WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

OPDP Monthly Webinar: Security as one of the WA Privacy Principles

September 30, 2021

Agenda for September 30, 2021 Meeting

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Agenda

10:00 Welcome and introductions – Zack Hudgins OPDP Privacy Manager
10:05 Shane Swanson – OCS Deputy Director CISO
10:30 Aaron Munn – SAO CISO
10:55 Q&A
11:00 Wrap-up and Thank you

OPDP

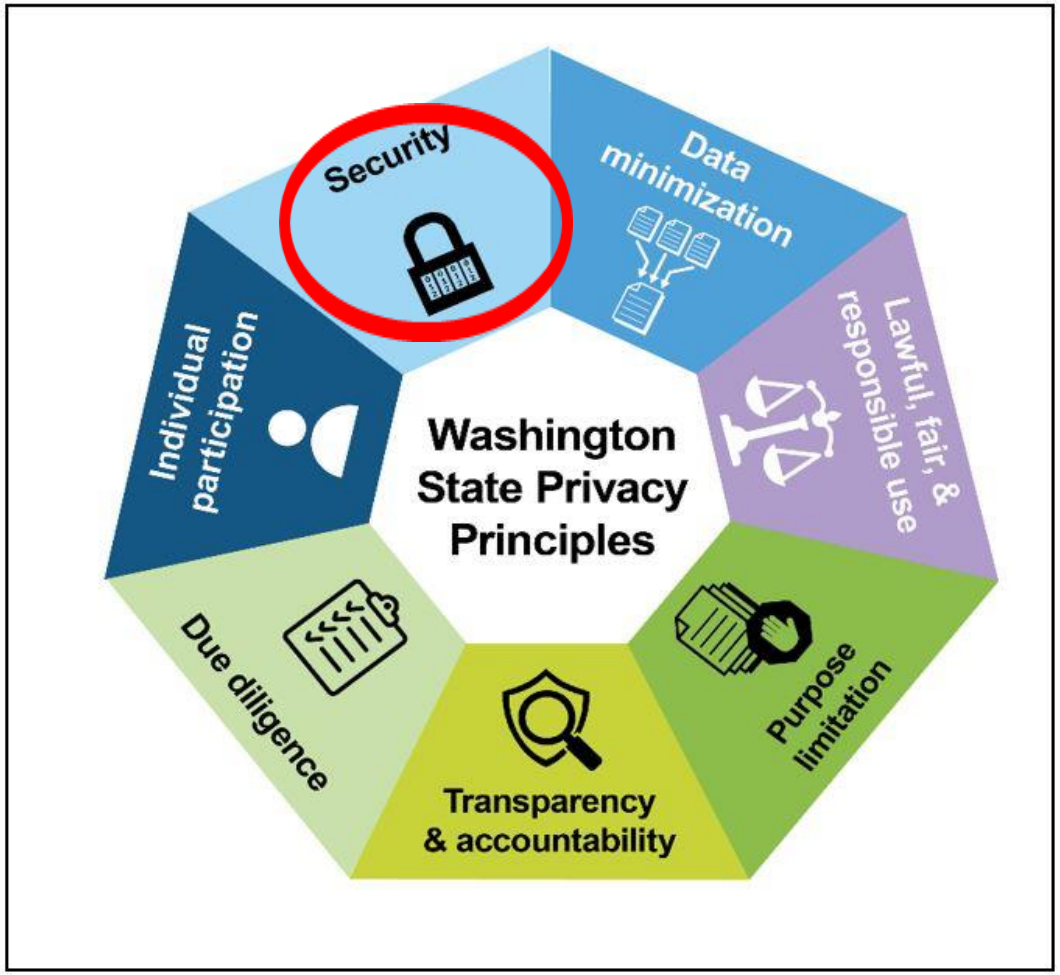
WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Welcome and Introductions

