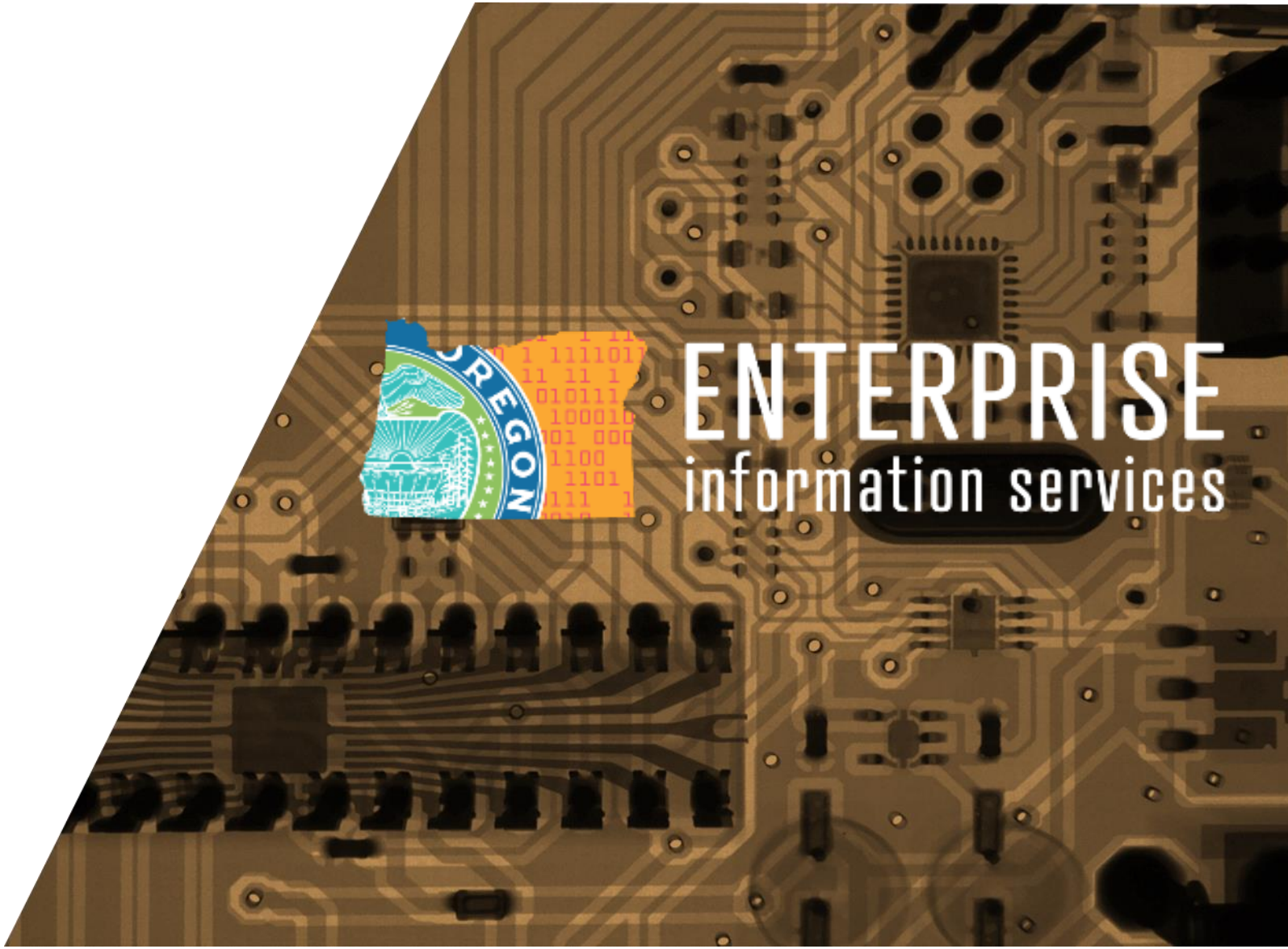
# LOC 2023

Preparing for Cyber Threats

**April 2023**



# Cyber Strategy

Cyber is **not** just an IT issue

