WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementing ESSB 5432

Office of Privacy and Data Protection
Office of Cybersecurity
June 24, 2021

ESSB 5432 – Concerning cybersecurity and data sharing in Washington state government

- Data governance report
- Data sharing agreements
- OCS creation
- Catalog of services
- Incident response
- Independent security assessment

Best Practices Report

OPDP

Section 4

The office of cybersecurity, in collaboration with the office of privacy and data protection and the office of the attorney general, shall:

- Research and examine existing best practices for
  - data governance,
  - data protection,
  - the sharing of data relating to cybersecurity, and
  - the protection of state and local governments' information technology systems and infrastructure
- including, but not limited to,
  - model terms for data-sharing contracts and
  - adherence to privacy principles.
- Report on findings and recommendations due 12/1/2021

OPDP

Section 4

The office of cybersecurity, in collaboration with the office of privacy and data protection and the office of the attorney general, shall:

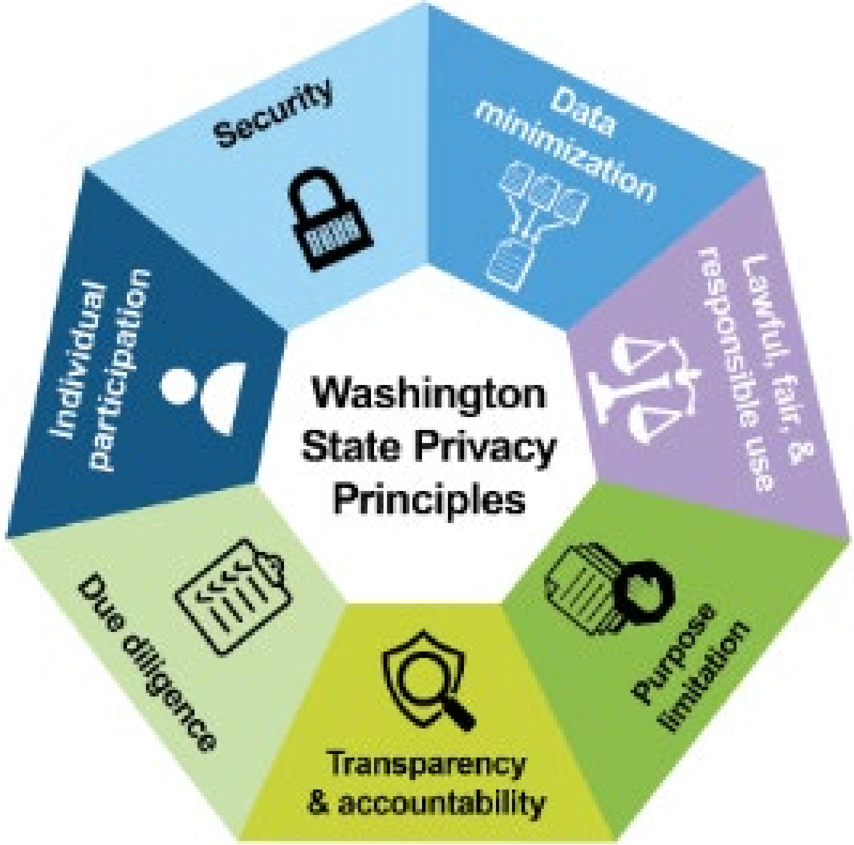
- Research and examine existing best practices for
  - data governance,
  - data protection,
  - the sharing of data relating to cybersecurity, and
  - the protection of state and local governments' information technology systems and infrastructure
- including, but not limited to,
  - model terms for data-sharing contracts and
  - adherence to privacy principles.
- Report on findings and recommendations due 12/1/2021

General topics

OPDP

Specific topics

- adherence to privacy principles
- model terms for data-sharing contracts



Washington State Privacy Principles

Data Sharing Agreement Requirements

OPDP

Think fast!

New data sharing requirements effective July 25, 2021

(but how new are they?)

Section 5

New section in chapter 39.26 RCW

- Before an agency shares with a *contractor* category 3 or higher data,
  - as defined in policy established in accordance with RCW 43.105.054,
- a written data-sharing agreement must be in place.
  - Such agreements shall conform to the policies for data sharing specified by the office of cybersecurity under the authority of RCW 43.105.054.