OPDP

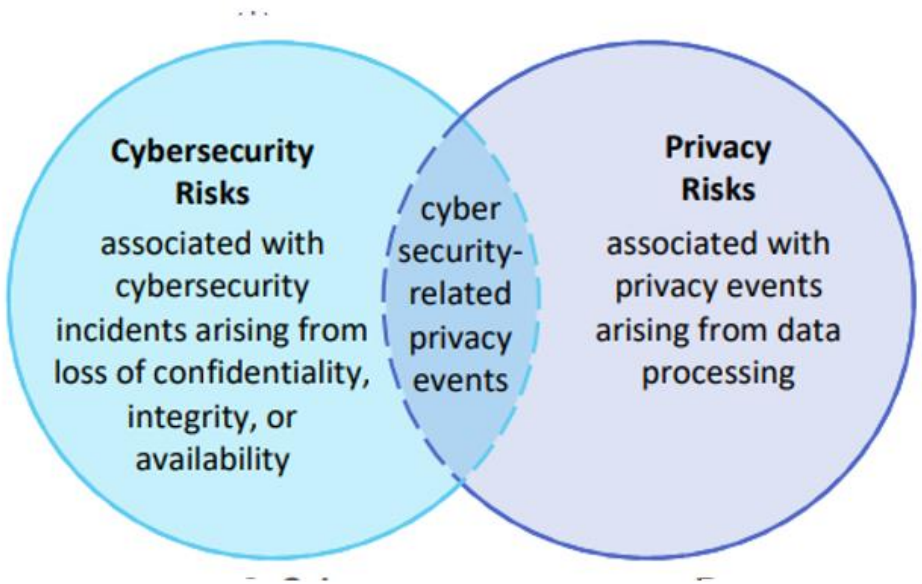
WA State Privacy Principles

- Lawful, fair, & responsible use
- Data minimization
- Purpose Limitation
- Transparency & accountability
- Due diligence
- Individual participation
- Security



Overview

- Today's topic is about two cyber security frameworks used to help organizations become more resilient as they face complex threats to data security.
- NIST CSF and CIS controls are the frameworks we will be focusing on today.



- Security and Privacy are separate and overlapping disciplines with the similar goals of data protection.

Two Major Security Frameworks

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Center for Internet Security –

CIS is a community-driven nonprofit, responsible for developing globally recognized best practices for securing IT systems and data. CIS leads an effort to continuously evolve standards and provide products and services to proactively safeguard against emerging threats.

https://www.cisecurity.org/

CIS Center for Internet Security®
Confidence in the Connected World®

National Institutes of Standards and Technology –

NIST develops cybersecurity standards, guidelines, best practices, and resources to meet the needs of U.S. industry, federal agencies, and the broader public.