People, Process, and Technology

Interdependency

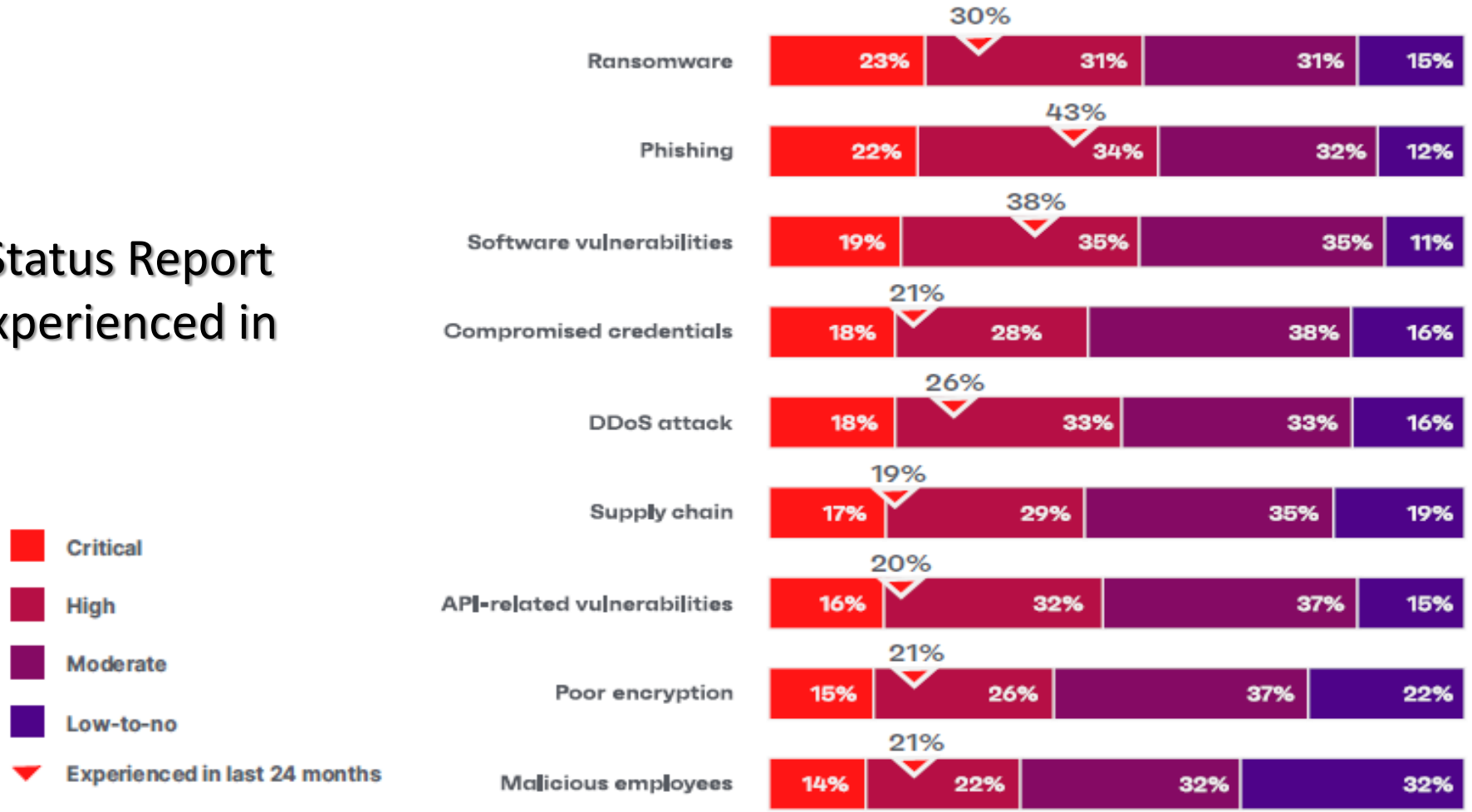
- Infrastructure
- Communications
- Third Parties (Vendors/Business Partners)