Chapter 39.26 RCW = Procurement of Goods and Services

Agency = state agencies

Covers sharing with contractors

RCW 43.105.054 = OCIO powers and duties to establish statewide policy

Section 6

New section in chapter 39.34 RCW

- If a public agency is requesting *from another public agency* category 3 or higher data,
  - as defined in policy established in accordance with RCW 43.105.054,
- the requesting agency shall provide for a written agreement between the agencies that conforms to the policies of the office of cybersecurity.

Chapter 39.34 RCW = Interlocal Cooperation Act

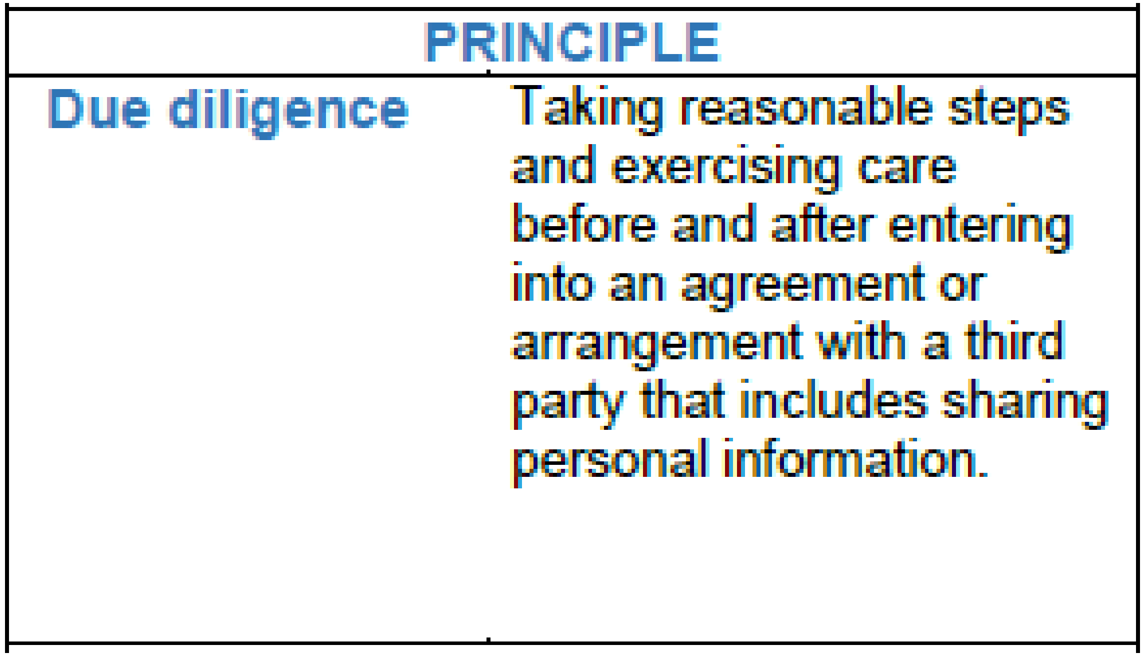
Public agency = all state and local agencies

Covers sharing between agencies

OCIO Policy #141.10

"When sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law."