https://www.nist.gov/cybersecurity

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

OPDP

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

OPDP

Shane Swanson – Deputy CISO

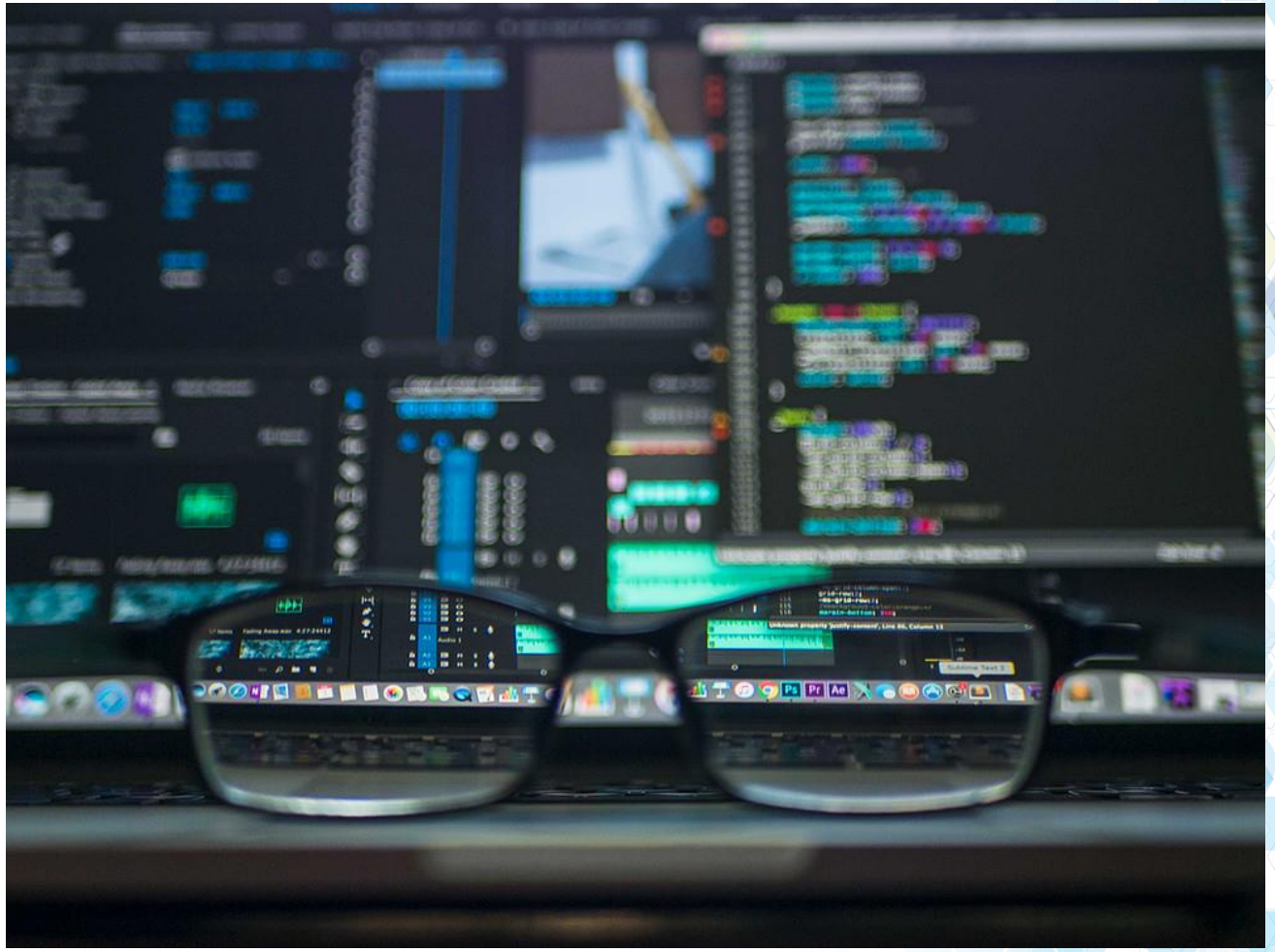
WA State Office of Cyber Security

National Institute of Standards and Technology Framework

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Cybersecurity Risk Management

Shane Swanson, Deputy CISO, State of Washington



≠

Compliance Is A Requirement, But Doesn't Equate To Improved Cybersecurity

An Enhanced Approach to Cybersecurity Risk Management

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Inputs

Standards

- OCIO 141.10
- NIST Risk Management Framework
- NIST Cybersecurity framework
- CIS Controls Assessment

Threat Landscape

- Who might attack?
- What are they after?
- What tactics will they use?

Cybersecurity Principles

SECURE

Establish risk-prioritized controls to protect against known and emerging threats, and comply with standards and regulations

DEFEND

Create situational risk and threat awareness across the environment to detect violations and suspicious behavior

RESPOND

Develop a capability to handle critical incidents, quickly return to normal agency operations, and repair damage to the State

Identify
Protect
Detect
Respond
Recover

How We Reduce Cybersecurity Risk

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

OPDP

Industry Standards and Leading Practices

+

Managing our Threat Landscape & our Attack Surface

Security Management Framework

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Cyber Security Framework

State Objectives

- Growth / Innovation
- Risk Based Decision Making
- Reputation
- Operational Efficiency
- Compliance