# Cyber Strategy

- People - Build Relationships
- Process
  - Formalize Cyber Security
  - Define Roles/Responsibilities
  - Train
  - Exercise
- Technology - Test Systems

# Cybersecurity Overview & Industry Trends

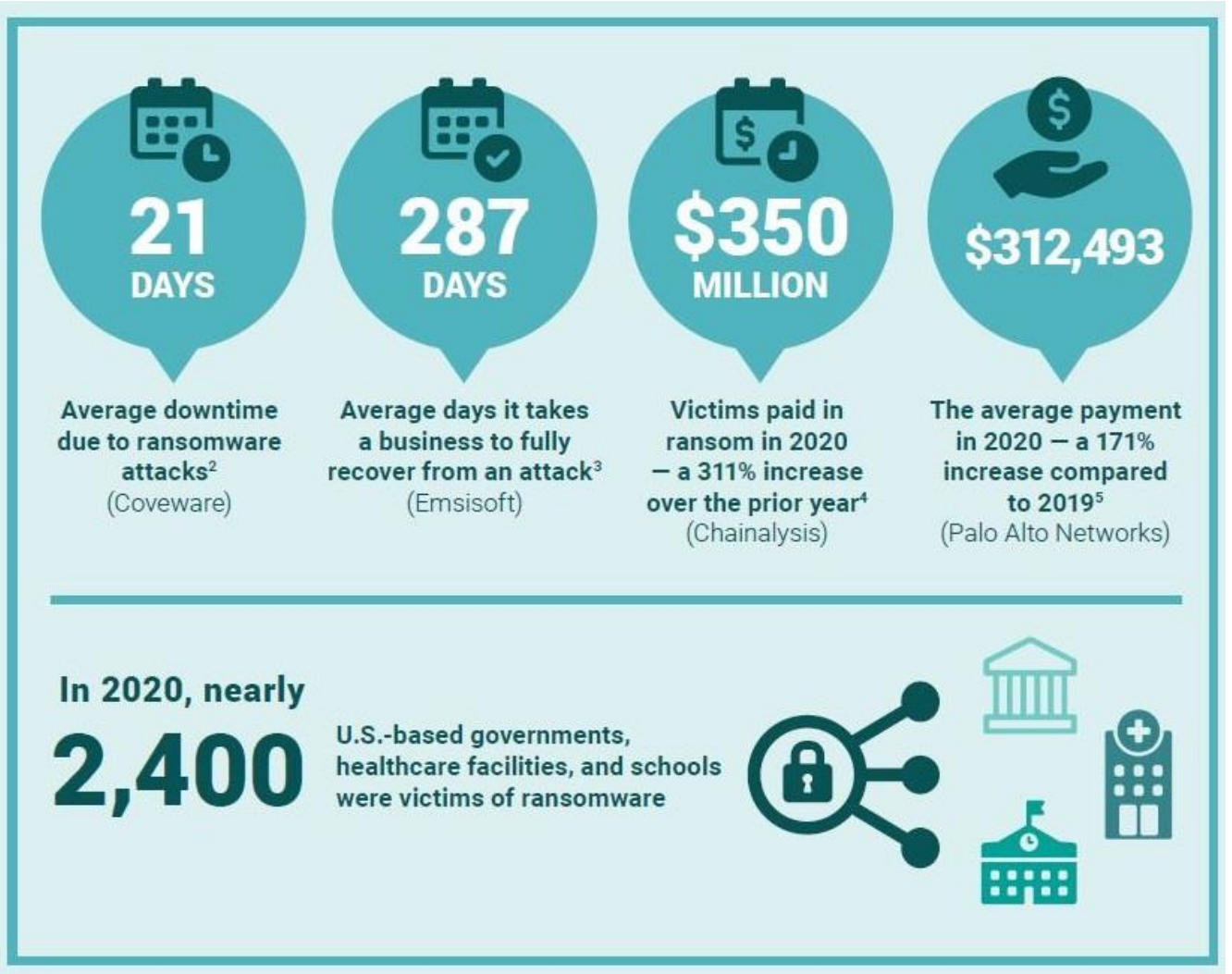
2023 Global Cyber Status Report
Malicious activity Experienced in the last 24 months.




