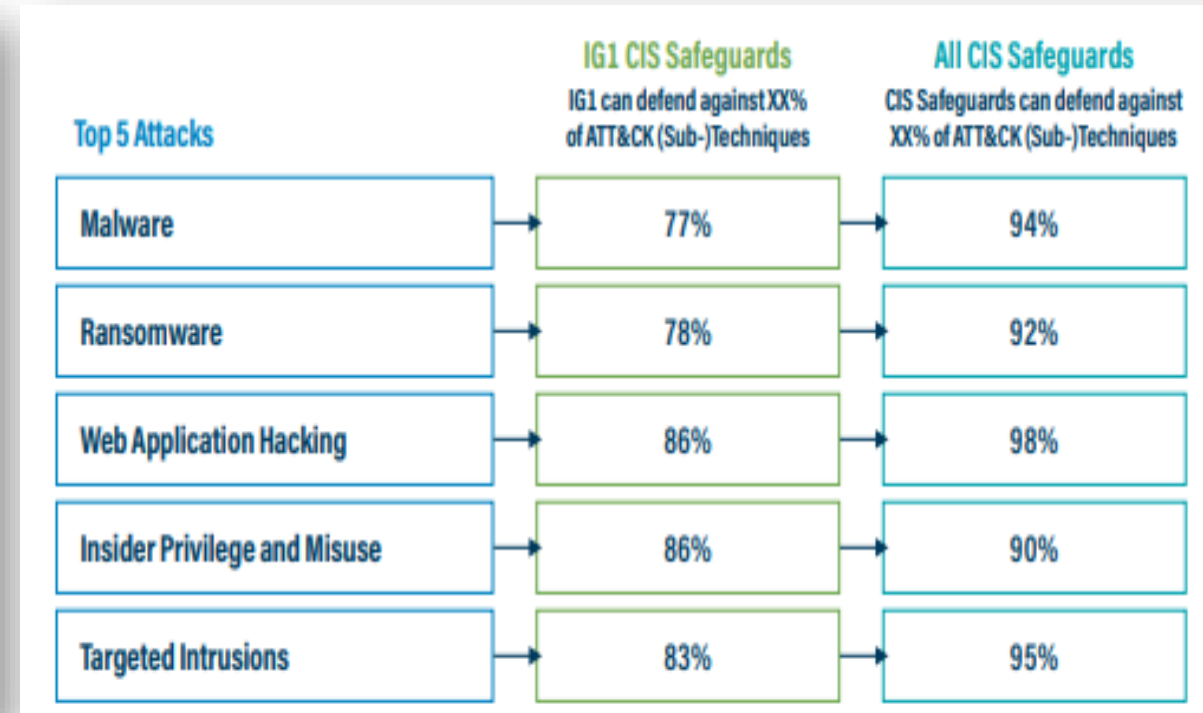
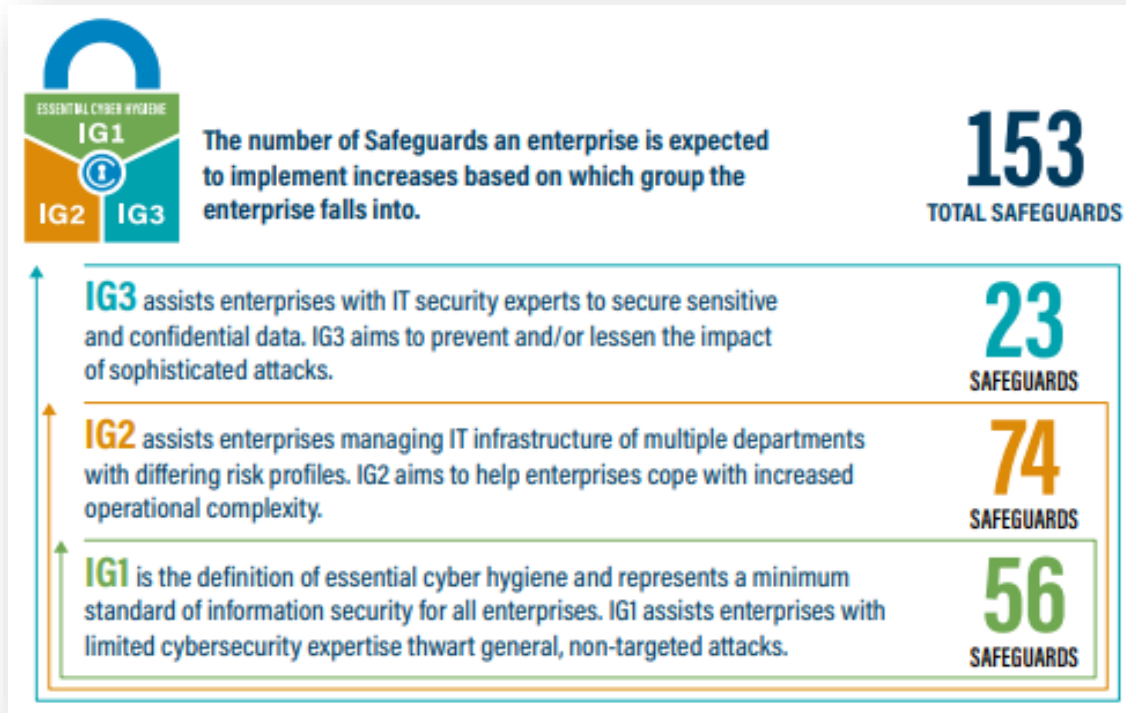
Code	Description
AC	Access Control
AT	Awareness And Training
AU	Audit And Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection

