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

September 30, 2021
Agenda for September 30, 2021 Meeting

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
Welcome and Introductions
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

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/

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
Shane Swanson – Deputy CISO

WA State Office of Cyber Security

National Institute of Standards and Technology Framework
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

**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**

**Detect**

**Protect**

**Respond**

**Recover**

**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?
How We Reduce Cybersecurity Risk

Industry Standards and Leading Practices

+ 

Managing our Threat Landscape & our Attack Surface
## Security Management Framework

<table>
<thead>
<tr>
<th>State Objectives</th>
<th>Operating Model Component</th>
<th>IT and Information Security Risk Domains*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Growth / Innovation</td>
<td>Risk Based Decision Making</td>
<td>Governance &amp; Oversight The organizational structure, committees, and roles to manage cybersecurity risk</td>
</tr>
<tr>
<td>Risk Based Decision Making</td>
<td>Policies &amp; Standards Define and communicate requirements for managing cybersecurity risk</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>Management Processes Processes to manage cybersecurity risk</td>
<td></td>
</tr>
<tr>
<td>Operational Efficiency</td>
<td>Tools &amp; Technology Tools to support the cybersecurity risk management lifecycle</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Risk Metrics Reports that identify cybersecurity risks and performance</td>
<td></td>
</tr>
</tbody>
</table>

**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
9. Vulnerability Management
10. Threat Intelligence
11. Endpoint Monitoring

**DEFEND**

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

---

Office of Privacy and Data Protection
Agency Characterization

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).

- 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

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

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

Defend
- Vulnerability Management
- Threat Intelligence
- End-Point Monitoring
- Security Operations
- Predictive Analytics
- Insider Threat Monitoring
- Crisis Management
- Resiliency & Recovery
- Cyber Simulation
- Incident Response & Forensics

Relative Posture
0 1 2 3 4 5
Basic Cyber Hygiene
Intermediate Cyber Hygiene
Advanced Protective
Aaron Munn – CISO w/WA State Auditor

Center for Internet Security Framework
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
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?

“What 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?

<table>
<thead>
<tr>
<th>#</th>
<th>Description – Controls v7</th>
<th>#</th>
<th>Description – Controls v8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory of hardware</td>
<td>1</td>
<td>Inventory and control of enterprise assets</td>
</tr>
<tr>
<td>2</td>
<td>Inventory of software</td>
<td>2</td>
<td>Inventory and control of software assets</td>
</tr>
<tr>
<td>3</td>
<td>Continuous vulnerability management</td>
<td>3</td>
<td>Data protection</td>
</tr>
<tr>
<td>4</td>
<td><strong>Control of administrative privileges</strong></td>
<td>4</td>
<td>Secure configuration of enterprise assets and software</td>
</tr>
<tr>
<td>5</td>
<td>Secure configuration</td>
<td>5</td>
<td>Account management</td>
</tr>
<tr>
<td>6</td>
<td>Maintenance and analysis of logs</td>
<td>6</td>
<td>Access control management</td>
</tr>
<tr>
<td>7</td>
<td>Email and browser protections</td>
<td>7</td>
<td>Continuous vulnerability management</td>
</tr>
<tr>
<td>8</td>
<td>Malware defenses</td>
<td>8</td>
<td>Audit log management</td>
</tr>
<tr>
<td>9</td>
<td>Limitation of ports and protocols OUT</td>
<td>9</td>
<td>Email and web browser protections</td>
</tr>
<tr>
<td>10</td>
<td>Data recovery</td>
<td>10</td>
<td>Malware defenses</td>
</tr>
<tr>
<td>11</td>
<td><strong>Secure configuration of network devices</strong></td>
<td>11</td>
<td>Data recovery</td>
</tr>
<tr>
<td>12</td>
<td>Boundary defense OUT</td>
<td>12</td>
<td>Network infrastructure management</td>
</tr>
<tr>
<td>13</td>
<td>Data protection</td>
<td>13</td>
<td>Network monitoring and defense</td>
</tr>
<tr>
<td>14</td>
<td>Controlled access based on need to know</td>
<td>14</td>
<td>Security awareness and skills training</td>
</tr>
<tr>
<td>15</td>
<td>Wireless access control OUT</td>
<td>15</td>
<td><strong>Service provider management</strong></td>
</tr>
<tr>
<td>16</td>
<td>Account monitoring and control</td>
<td>16</td>
<td>Application software security</td>
</tr>
<tr>
<td>17</td>
<td>Security awareness training</td>
<td>17</td>
<td>Incident response management</td>
</tr>
<tr>
<td>18</td>
<td>Application security</td>
<td>18</td>
<td>Penetration testing</td>
</tr>
<tr>
<td>19</td>
<td>Incident management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Penetration testing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*NEW*  

*OUT*
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 to thwart general, non-targeted attacks.