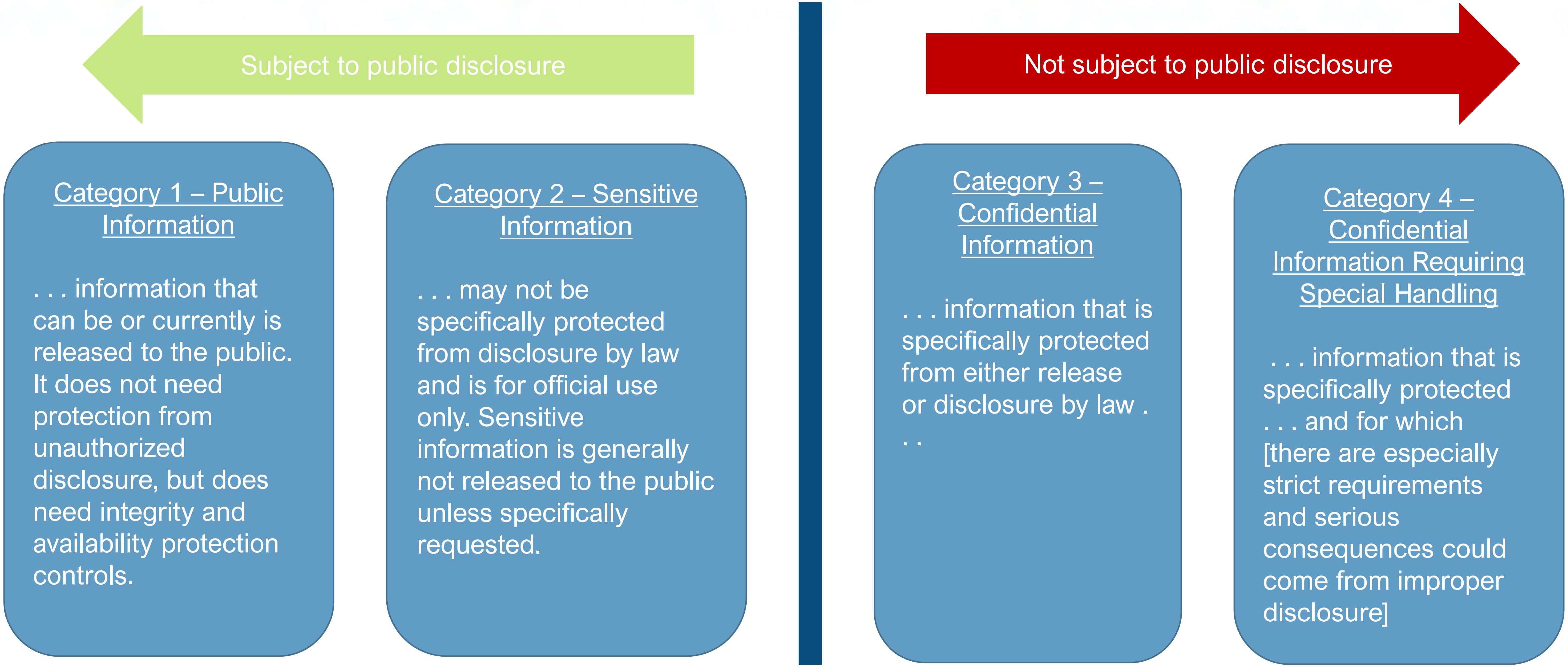
Due diligence



PRINCIPLE	
Due diligence	Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.

Steps to implementation

- Understand data classification
- Identify when an agreement is needed
- Execute appropriate agreements



Subject to public disclosure

Not subject to public disclosure

Category 1 – Public Information

. . . information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information

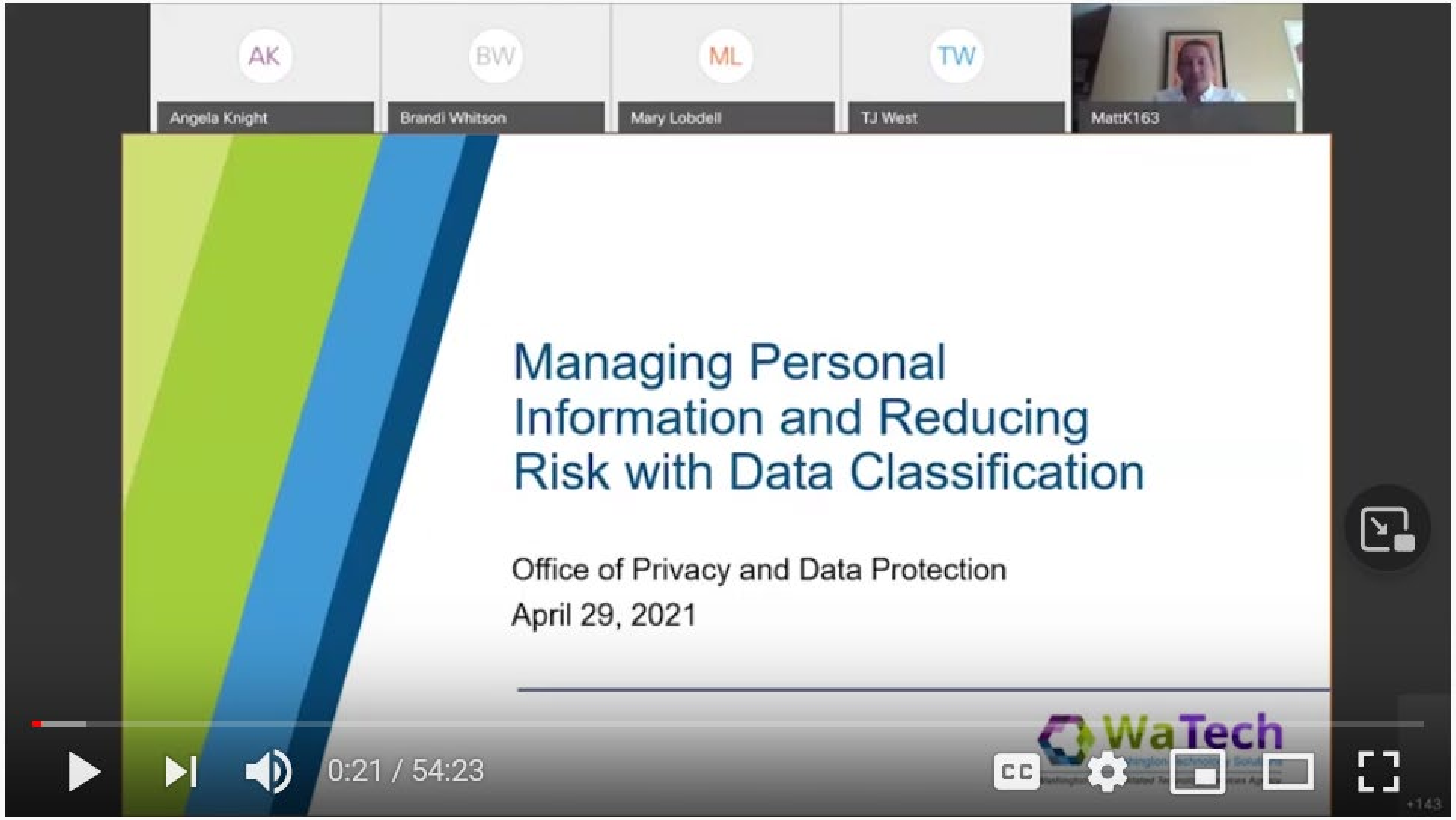
. . . may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information