Press Reset: A 2023 Cybersecurity Status Report 11

ENTERPRISE information services

# Ransomware




Source: Institute for Security and Technology

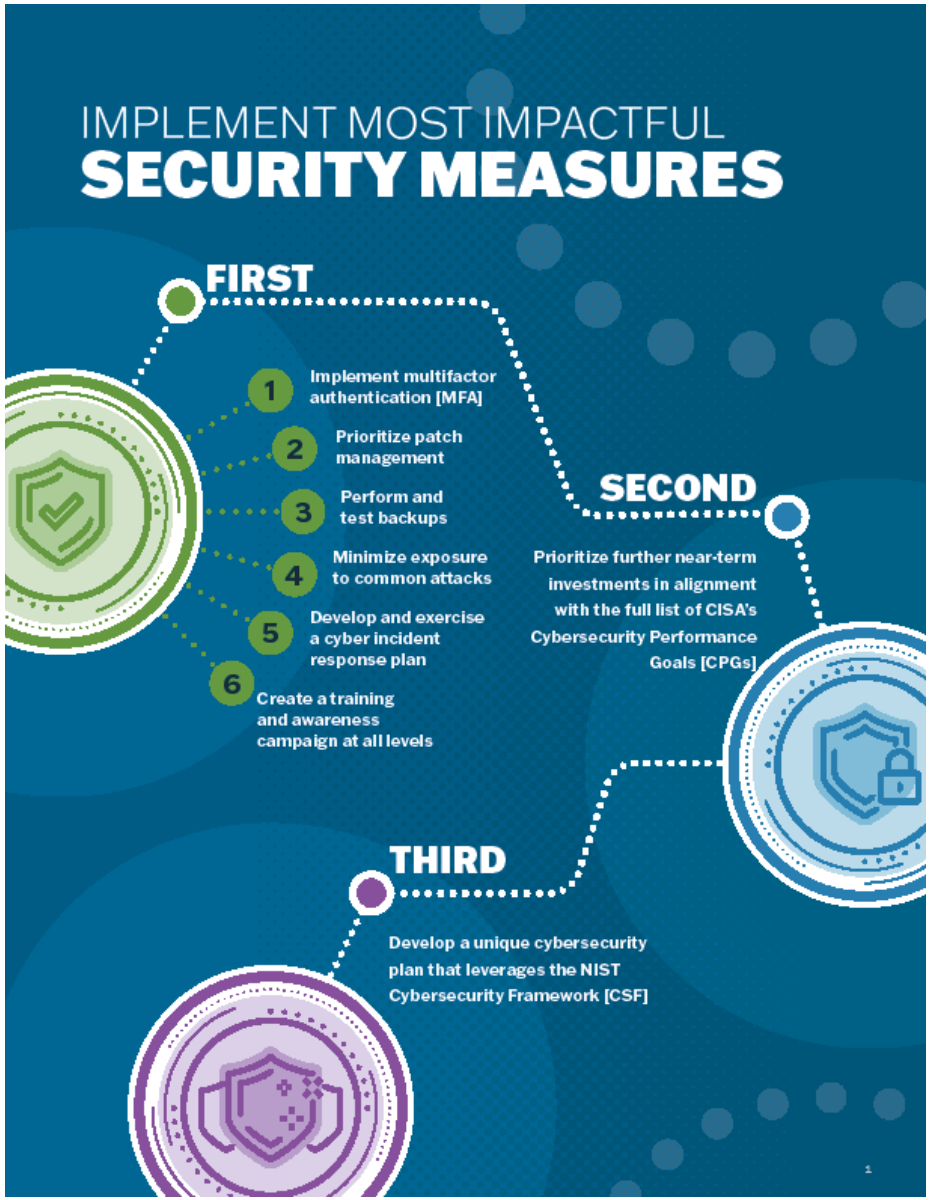
# Ransomware


PROTECT AGAINST RANSOMWARE
Maintain offline backups.
Automate software patching and updates.
Learn how to identify phishing emails.
Use multi-factor authentication.
Ensure antivirus/antimalware software is up to date.
CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Learn more: CISA.gov/ransomware