Operating Model Component

- **Governance & Oversight** – The organizational structure, committees, and roles to manage cybersecurity risk
- **Policies & Standards** – Define and communicate requirements for managing cybersecurity risk
- **Management Processes** – Processes to manage cybersecurity risk
- **Tools & Technology** – Tools to support the cybersecurity risk management lifecycle
- **Risk Metrics** – Reports that identify cybersecurity risks and performance

IT and Information Security Risk Domains*

SECURE

1. Risk & Compliance Management
2. Identity & Access Management
3. Data Protection & Management
4. Infrastructure Security
5. Application Security & SDLC
6. Asset Management
7. Third Party Management
8. Physical Security

DEFEND

9. Vulnerability Management
10. Threat Intelligence
11. Endpoint Monitoring
12. Security Operations
13. Predictive Analytics
14. Insider Threat Monitoring

RESPOND

15. Crisis Management
16. Resiliency & Recovery
17. Cyber Simulation
18. Incident Response

*NIST CSF and Leading Practice

Agency Characterization

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

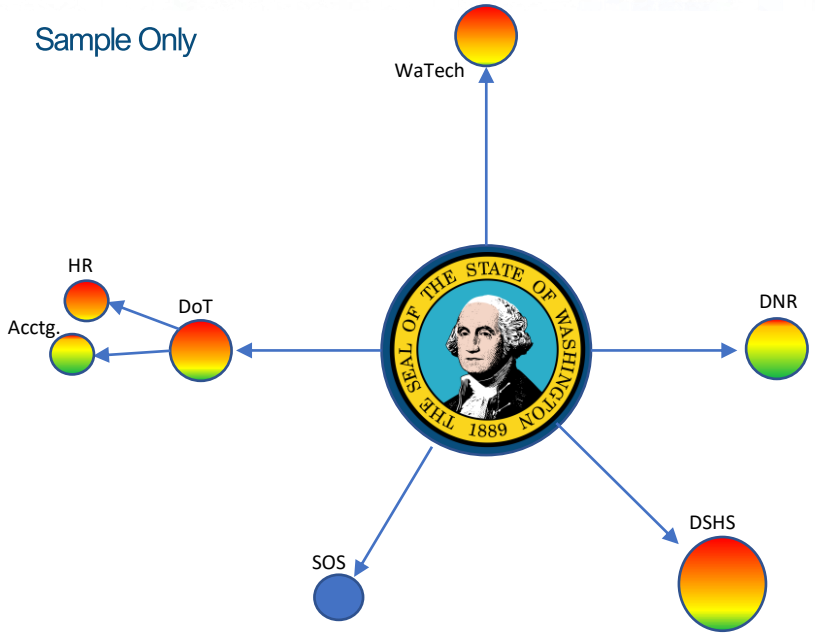
Sensitive data to protect

Agencies house numerous types of sensitive data (e.g., PII, PHI, FTI, Critical Infrastructure, IP), which requires increased focus to protect and avoid reputational, compliance and financial damage associated with breaches.

Extended attack surface

Innovation drives growing use of mobile, cloud, web-applications and telematics to enhance Citizen engagement with their elected leaders.

The state is a unique and attractive target for a variety of malicious actors (e.g., nation-states, hacktivists, organized crime).

