Enterprise Information Services Security Report

Ben Gherezgiher, State Chief Information Security Officer

Joint Legislative Committee on Information Management & Technology

May 31, 2023

ENTERPRISE information services

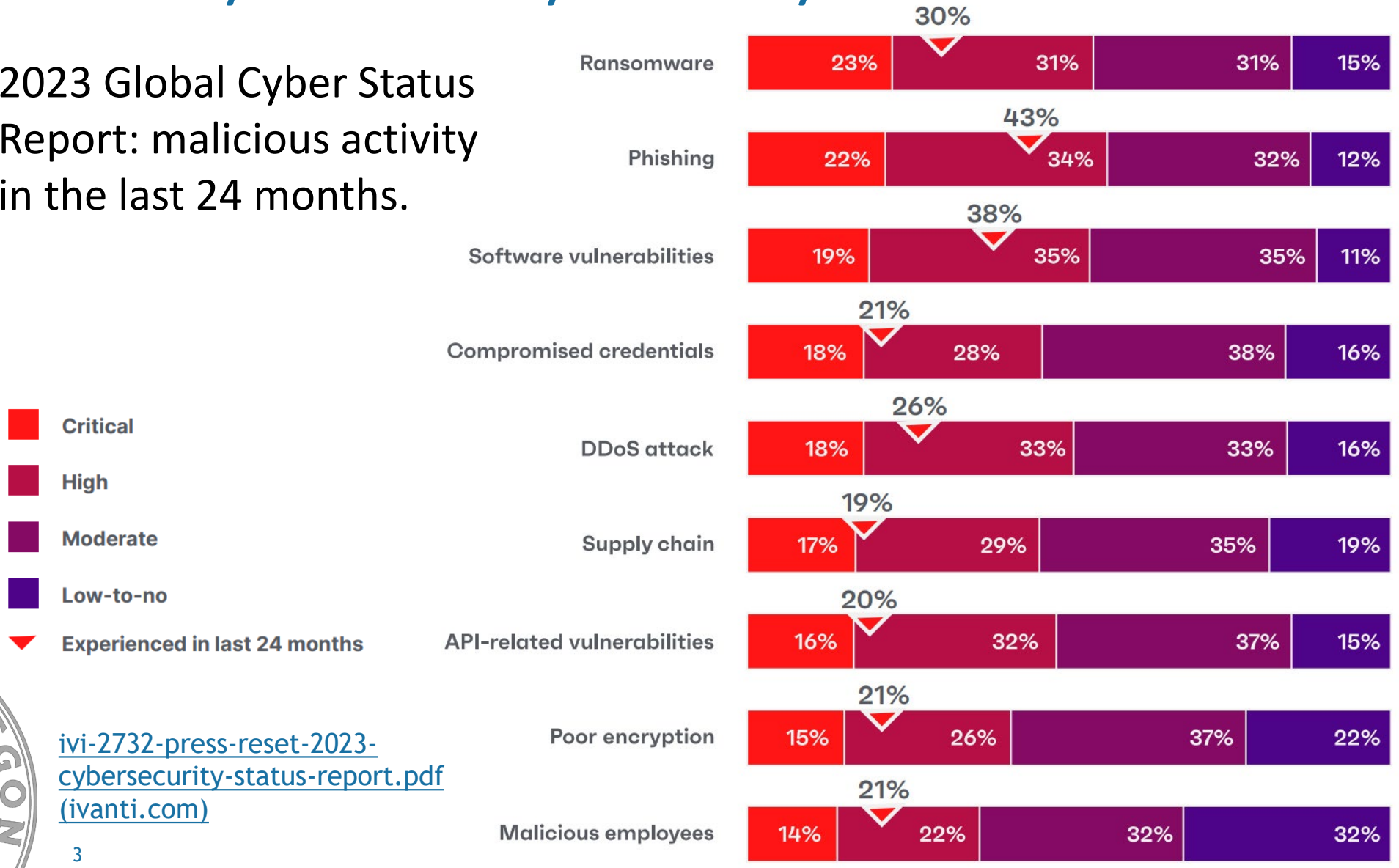
Agenda

- Global Cybersecurity Industry Overview
- EIS Cyber Security Services (CSS) Organization Overview
- CSS Service Catalog
- NIST Framework Details
- CSS Goals
- CSS Services
- CSS High Level Metrics
- CSS Projects & Initiatives
- IIJA State and Local Government Cybersecurity Grant Program Update