# Take Action


IF YOU EXPERIENCE AN ATTACK
Identify and isolate affected systems.
Only if you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
Triage impacted systems for restoration and recovery.
Notify the FBI/U.S. Secret Service and CISA.
CISA does not recommend paying ransom since there is not any guarantee cybercriminals will restore your data.
Learn more: CISA.gov/ransomware
CISA

# Implement

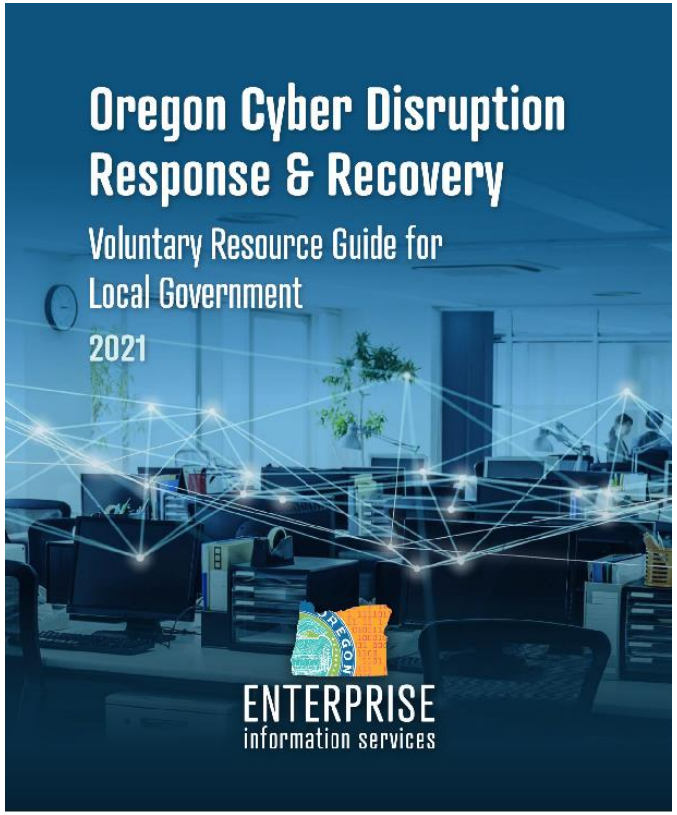

IMPLEMENT MOST IMPACTFUL
SECURITY MEASURES
FIRST
1 Implement multifactor authentication [MFA]
2 Prioritize patch management
3 Perform and test backups
4 Minimize exposure to common attacks
5 Develop and exercise a cyber incident response plan
6 Create a training and awareness campaign at all levels
SECOND
Prioritize further near-term investments in alignment with the full list of CISA's Cybersecurity Performance Goals [CPGs]
THIRD
Develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework [CSF]