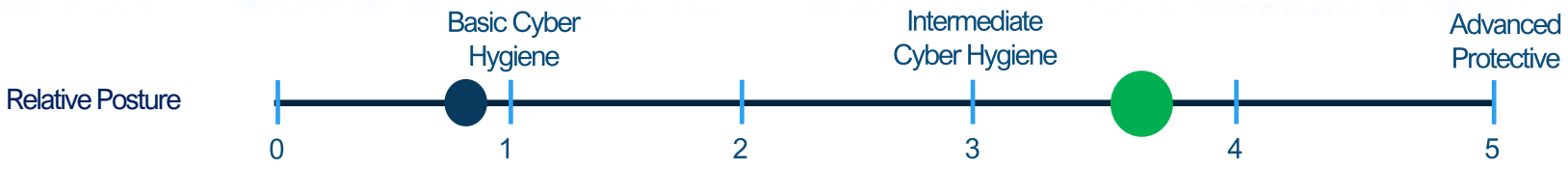


What Data Resides Where?
On-Prem
Cloud

- Use the Cybersecurity Risk Management Framework (CRMF)
- Assess against the (18) Cybersecurity Capability Domains (CCDs) Tie back to OCIO/NIST Standard Requirements
- Develop a state-wide view: Attack Surface, Capability & Risk

Current State Maturity vs. Target State

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency



Operating Model Components

0 1 2 3 4 5

- Governance & Oversight
- Policies & Standards
- Management Processes
- Tools & Technology
- Risk Metrics

Secure

0 1 2 3 4 5

- Risk & Compliance
- Application Security
- Identity Access Management
- Asset Management
- Data Protection & Management
- Third-Party Management
- Infrastructure Security
- Physical Security

Defend

0 1 2 3 4 5

- Vulnerability Management
- Threat Intelligence
- End-Point Monitoring
- Security Operations
- Predictive Analytics
- Insider Threat Monitoring

Response

0 1 2 3 4 5

- Crisis Management
- Resiliency & Recovery
- Cyber Simulation
- Incident Response & Forensics

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Aaron Munn – CISO w/WA State Auditor

Center for Internet Security Framework

O
P
D
P

Center for Internet Security (CIS) Controls and Measuring Government Security

Aaron Munn
Chief Information Security Officer

Office of Privacy and Data Protection Monthly Webinar
September 30, 2021

Office of the Washington State Auditor
Pat McCarthy

Topics for today's presentation

- SAO Cybersecurity Audit Program Highlights
- CIS Controls Version 8 Overview
- CIS Controls and The Cybersecurity Framework

SAO Cybersecurity Audit program

- Funding provided by Initiative 900
- Includes both state agencies and local governments
- Audit scope
  - Penetration testing
  - Leading practice assessment
- Audits use CIS Controls as leading practice framework
  - Controls Version 7 for work begun in 2021
  - Controls Version 8 for work starting in 2022
- Audit confidentiality – RCW 42.56.420(4)

What are the CIS Controls?

"Recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks."

The Center for Internet Security

Why use CIS Controls?

- Prioritized controls and safeguards
- Measurable
- Built on stakeholder consensus
- Defensible against real-world threats
- Mapped to most frameworks and regulations
- Security investment maximization
- Focus on simplicity

What is new in Version 8?

#	Description – Controls v7	
1	Inventory of hardware	
2	Inventory of software	
3	Continuous vulnerability management	
4	**Control of administrative privileges**	
5	**Secure configuration**	
6	Maintenance and analysis of logs	
7	Email and browser protections	
8	Malware defenses	
9	Limitation of ports and protocols	**OUT**
10	Data recovery	
11	**Secure configuration of network devices**	
12	Boundary defense	**OUT**
13	Data protection	
14	**Controlled access based on need to know**	
15	Wireless access control	**OUT**
16	Account monitoring and control	
17	Security awareness training	
18	Application security	
19	Incident management	
20	Penetration testing	

	#	Description – Controls v8
	1	Inventory and control of enterprise assets
	2	Inventory and control of software assets
	3	Data protection
	4	**Secure configuration of enterprise assets and software**
	5	Account management
	6	**Access control management**
	7	Continuous vulnerability management
	8	Audit log management
	9	Email and web browser protections
	10	Malware defenses
	11	Data recovery
	12	Network infrastructure management
	13	Network monitoring and defense
	14	Security awareness and skills training
NEW	15	**Service provider management**
	16	Application software security
	17	Incident response management
	18	Penetration testing