ENTERPRISE information services

Global Cybersecurity Industry Overview

2023 Global Cyber Status Report: malicious activity in the last 24 months.

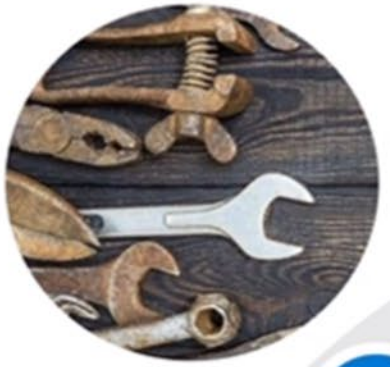


[ivi-2732-press-reset-2023-cybersecurity-status-report.pdf (ivanti.com)]

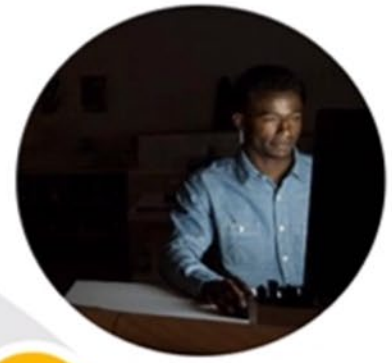
Global Cybersecurity Industry Overview (cont.)

Frequency and cost of cybersecurity attacks on government is rising

Conventional cybersecurity tools have not kept pace



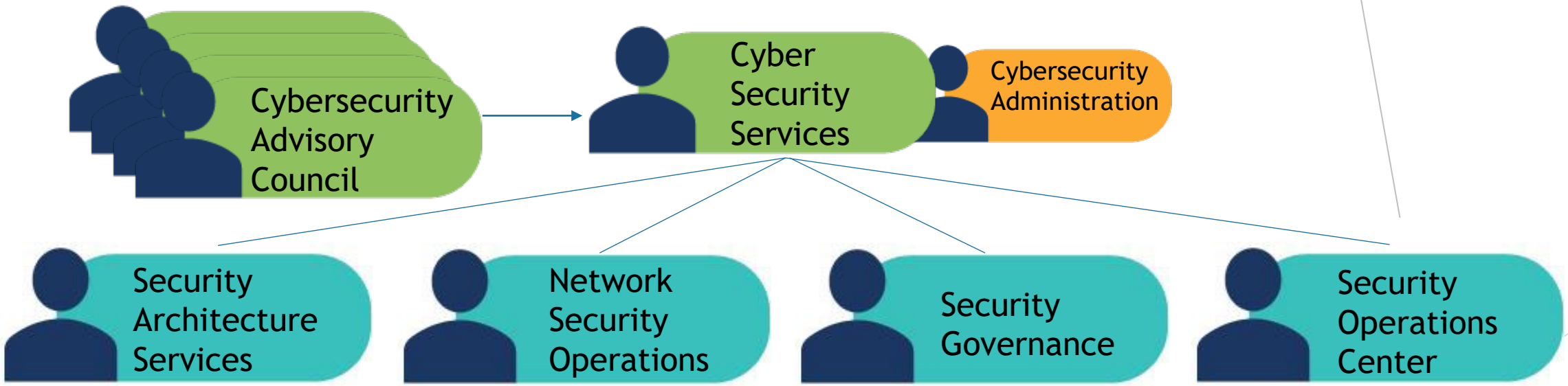
Cybersecurity skills and resources are constrained



Shields Up | CISA

ENTERPRISE information services

EIS Cyber Security Services Organization Overview



ENTERPRISE information services

CSS Service Catalog

Cyber Security Services Service Catalog begins to drive value across the state enterprise by establishing scope of services and accountability. Furthermore, it clarifies the level of service by declaring time estimates to deliver the cataloged services.

Cybersecurity is a business-driven service that is focused on Identifying mission critical information assets, diligently Protecting the assets by detecting threats against them, and implementing mitigating controls that defend against internal and external threat actors. Responding to compromises and Recovering services back to operation via predictable, demonstrated set of activities. ***~~NIST FRAMEWORK~~***

(National Institute of Standards and Technology)

ENTERPRISE information services

NIST Framework Details

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.