# Resources

| Service | State | | Federal | | Dual Role | |
|---|---|---|---|---|---|---|
| | Cyber Security Services (CSS) | Office of Emergency Manage-ment (OEM) | Cybersecurity Infrastructure Security Agency (CISA) | Multi State-Information Sharing & Analysis Center (MSISAC) | Oregon Titan Fusion Center | Oregon National Guard |
| Proactive | | | | | | |
| Advisories/Threat Notification | ✓ | ✓ | ✓ | ✓ | ✓ | |
| CIS SecureSuite Membership | | | | ✓ | | |
| Consulting | | | | ✓ | | |
| Continuity Planning | | | | | | ✓ |
| Cyber Assessments | | | ✓ | | | ✓ |
| Cyber Exercise Planning | | | ✓ | | | ✓ |
| Cyber Training/Education Resources | ✓ | | ✓ | ✓ | | |
| Cyber Vendor Contracts | | | | | | |
| Malicious Domain Bloacking | | | | ✓ | | |
| Managed Security Services | | | | ✓ | | |
| Network Monitoring | | | | ✓ | | |
| Penetration Testing | | | ✓ | | | ✓ |
| Phishing Campaign Assessments | | | ✓ | | | |
| Risk & Vulnerability Assessment | | | ✓ | | | |
| Validated Architecture Design | | | ✓ | | | |
| Vulnerability Scanning | | | ✓ | ✓ | | |
| Web Application Scanning | | | ✓ | | | |
| | | | | | | |
| Alerts | ✓ | | ✓ | ✓ | ✓ | |
| Emergency Declaration | | ✓ | | | | |
| Incident Response Assistance | ✓ | | ✓ | ✓ | | |
| Malicious Code Analysis Platform | | | | ✓ | | |
| Malware Analysis | | | ✓ | ✓ | | |
| Vulnerability Assessment | | | | ✓ | | |
| Vulnerability Management Program | | | | ✓ | | |

# Cyber Disruption Response and Recovery Plan

Whole of Government approach
Community Driven
Common Framework
Voluntary
Leverage resources
Communications
Education
**security.oregon.gov/cyberdisruption**



# CISA Cyber Services (all offered at *no charge*)

- Vulnerability & Web Application Scanning
- Phishing Exercise
- Remote Pen Testing
- Risk & Vulnerability Assessment
- Malware Analysis
- Various cyber assessments – virtual/onsite or self-assessments
- Cyber Table-Top Exercise
- Lots of other CISA resources at https://www.cisa.gov

# Funding – State and Local Cyber Grant Program

## Who is eligible to apply:

The State Administrative Agency (SAA)'s for states and territories are the only eligible applicants. In addition, two or more eligible entities may apply jointly for assistance as a multi-entity group. Under SLCGP, that means two or more SAAs may apply for joint projects, but they still must submit separate applications.

## Role of the SAA:

The SAA is responsible for managing the grant application and award. Working with the Cybersecurity Planning Committee, the SAA must ensure at least 80% of the federal funds awarded under the SLCGP are passed-through to local entitles. Leaving 20% for state entities. In addition, at least 25% of the total funds made available under the grant must be passed through to rural communities.

# SLCGP Grant Priorities

## First Year:

In the first year, the focus is on establishing a strong foundation on which to build a sustainable cybersecurity program. Initial priorities include the following, all of which are statutory conditions for receiving a grant:

- Establish a Cybersecurity Planning Committee that can lead entity-wide efforts.
- Develop a Cybersecurity Plan that addresses the entire jurisdiction and incorporates cybersecurity best practices.
- Conduct assessments and evaluations to identify gaps that can be mitigated by individual projects throughout the life of the grant program.
- SLCGP_INFO@DAS.OREGON.GOV

# SLCGP Cybersecurity Plan

- Statewide Cybersecurity Plan Template and the plan development effort estimate.
- 16 Key Elements must be on the plan.