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

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

Total Safeguards 153

56 Cyber defense Safeguards

74 Additional cyber defense Safeguards

23 Additional cyber defense Safeguards
### CIS Control 3: Data protection

<table>
<thead>
<tr>
<th></th>
<th>Data Protection</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Establish and Maintain a Data Management Process</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.2</td>
<td>Establish and Maintain a Data Inventory</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.3</td>
<td>Configure Data Access Control Lists</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.4</td>
<td>Enforce Data Retention</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.5</td>
<td>Securely Dispose of Data</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.6</td>
<td>Encrypt Data on End-User Devices</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.7</td>
<td>Establish and Maintain a Data Classification Scheme</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.8</td>
<td>Document Data Flows</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.9</td>
<td>Encrypt Data on Removable Media</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.10</td>
<td>Encrypt Sensitive Data in Transit</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.11</td>
<td>Encrypt Sensitive Data at Rest</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.12</td>
<td>Segment Data Processing and Storage Based on Sensitivity</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.13</td>
<td>Deploy a Data Loss Prevention Solution</td>
<td>![Progress Indicator]</td>
</tr>
<tr>
<td>3.14</td>
<td>Log Sensitive Data Access</td>
<td>![Progress Indicator]</td>
</tr>
</tbody>
</table>
# Measuring CIS Control 3


<table>
<thead>
<tr>
<th>ID</th>
<th>CIS Control Detail</th>
<th>NIST CSF</th>
<th>Implementation Groups</th>
<th>Sensor or Baseline</th>
<th>Policy Defined</th>
<th>Control Implemented</th>
<th>Control Automated or Technically Enforced</th>
<th>Control Reported to Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>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.</td>
<td>Identify 1,2,3</td>
<td>Data Inventory System</td>
<td>Informal Policy</td>
<td>Parts of Policy Implemented</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>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.</td>
<td>Identify 1,2,3</td>
<td>Data Inventory System</td>
<td>Approved Written Policy</td>
<td>Implemented on Some Systems</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>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.</td>
<td>Protect 1,2,3</td>
<td>Access Management System</td>
<td>Informal Policy</td>
<td>Implemented on Some Systems</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum</td>
<td>Protect 1,2,3</td>
<td>Access Management System</td>
<td>Written Policy</td>
<td>Implemented on Most Systems</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>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.</td>
<td>Protect 1,2,3</td>
<td>Physical Security Program</td>
<td>Written Policy</td>
<td>Implemented on Some Systems</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows Bitlocker®, Apple FileVault®, Linux® dm-crypt.</td>
<td>Protect 1,2,3</td>
<td>Removable Media Protection System</td>
<td>Approved Written Policy</td>
<td>Parts of Policy Implemented</td>
<td>Parts of Policy Automated</td>
<td>Not Reported</td>
<td></td>
</tr>
</tbody>
</table>
Measuring CIS Control 3
Aligning CIS Control 3 and NIST’s Cybersecurity Framework

- [www.cisecurity.org/controls/cis-controls-navigator/](http://www.cisecurity.org/controls/cis-controls-navigator/)
- [www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/](http://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/)

---

**CIS Control 3 - Data Protection**

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Asset Type</th>
<th>Implementation Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Establish and Maintain a Data Management Process</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.2</td>
<td>Establish and Maintain a Data Inventory</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.3</td>
<td>Configure Data Access Controls List</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.5</td>
<td>Securely Dispose of Data</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.7</td>
<td>Establish and Maintain a Data Classification Scheme</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.8</td>
<td>Document Data Flows</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.9</td>
<td>Encrypt Data on Removable Media</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.10</td>
<td>Encrypt Sensitive Data in Transit</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.11</td>
<td>Encrypt Sensitive Data at Rest</td>
<td>Data</td>
<td>4 4 4 4 4</td>
</tr>
<tr>
<td>3.12</td>
<td>Segment Data Processing and Storage Based on Sensitivity</td>
<td>Network</td>
<td>4 4 4 4 4</td>
</tr>
</tbody>
</table>
Control 3 and Cybersecurity Framework

<table>
<thead>
<tr>
<th>CIS Control 3 - Data Protection</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.</td>
<td></td>
</tr>
<tr>
<td>3.1 Establish and Maintain a Data Management Process</td>
<td>Data</td>
</tr>
<tr>
<td>3.2 Establish and Maintain a Data Inventory</td>
<td>Data</td>
</tr>
<tr>
<td>3.3 Configure Data Access Control Lists</td>
<td>Data</td>
</tr>
<tr>
<td>3.4 Enforce Data Retention</td>
<td>Data</td>
</tr>
<tr>
<td>3.5 Securely Dispose of Data</td>
<td>Data</td>
</tr>
</tbody>
</table>

- 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
Resources and tools

- CIS Controls
  www.cisecurity.org/controls

- CIS Controls Navigator
  www.cisecurity.org/controls/cis-controls-navigator/

- CSF Policy Template Guide

- 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
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:
Thank you!
privacy@ocio.wa.gov