CIS Controls Implementation Groups

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74
Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
Additional cyber defense Safeguards

Total Safeguards **153**

Office of the Washington State Auditor
Pat McCarthy

CIS Control 3: Data protection

03 Data Protection

3.1	Establish and Maintain a Data Management Process	●	●	●
3.2	Establish and Maintain a Data Inventory	●	●	●
3.3	Configure Data Access Control Lists	●	●	●
3.4	Enforce Data Retention	●	●	●
3.5	Securely Dispose of Data	●	●	●
3.6	Encrypt Data on End-User Devices	●	●	●
3.7	Establish and Maintain a Data Classification Scheme		●	●
3.8	Document Data Flows		●	●
3.9	Encrypt Data on Removable Media		●	●
3.10	Encrypt Sensitive Data in Transit		●	●
3.11	Encrypt Sensitive Data at Rest		●	●
3.12	Segment Data Processing and Storage Based on Sensitivity		●	●
3.13	Deploy a Data Loss Prevention Solution			●
3.14	Log Sensitive Data Access			●

Measuring CIS Control 3

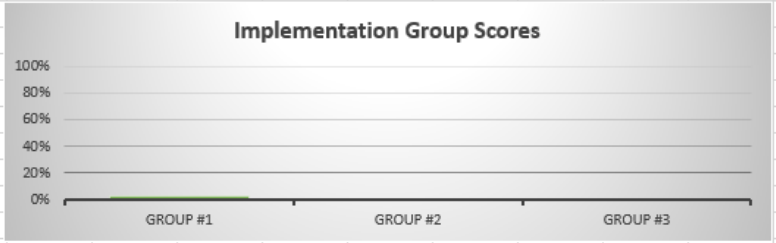
www.auditscripts.com/free-resources/critical-security-controls/

ID	CIS Control Detail	NIST CSF	Implementation Groups	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Business
3.1	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Identify	1,2,3	Data Inventory System	Informal Policy	Parts of Policy Implemented	Not Applicable	Not Applicable
3.2	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Identify	1,2,3	Data Inventory System	Approved Written Policy	Implemented on Some Systems	Not Applicable	Not Applicable
3.3	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Protect	1,2,3	Access Management System	Informal Policy	Implemented on Some Systems	Not Applicable	Not Applicable
3.4	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum	Protect	1,2,3	Access Management System	Written Policy	Implemented on Most Systems	Not Applicable	Not Applicable
3.5	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Protect	1,2,3	Physical Security Program	Written Policy	Implemented on Some Systems	Not Applicable	Not Applicable
3.6	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Protect	1,2,3	Removable Media Protection System	Approved Written Policy	Parts of Policy Implemented	Parts of Policy Automated	Not Reported

Measuring CIS Control 3

ATT&CK Activity	Preventive Capability	Detective Capability
Initial Access	Low	Low
Execution	Low	Low
Persistence	Low	Low
Privilege Escalation	Low	Low
Defense Evasion	Low	Low
Credential Access	Low	Low
Discovery	Low	Low
Lateral Movement	Low	Low
Collection	Low	Low
Command and Control	Low	Low
Exfiltration	Low	Low