. . . information that is specifically protected from either release or disclosure by law . . .

Category 4 – Confidential Information Requiring Special Handling

. . . information that is specifically protected . . . and for which [there are especially strict requirements and serious consequences could come from improper disclosure]



Managing Personal Information and Reducing Risk with Data Classification

Office of Privacy and Data Protection
April 29, 2021

Available on OPDP's Government Agency Resources page

OPDP

Do you know where your data is?

- Gates to ensure information is only shared when appropriate
- Data sharing checklist as part of contracting process
- Data sharing not otherwise tied to a contract
- Data transmission inventory
- Appropriate scope of “data sharing”
- Policies to require data sharing agreements

Data Share Request Forms

Allows agencies to gather information from data requestors about:

- Requested data
- Intended use
- Authority to share
- Security and privacy controls

OPDP

Data Share Request Forms

Primary privacy benefit = ability to evaluate against WSAPP

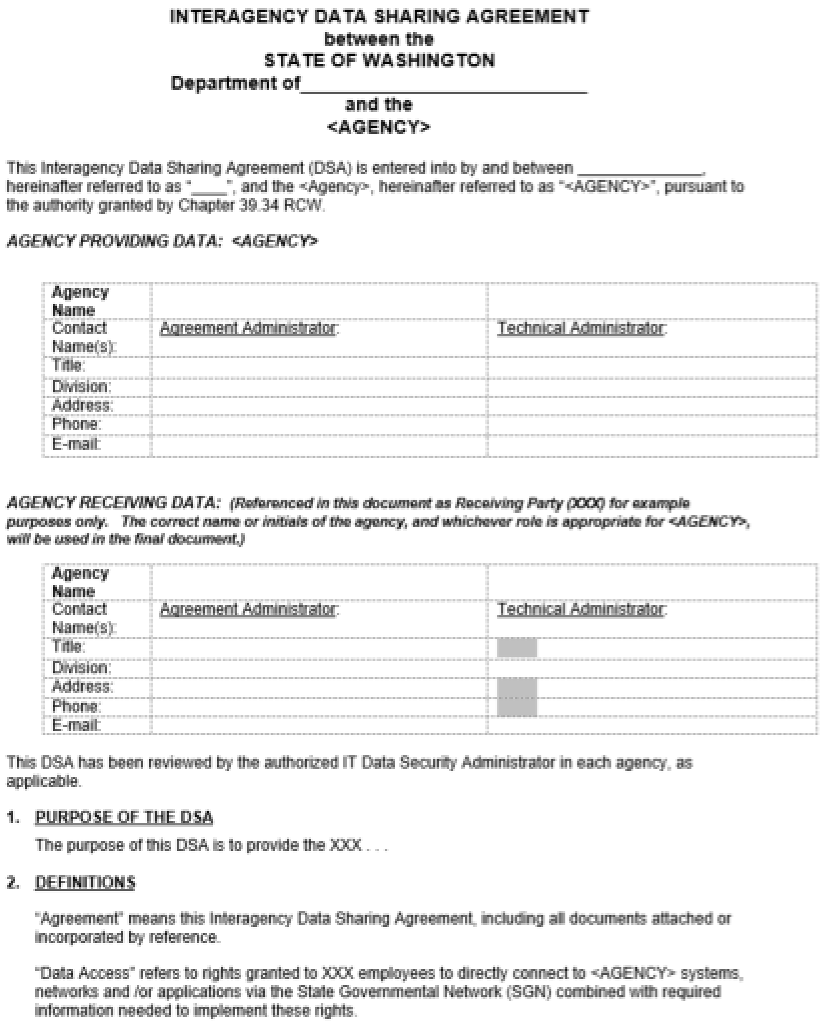
- Verify consistency with original intended use (Purpose limitation)
- Ensure both the intended use and shared data are limited in scope (Data minimization)
- Confirm authority to share (Lawful, fair, and responsible use)
- Evaluate other possible privacy impacts, and consistency with agency mission and values (Lawful, fair, and responsible use)