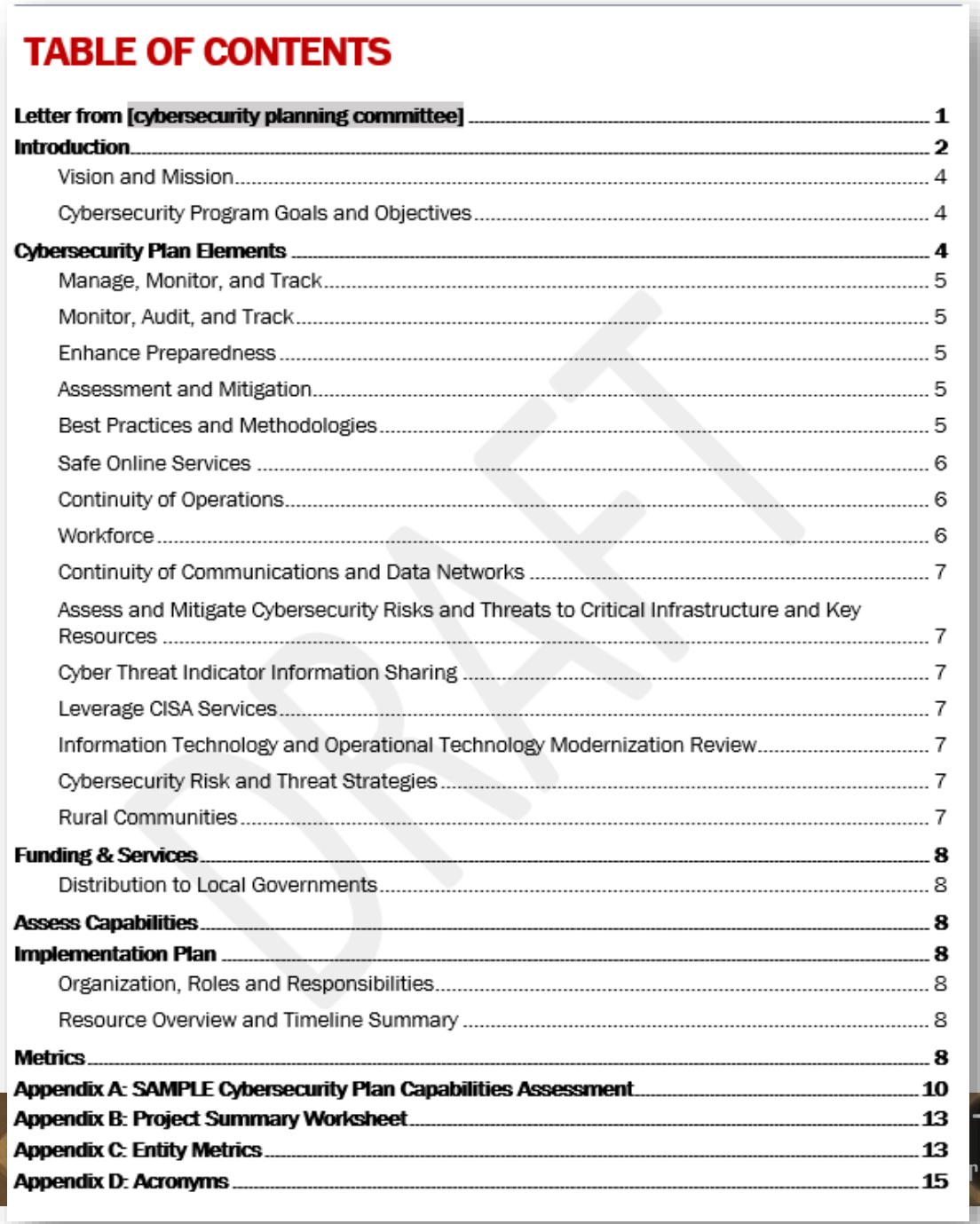


TABLE OF CONTENTS

# Cyber Security Services Catalog Approach

## Tiered Approach

### Tier 1: Basic Cyber Hygiene

- Security awareness training program that includes phishing service
- Centralized cybersecurity workforce development – Online training services

### Tier 2: Tactical

- MFA implementation assistance program
- Patch management
- Tenable scans service

### Tier 3: Strategic

- Cybersecurity Strategic planning assistance
- Security assessment of government information assets in Oregon