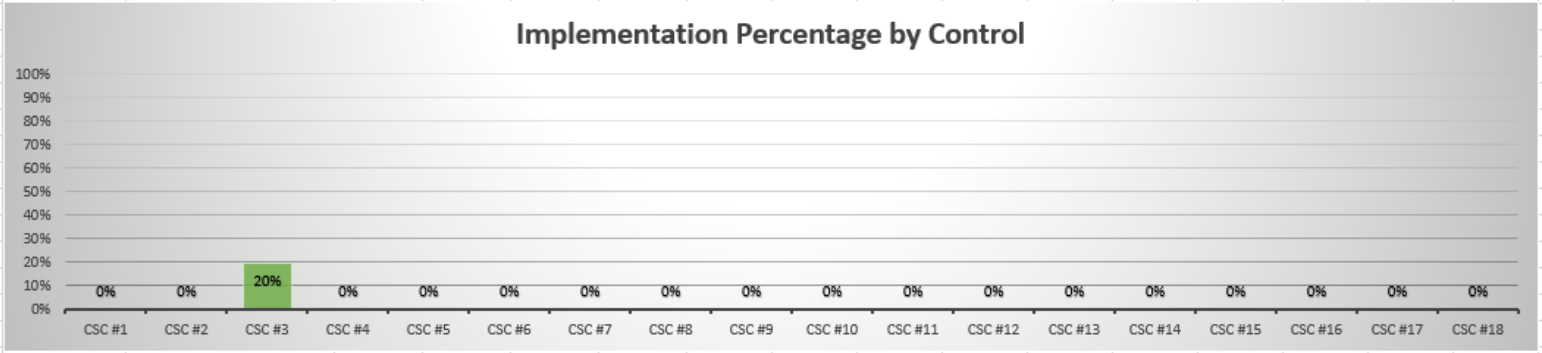
Implementation Group Scores					
Group #1	3%	Group #2	1%	Group #3	1%



Maturity level:	Description:	Score:
Level One	Policies Complete	0.03
Level Two	Controls 1-5 Implemented	0.06
Level Three	All Controls Implemented	0.00
Level Four	All Controls Automated	0.00
Level Five	All Controls Reported	0.00

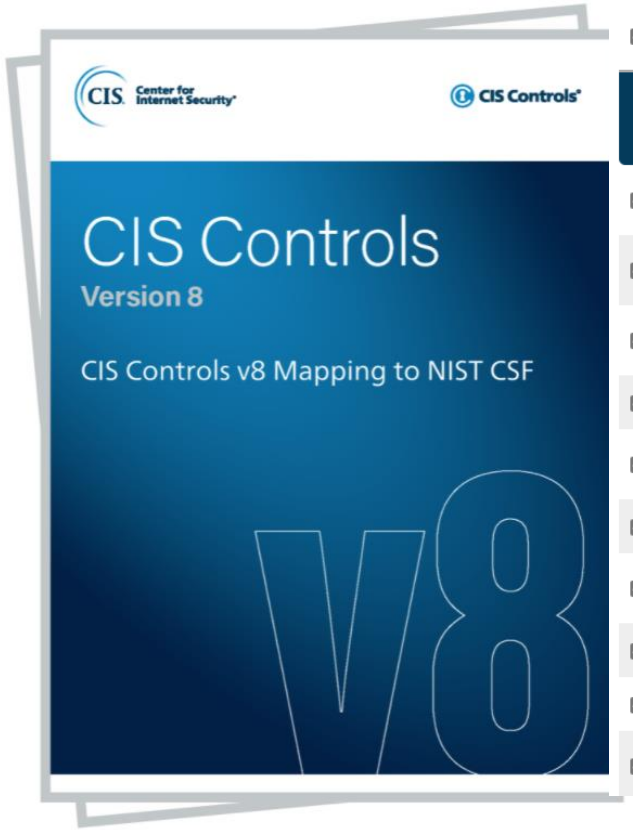
Maturity Rating*: 0.09

*Rating is on a 0-5 scale.



Aligning CIS Control 3 and NIST's Cybersecurity Framework

- www.cisecurity.org/controls/cis-controls-navigator/
- www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/



☑	Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3	NISTCSF
CIS Control 3 - Data Protection Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.								
☑	3.1	Establish and Maintain a Data Management Process	Data		●	●	●	●
☑	3.2	Establish and Maintain a Data Inventory	Data		●	●	●	●
☑	3.3	Configure Data Access Control Lists	Data		●	●	●	●
☑	3.5	Securely Dispose of Data	Data		●	●	●	●
☑	3.7	Establish and Maintain a Data Classification Scheme	Data			●	●	●
☑	3.8	Document Data Flows	Data			●	●	●
☑	3.9	Encrypt Data on Removable Media	Data			●	●	●
☑	3.10	Encrypt Sensitive Data in Transit	Data			●	●	●
☑	3.11	Encrypt Sensitive Data at Rest	Data			●	●	●
☑	3.12	Segment Data Processing and Storage Based on Sensitivity	Network			●	●	●