OCIO Policy #141.10

The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following:

(1) The data that will be shared.
(2) The specific authority for sharing the data.
(3) The classification of the data shared
(4) Access methods for the shared data.
(5) Authorized users and operations permitted
(6) Protection of the data in transport and at rest.
(7) Backup requirements for the data if applicable
(8) Other applicable data handling requirements.

Sample Data Sharing Agreement



INTERAGENCY DATA SHARING AGREEMENT
between the
STATE OF WASHINGTON
Department of______________________________
and the
<AGENCY>

This Interagency Data Sharing Agreement (DSA) is entered into by and between _______________, hereinafter referred to as "____", and the <Agency>, hereinafter referred to as "<AGENCY>", pursuant to the authority granted by Chapter 39.34 RCW.

AGENCY PROVIDING DATA: <AGENCY>

Agency Name		
Contact Name(s):	Agreement Administrator:	Technical Administrator:
Title:		
Division:		
Address:		
Phone:		
E-mail:		

AGENCY RECEIVING DATA: ***(Referenced in this document as Receiving Party (XXX) for example purposes only. The correct name or initials of the agency, and whichever role is appropriate for <AGENCY>, will be used in the final document.)***

Agency Name		
Contact Name(s):	Agreement Administrator:	Technical Administrator:
Title:		
Division:		
Address:		
Phone:		
E-mail:		

This DSA has been reviewed by the authorized IT Data Security Administrator in each agency, as applicable.