Code	Description
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management





## Value of Cyber Assessments



Complete implementation of Center for Internet Security V8.0 IG1 controls shows an average of 82% defense capability achievement against the top 5 attacks listed above.



## CSS Cyber Assessments





## Cybersecurity Assessments 2023-2025

### ► Assessments Completed

#### **July - December 2023**

- 31 CIS control assessments
- 1 web app assessment
- 3 CISA RVAs

#### **January - December 2024**

- 14 CIS control assessments
- 2 web app assessments
- 4 CISA RVAs

### ► Assessment Activity Targets for January – June 2025:

- 25 CIS control assessments
- 4 web app assessments
- 4 CISA RVAs

CIS – Center for Internet Security

CISA – Cybersecurity and Infrastructure Security Agency

RVA – Risk and Vulnerability Assessment





# Cybersecurity Assessments 2023-2025

## Ad Hoc Services

- ▶ AD Attack Path Analysis (BloodHound)
- ▶ Threat Modeling
- ▶ Vulnerability Analysis
- ▶ Open-Source Intelligence (OSINT) Analysis
- ▶ Known Exploited Vulnerability Enumeration
- ▶ Adversary Emulation
- ▶ Penetration Testing
- ▶ Cloud Security Analysis



## CSS Projects and Initiatives





## Projects – In Flight

- ▶ Microsoft 365 Security Enhancements
- ▶ Network and Security Modernization Program
- ▶ Enterprise Mobile Security

## Initiatives – In Flight

- ▶ Integrated Risk Management Portal
- ▶ Enterprise Identity and Access Management Roadmap
- ▶ Modernize Network Threat Detection and Response (NDR)
- ▶ 24/7 managed service implementation for the ESOC





**ENTERPRISE**  
information services

# Cyber Security Services

## Proactive Cyber Threat Monitoring Capability

### State Cybersecurity Services

Secure Enterprise Monitoring



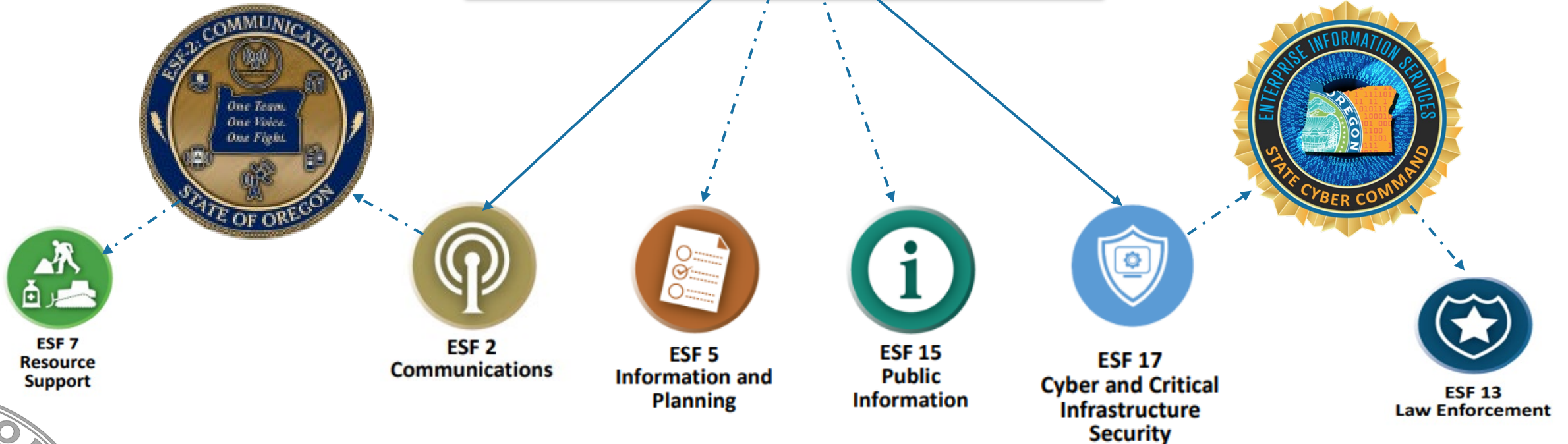
Landing Page	SolarWinds Active Sessions	Global Threats Last 7 Days	Global Threat Map	Hybrid Domain Join Stats	Cyber Security Assessments	Devices Current State
Devices History	Onboarding Trend	Recommendations Compliance	Oregon County Cyber Outlook	MDM Totals	Agency Mobile Inventory	Agency Inventory - Intune
Phishing	Threat Alerts	Response Times	Methods	Threat Anomalies	Threat by Service	Analyst Activity
Analyst Performance	CISA WebApp Vul Scan	NetSec	VPN Usage	Statewide Enterprise Assets	Partnership Engagements	