Control 3 and Cybersecurity Framework

CIS Control 3 - Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

☑	3.1	Establish and Maintain a Data Management Process	Data	●	●	●
☑	3.2	Establish and Maintain a Data Inventory	Data	●	●	●
☑	3.3	Configure Data Access Control Lists	Data	●	●	●
☑	3.4	Enforce Data Retention	Data	●	●	●
☑	3.5	Securely Dispose of Data	Data	●	●	●

Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

NIST CSF Groups

PR.DS-3
Assets are formally managed throughout removal, transfers, and disposition

PR.IP-6
Data is destroyed according to policy

Cybersecurity Framework Policy Template Guide

CIS Center for Internet Security

MS-ISAC Multi-State Information Sharing & Analysis Center

NIST Cybersecurity Framework

Policy Template Guide

CIS Center for Internet Security

MS-ISAC Multi-State Information Sharing & Analysis Center

Contents

Resources and tools

- CIS Controls

  www.cisecurity.org/controls

- CIS Controls Navigator

  www.cisecurity.org/controls/cis-controls-navigator/

- CSF Policy Template Guide

  www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf

- Audit Scripts CIS Resources

  www.auditscripts.com/free-resources/critical-security-controls/

SAO audit contacts

- SAOITAudit@sao.wa.gov
- www.sao.wa.gov/about-audits/about-cybersecurity-audits

Questions

Contact information

Contact Aaron Munn

Aaron.Munn@sao.wa.gov

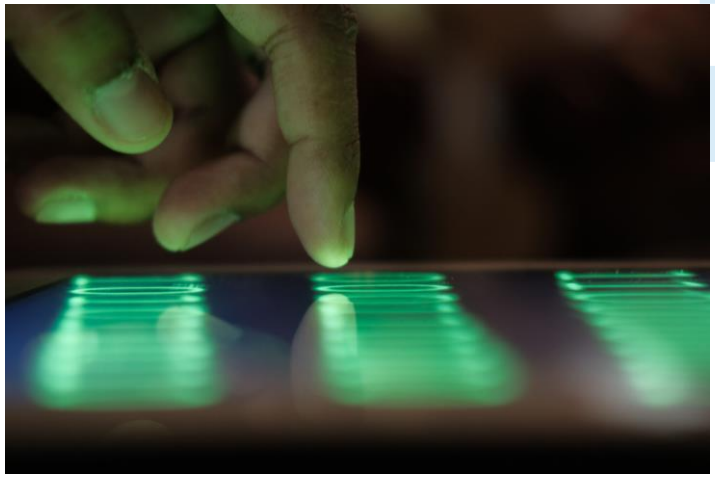
(564) 999-0902

Q&A

Wrap-up

Resources

- OPDP Webinars – The Washington State Office of Privacy and Open Data does monthly webinars on a variety of topics. Check the website https://watech.wa.gov/privacy for past webinars, or watch for …
- OPDP Privacy Points – The monthly newsletter from the Chief Privacy Officer – Katy Ruckle. Important information, new trainings and resources, and what we are watching are all part of the easy to sign up for email blast.
- OPDP Website – There are also resources for State Agencies, Local Governments and Tribal Partners available on the OPDP website. https://watech.wa.gov/privacy



Join our collaboration and work at OPDP
https://watech.wa.gov/Privacy

Sign up for OPDP newsletter –

See what OPDP is up to, receive news, learn about new resources and trainings, in the "***Privacy Points***" blog by Chief Privacy Officer – Katy Ruckle

Scroll to bottom of Privacy pages on WaTech website and look for this link:

O P D P

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Thank you!

privacy@ocio.wa.gov

O
P
D
P