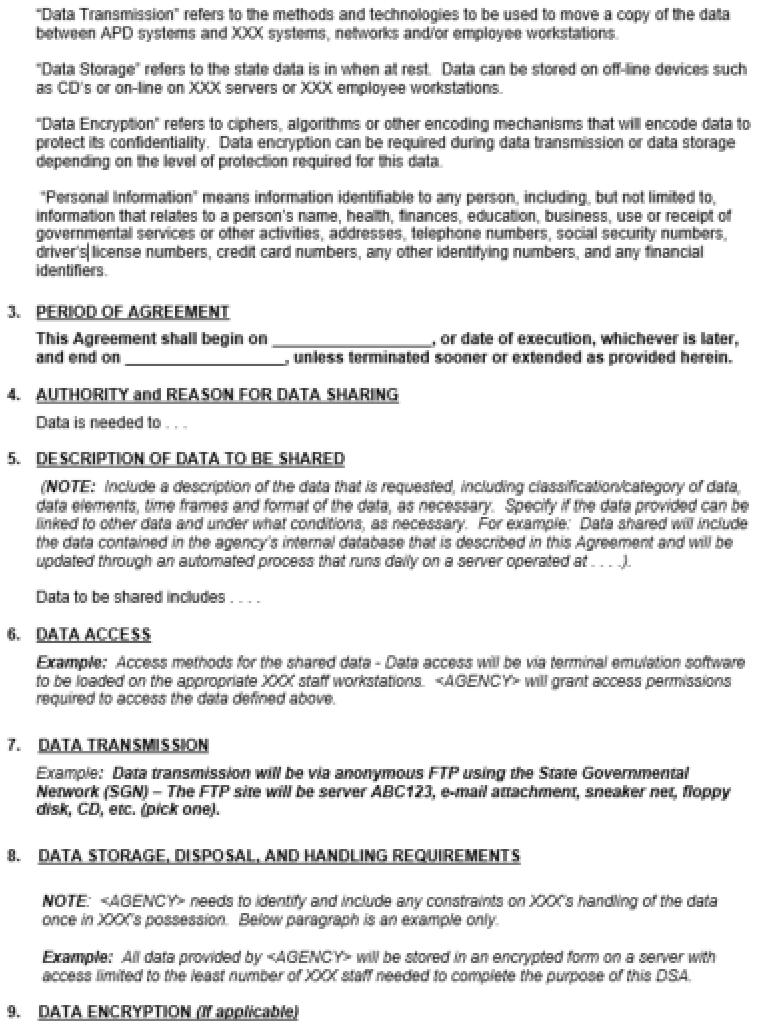
1. **PURPOSE OF THE DSA**

The purpose of this DSA is to provide the XXX . . .

2. **DEFINITIONS**

"Agreement" means this Interagency Data Sharing Agreement, including all documents attached or incorporated by reference.

"Data Access" refers to rights granted to XXX employees to directly connect to <AGENCY> systems, networks and /or applications via the State Governmental Network (SGN) combined with required information needed to implement these rights.



"Data Transmission" refers to the methods and technologies to be used to move a copy of the data between APD systems and XXX systems, networks and/or employee workstations.

"Data Storage" refers to the state data is in when at rest. Data can be stored on off-line devices such as CD's or on-line on XXX servers or XXX employee workstations.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

"Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

3. **PERIOD OF AGREEMENT**

This Agreement shall begin on ___________________, or date of execution, whichever is later, and end on ___________________, unless terminated sooner or extended as provided herein.

4. **AUTHORITY and REASON FOR DATA SHARING**

Data is needed to . . .

5. **DESCRIPTION OF DATA TO BE SHARED**

*(**NOTE:** Include a description of the data that is requested, including classification/category of data, data elements, time frames and format of the data, as necessary. Specify if the data provided can be linked to other data and under what conditions, as necessary. For example: Data shared will include the data contained in the agency's internal database that is described in this Agreement and will be updated through an automated process that runs daily on a server operated at . . . .).*

Data to be shared includes . . . .

6. **DATA ACCESS**

Example: *Access methods for the shared data - Data access will be via terminal emulation software to be loaded on the appropriate XXX staff workstations. <AGENCY> will grant access permissions required to access the data defined above.*

7. **DATA TRANSMISSION**

Example: ***Data transmission will be via anonymous FTP using the State Governmental Network (SGN) – The FTP site will be server ABC123, e-mail attachment, sneaker net, floppy disk, CD, etc. (pick one).***

8. **DATA STORAGE, DISPOSAL, AND HANDLING REQUIREMENTS**

NOTE: *<AGENCY> needs to identify and include any constraints on XXX's handling of the data once in XXX's possession. Below paragraph is an example only.*

Example: *All data provided by <AGENCY> will be stored in an encrypted form on a server with access limited to the least number of XXX staff needed to complete the purpose of this DSA.*

9. **DATA ENCRYPTION *(If applicable)***

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

✓ The data that will be shared.

✓ The classification of the data shared

Data to be shared includes . . .

5. DESCRIPTION OF DATA TO BE SHARED

- *description of the data that is requested*
- *classification/category of data*
- *data elements*
- *time frames for data disclosure or exchange (both when and for how long)*
- *format of the data*
- *Specify if the data provided can be linked to other data and under what conditions*

OPDP

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

✓ The specific authority for sharing the data.

4. AUTHORITY AND REASON FOR DATA SHARING

- The legal authority for sharing data identified in this agreement is …
- Data is needed to . . .

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

✓ Access methods for the shared data.

6. DATA ACCESS

- *Access methods for the shared data*
- *E.g. Data access will be via terminal emulation software to be loaded on the appropriate XXX staff workstations.*
- *<AGENCY> will grant access permissions required to access the data defined above.*
- *Requirements for Access. Access to data shall be limited to staff whose duties specifically require access to such data in the performance of their assigned duties.*

OPDP

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

✓ Authorized users and operations permitted.