# Contact

**Sherri Yoakum**

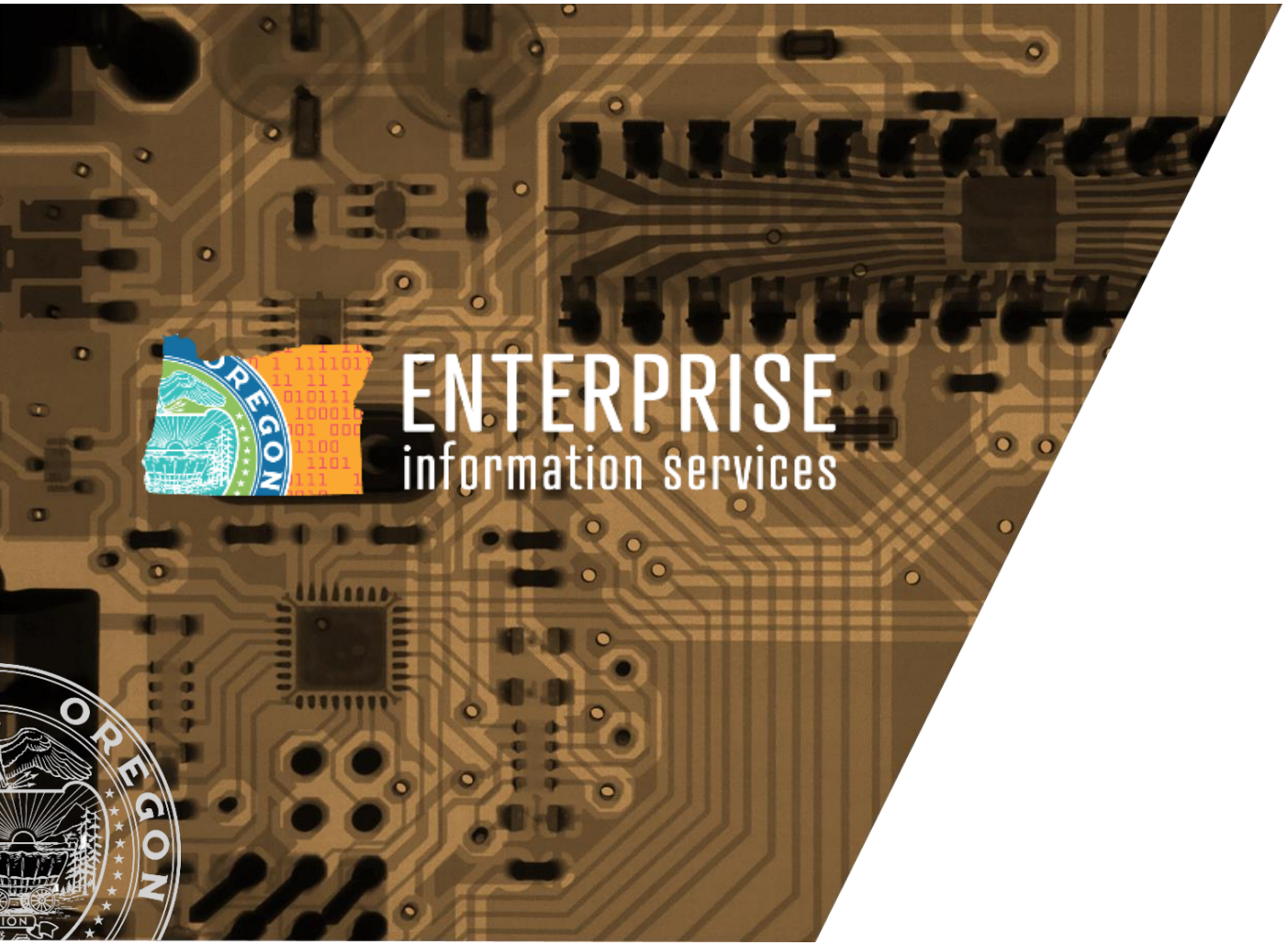
Cyber Security Services (CSS), Enterprise Information Services

Email:  sherri.m.yoakum@das.Oregon.gov

**Mariah O'Seanecy**

Cyber Security Services (CSS), Enterprise Information Services

Email: mariah.oseanecy@das.Oregon.gov




# Thank you