IDENTIFY

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

PROTECT

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

RESPOND

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

DETECT

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

ENTERPRISE information services

Cyber Security Services Goals

- **Identify:** Implement cybersecurity risk management measures and risk management processes to reduce cybersecurity risks across the enterprise.
- **Protect:** Develop and implement enterprise safeguards to reduce risk and increase awareness and resiliency.
- **Detect:** Develop tools and processes to accelerate notification of cybersecurity threats; defeat threat actors before they have impact on state information assets.
- **Respond:** Consistently respond to anomalies and suspected events.
- **Recover:** Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.

CSS Services

ENTERPRISE information services

CSS – State Security Operations Center (SOC)

Core Services

ENTERPRISE information services

CSS – Network Security Operations (Net-Sec)

Core Services

ENTERPRISE information services

CSS – Security Services Continued

Cybersecurity Governance

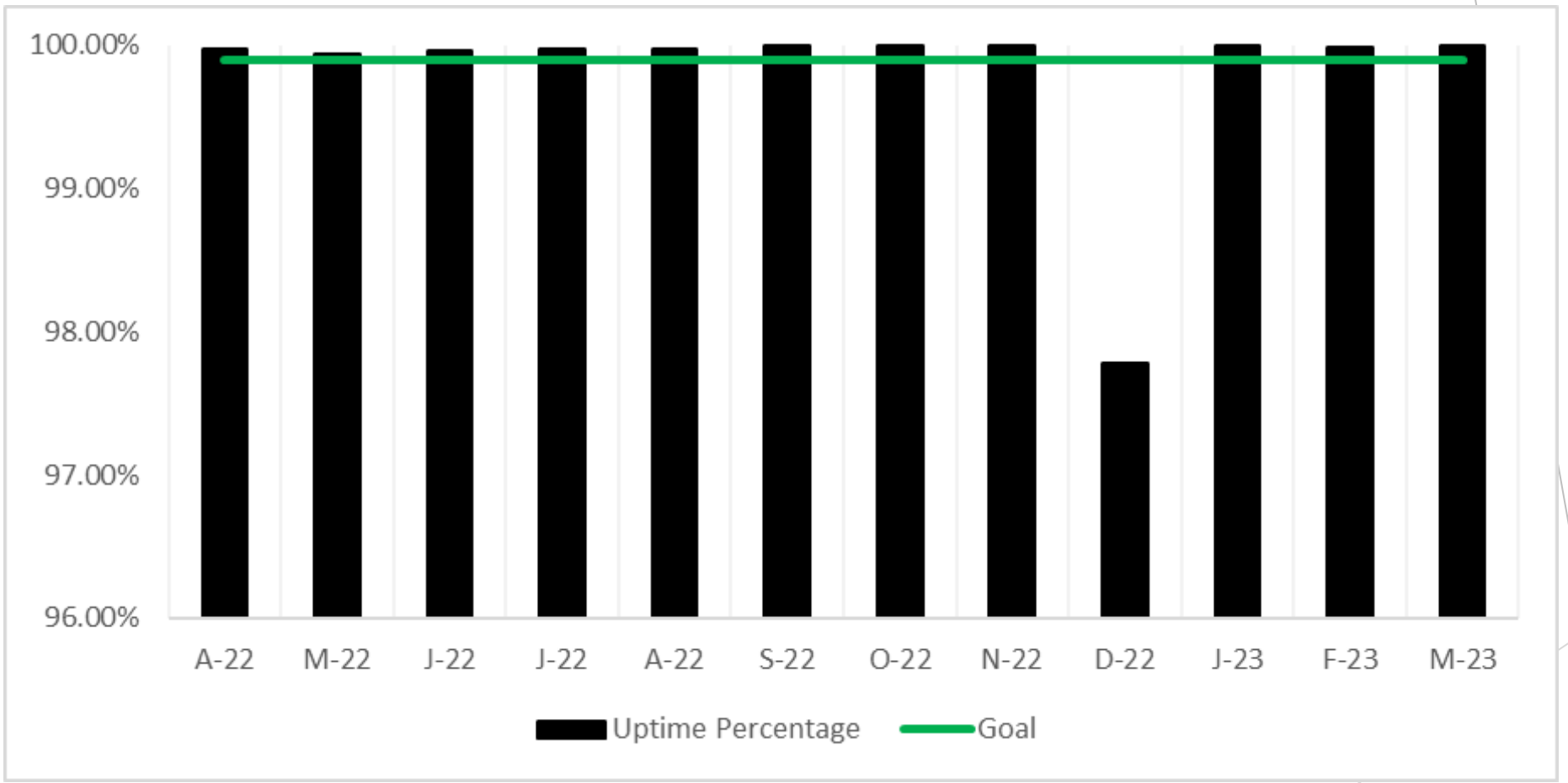
Cybersecurity Assessment

Cybersecurity Miscellaneous Services

ENTERPRISE information services

CSS High Level Metrics

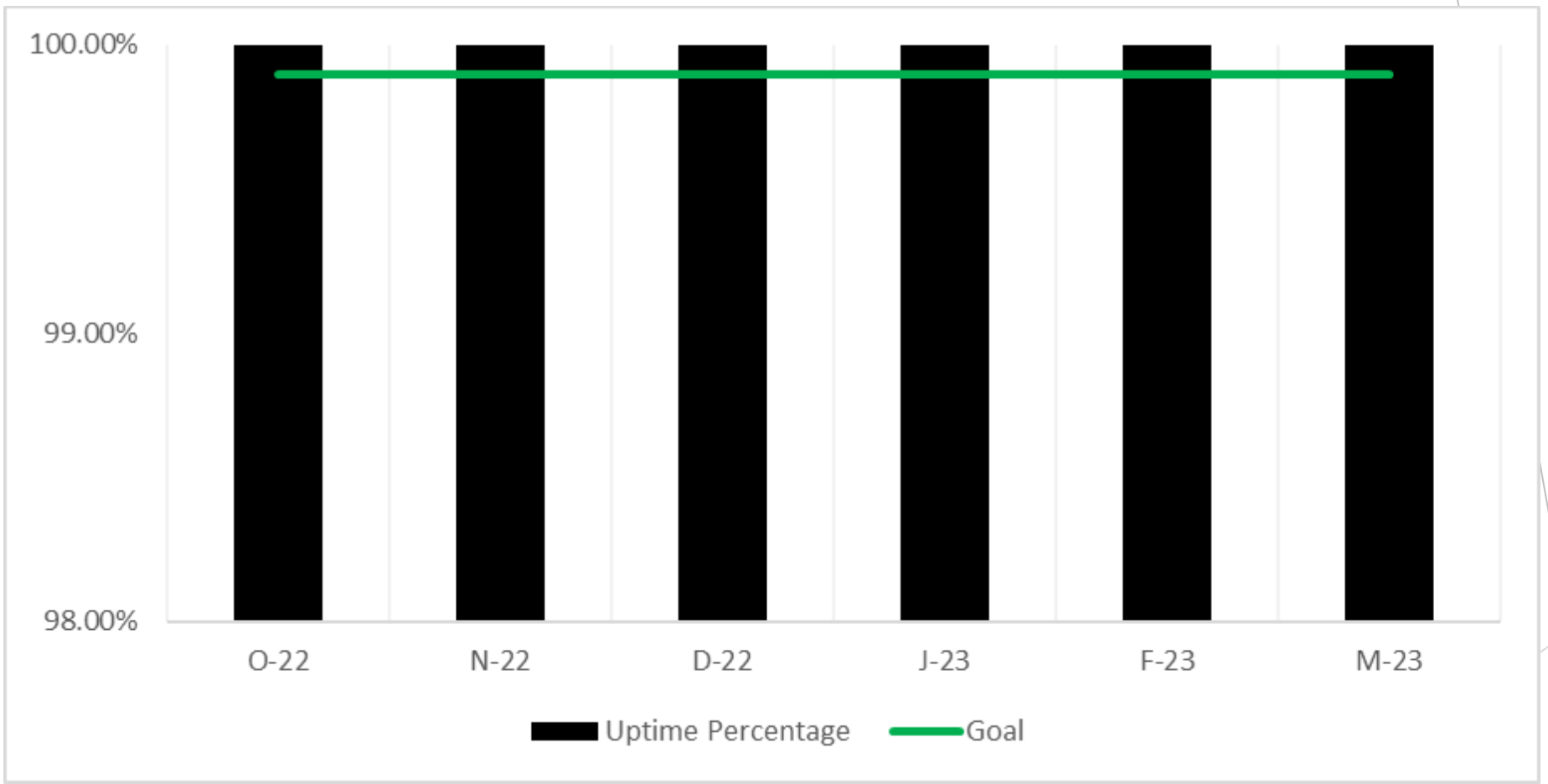
CSS High Level Metrics – Network Security Services