**ENTERPRISE**  
information services

# Cyber Security Services



## EIS ESF 17 Emergency Roles



Cyber Security Services

CSS Cyber Awareness and Partnerships





## Cybersecurity Awareness Campaign

**ENTERPRISE**  
information services  
CYBER SECURITY SERVICES

**RANSOMWARE AWARENESS CAMPAIGN**

July 2023 | Volume 1

IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER



### What is Ransomware? & How Does it Happen?

Ransomware is a type of malicious software that encrypts the data on a victim's device or network and demands a ransom for its decryption. The ransom is usually paid in cryptocurrency or other untraceable forms of payment.

If the ransom is not paid within a specified time, the data may be permanently deleted or exposed to the public. Ransomware attacks can cause significant damage to individuals, businesses, and organizations by disrupting their operations, compromising their privacy and security, and extorting large sums of money.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's been infected with malware. Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

**GOAL:** The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm  
» October 13, 2023 9am – 10am

**SOME COMMON RANSOMWARE VECTORS OF ATTACK ARE:**

- » Phishing emails with malicious attachments or links
- » Exploiting unpatched vulnerabilities in software or systems
- » Remote desktop protocol (RDP) compromise or brute force
- » Drive-by downloads from compromised websites
- » Network propagation through shared drives or devices



For more information scan the QR code or visit our website  
[ransomwareinfo.oregon.gov](https://ransomwareinfo.oregon.gov)



ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

**ENTERPRISE**  
information services  
CYBER SECURITY SERVICES

**RANSOMWARE AWARENESS CAMPAIGN**

August 2023 | Volume 2

IDENTIFY



### Identify

Identify, the first of five core functions within what is called the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), is widely adopted by organizations as a flexible and adaptable tool for improving their cybersecurity posture. It also provides a structured approach to assessing and managing cybersecurity risks, regardless of an organization's size, industry, or sector.

CSF consists of five core functions: Identify, Protect, Detect, Respond and Recover. By using the CSF, an organization can assess its current cybersecurity posture, identify gaps, and prioritize actions to improve its resilience against ransomware and other cyber threats. Organizations can also use it to align their cybersecurity efforts with their business goals, prioritize investments, and communicate their cybersecurity practices to stakeholders effectively.



**Cybersecurity Framework**

**GOAL:** The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm  
» October 13, 2023 9am – 10am

**IDENTIFY IS ESSENTIAL FOR:**

- » Understanding your computing environment
- » Assessing risks to the protection of customer data
- » Determining the resiliency of services that rely on technology
- » Creating disaster recovery or business continuity plans
- » Preparedness when responding to a cyber security incident



For more information scan the QR code or visit our website  
[ransomwareinfo.oregon.gov](https://ransomwareinfo.oregon.gov)



ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

**ENTERPRISE**  
information services  
CYBER SECURITY SERVICES

**RANSOMWARE AWARENESS CAMPAIGN**

August 2023 | Volume 3

PROTECT



### Protect

Protect is the second of five core functions within the Cybersecurity Framework (CSF). The function of protect is to limit or contain the impact of ransomware events. There are three categories within protect that we will cover.

**Identity Management & Access Control** – The purpose of Identity Management & Access Control is to limit who has access to information/systems and verify they are who they say they are. These include:

- Ensuring user accounts with administrator-level privileges are never used to browse the internet or access email. Employees should be directed to use a regular computer account for daily work.
- Ensuring unused or stale computer accounts are regularly reviewed and disabled or deleted.
- Requiring the use of long complex passwords/passphrases with a regular password reset interval.
- Utilizing Multi-Factor Authentication (MFA) on cloud-based accounts, when possible.

**Awareness & Training** – Because most ransomware events start by exploiting an organization's users, security awareness training can be highly effective in mitigating potential ransomware events. These include:

- Phishing awareness training – Teach employees how to recognize suspicious emails and report them.
- Social engineering training – Train employees how to recognize attacks that try to trick them into sharing sensitive information by using manipulation, impersonation and persuasion.

**GOAL:** The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm  
» October 13, 2023 9am – 10am

**PROTECT IS ESSENTIAL FOR:**

- » Understanding the need for different technologies to help mitigate ransomware events
- » Stopping ransomware from reaching your users
- » Blocking harmful or malicious content before they reach your systems
- » Limiting the effect and impact of ransomware events



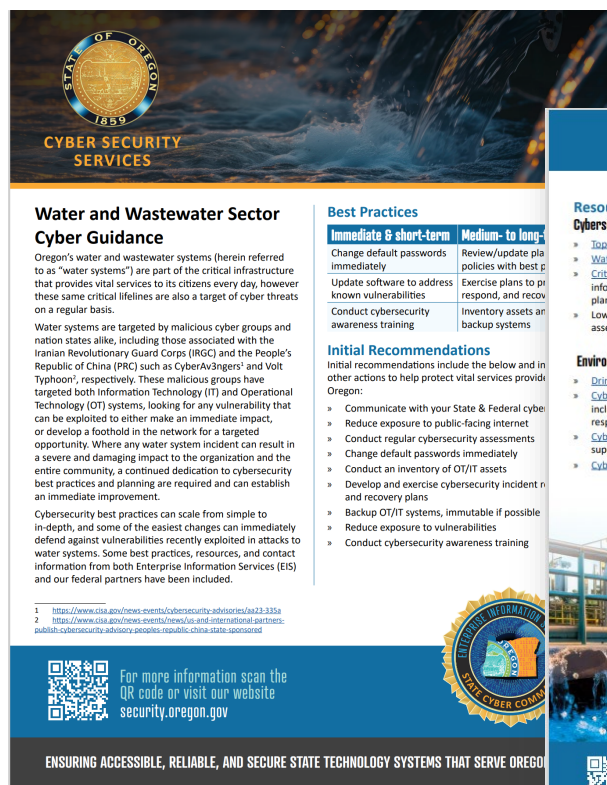
For more information scan the QR code or visit our website  
[ransomwareinfo.oregon.gov](https://ransomwareinfo.oregon.gov)



ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.



## Water and Wastewater Sector Cyber Guidance



**CYBER SECURITY SERVICES**

### Water and Wastewater Sector Cyber Guidance

Oregon's water and wastewater systems (herein referred to as "water systems") are part of the critical infrastructure that provides vital services to its citizens every day, however these same critical lifelines are also a target of cyber threats on a regular basis.

Water systems are targeted by malicious cyber groups and nation states alike, including those associated with the Iranian Revolutionary Guard Corps (IRGC) and the People's Republic of China (PRC) such as CyberAv3ngers<sup>1</sup> and Volt Typhoon<sup>2</sup>, respectively. These malicious groups have targeted both Information Technology (IT) and Operational Technology (OT) systems, looking for any vulnerability that can be exploited to either make an immediate impact, or develop a foothold in the network for a targeted opportunity. Where any water system incident can result in a severe and damaging impact to the organization and the entire community, a continued dedication to cybersecurity best practices and planning are required and can establish an immediate improvement.

Cybersecurity best practices can scale from simple to in-depth, and some of the easiest changes can immediately defend against vulnerabilities recently exploited in attacks to water systems. Some best practices, resources, and contact information from both Enterprise Information Services (EIS) and our federal partners have been included.

**Best Practices**

Immediate & short-term	Medium- to long-term
Change default passwords immediately	Review/update policies with best practices
Update software to address known vulnerabilities	Exercise plans to respond, and recovery
Conduct cybersecurity awareness training	Inventory assets and backup systems

**Initial Recommendations**

Initial recommendations include the below and in other actions to help protect vital services provided in Oregon:

- Communicate with your State & Federal cyber
- Reduce exposure to public-facing internet
- Conduct regular cybersecurity assessments
- Change default passwords immediately
- Conduct an inventory of OT/IT assets
- Develop and exercise cybersecurity incident response and recovery plans
- Backup OT/IT systems, immutable if possible
- Reduce exposure to vulnerabilities
- Conduct cybersecurity awareness training