Network Security Uptime – Perimeter

ENTERPRISE information services

CSS High Level Metrics – Network Security Services



Network Security Uptime – Border

ENTERPRISE information services

CSS High Level Metrics – Cybersecurity Assessments

- **Assessment Activity Statistics:**

Since fall of 2018

- 73 Center for Internet Security (CIS) control assessments
- 11 risk assessments

Calendar year 2022

- 20 CIS control assessments
- 8 web application security assessments
- 1 targeted risk assessment

- **Assessment Activity Targets for 2023:**
  - 43 agencies, boards and commissions in scope
  - Use of CIS Controls V8.1 with cloud companion

ENTERPRISE information services

CSS – Projects & Initiatives

ENTERPRISE information services

Projects – In Flight

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

Initiatives – In Flight

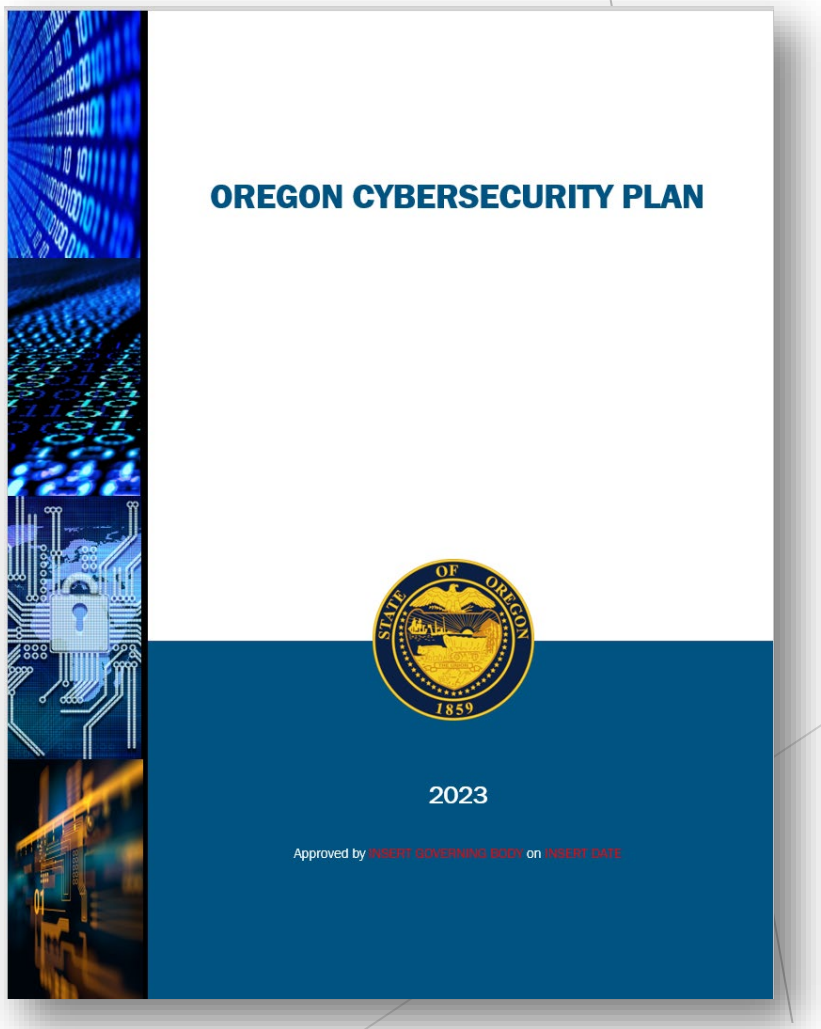
- Integrated Risk Management Portal
- Contracted Services
  - Enhance efficiency of network security services
  - Identity and Access Managements Baseline Strategy
  - Enhance Efficiency of Security Operations Center (SOC)

State and Local Government Cybersecurity Grant Program (SLGCP)

ENTERPRISE information services

Statewide Cybersecurity Plan Update

- Statewide Cybersecurity Plan draft is complete.
- Currently under review by the planning committee.
- Statewide Cybersecurity services catalog is drafted and prioritized in tiers by the planning committee.
- Grant application processing framework is currently being drafted.



ENTERPRISE information services

Thank you

Shirlene A Gonzalez
Legislative & Communications Director
shirlene.a.gonzalez@das.oregon.gov

ENTERPRISE
information services