**Resources**

**Cybersecurity & Infrastructure Security Agency (CISA)**

- Top Cyber Actions for Securing Water Systems | CISA
- Water and Wastewater Cybersecurity | CISA
- Critical Infrastructure Sectors page, that includes sector information and resources to include a sector-specific plan, working groups, and additional publications.
- Low- and no-cost services, including exercises, assessments, training, and more

**Environmental Protection Agency (EPA)**

- Drinking Water and Wastewater Resilience page
- Cybersecurity for the Water sector page which includes cybersecurity assessments, planning, training, response, and funding resources and information.
- Cybersecurity Technical Assistance Program that will support organizations in conducting an asset inventory.
- Cybersecurity Incident Action Checklist

**Oregon EIS Cyber Security Services (CSS)**

- Statewide guidance, policies, standards, and more be found at our website <https://security.oregon.gov>

**Additional Resources**

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Water Information Sharing and Analysis Center (WISAC) is the only all-threats security information for the water and wastewater sector

**Incident contact information**

**CISA**  
[report@cisa.gov](mailto:report@cisa.gov) | 888-282-0870 | [Report Site](https://www.cisa.gov/report)

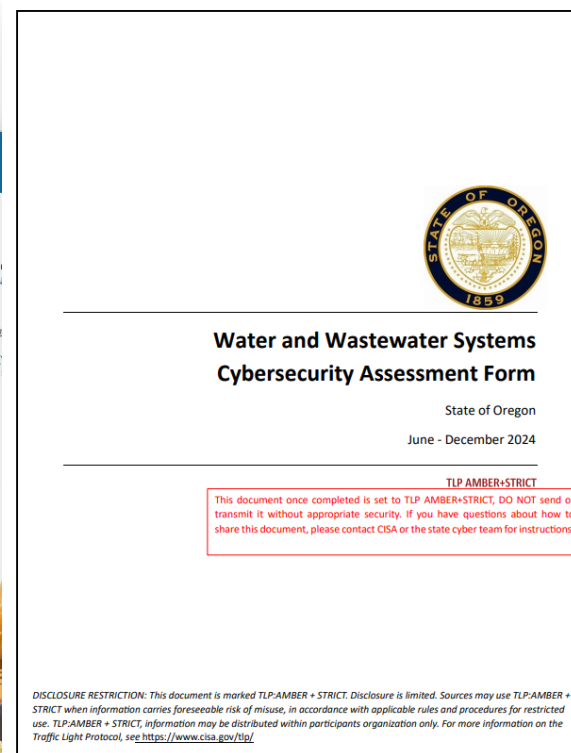
**EIS Security Operations Center (SOC)**  
[iso.soc@das.oregon.gov](mailto:iso.soc@das.oregon.gov) | 503-378-5930 | [CSS Site](https://www.cisa.gov/tip/)

**Footnote:**

1 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>  
2 <https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored>

For more information scan the QR code or visit our website [security.oregon.gov](https://security.oregon.gov)

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.



**Water and Wastewater Systems Cybersecurity Assessment Form**

State of Oregon  
June - December 2024

**TLP AMBER+STRICT**

This document once completed is set to TLP AMBER+STRICT, DO NOT send or transmit it without appropriate security. If you have questions about how to share this document, please contact CISA or the state cyber team for instructions.

**DISCLOSURE RESTRICTION:** This document is marked TLP-AMBER + STRICT. Disclosure is limited. Sources may use TLP-AMBER + STRICT when information carries foreseeable risk of misuse, in accordance with applicable rules and procedures for restricted use. TLP-AMBER + STRICT, information may be distributed within participants organization only. For more information on the Traffic Light Protocol, see <https://www.cisa.gov/tlp/>



**Water Sector Cyber Security Action Plan**

June 18, 2024



## Partnership Building Across Oregon





Cyber Security Services

# State and Local Cybersecurity Grant Program





# State and Local Cybersecurity Grant Program Update

(as of April 21, 2025)

Total number of federal awards: 3

Total number of subrecipient projects: 59 (+42 pending)

Total funds managed: \$9,035,602

FFY 22: \$2,988,286

- State match: Cost share waived
- Local projects: 57

FFY 23: \$6,047,316

- State match: Cost share waived
- Local projects: 2 (42 submitted to CISA pending approval)

FFY 24: \$6,513,815

- Federal share: \$4,559,670
- State match: \$1,954,145 cost share waiver requested





**ENTERPRISE**  
information services

# Cyber Security Services

# Thank you

Shirlene A Gonzalez

Legislative Director

[shirlene.a.gonzalez@das.oregon.gov](mailto:shirlene.a.gonzalez@das.oregon.gov)