8. DATA STORAGE, DISPOSAL, AND HANDLING REQUIREMENTS

NOTE: *<AGENCY> needs to identify and include any constraints on XXX's handling of the data once in XXX's possession. Below paragraph is an example only.*

Example: *All data provided by <AGENCY> will be stored in an encrypted form on a server with access limited to the least number of XXX staff needed to complete the purpose of this DSA.*

Data Disposal. At the end of the contract or when the data is no longer needed, data shall be returned to <AGENCY> or destroyed via an authorized method. Acceptable methods of destruction are as follows:

10. INTENDED USE OF DATA

Example: *The data described above shall be used for analysis purposes only to prepare required annual business summaries published by XXX. Specify operations permitted.*

11. CONSTRAINTS ON USE OF DATA

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

- ✓ Protection of the data in transport and at rest.

7. DATA TRANSMISSION

Example: Data transmission will be via anonymous FTP using the State Governmental Network (SGN) – The FTP site will be server ABC123, e-mail attachment, sneaker net, floppy disk, CD, etc. (pick one).

9. DATA ENCRYPTION *(If applicable)*

Example: <AGENCY> and XXX have agreed to use a software tool to encrypt data prior to transmission and during Data Storage. The tool is ____________ (Example: PKZIP PRO; the encryption algorithm to be use is Password + 3DES). The password will be transmitted separately from any data transmission event.

OPDP

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

- ✓ Backup requirements for the data if applicable

8. DATA STORAGE, DISPOSAL, AND HANDLING REQUIREMENTS

Example: Data stored for backup purposes. Data may be stored on portable media or non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of XXX's existing, documented backup process for business continuity or disaster recovery purposes. Data must be protected and disposed of as required by this agreement.

How the sample contract reflects OCIO policy 141.10 (4.2) DSA standards

✓ Other applicable data handling requirements.

12. **SECURITY OF DATA**

13. **NON-DISCLOSURE OF DATA**

14. **DATA CONFIDENTIALITY**

15. **OVERSIGHT**

16. **INCIDENT RESPONSE**

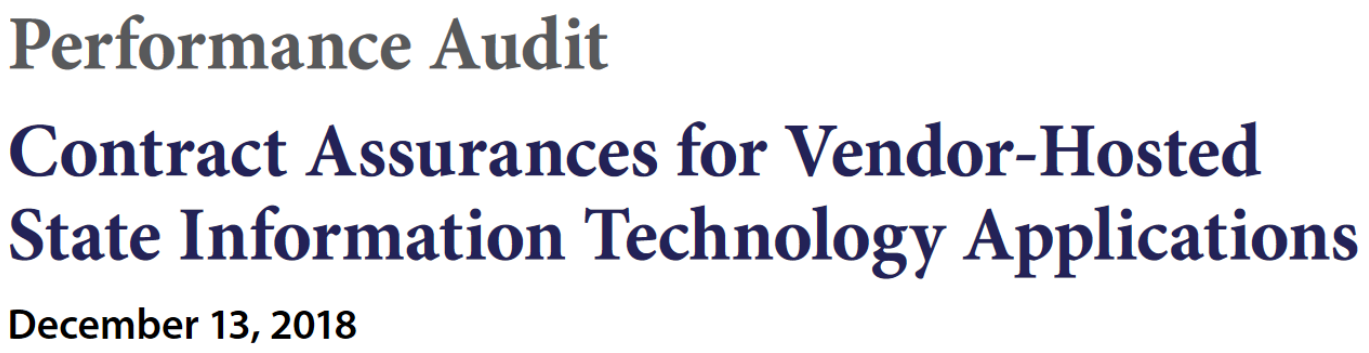
Things to keep in mind regarding the sample template:

- Intended to be a sample for those entities that do not currently have data share agreements
- Can be used to address gaps in current data share agreements
- Model terms required under ESSB 5432 will come from AGO/OCS/OPDP Report (12/1/21)
- Sample does not include terms less likely to be in contracts with interagency partners like:
  - Indemnification clauses
  - Cyber liability insurance

Beyond 141.10

- Incident response
    - Timing, cost, roles and responsibilities
- Compliance monitoring and enforcement
    - How to demonstrate compliance
- Cyber liability insurance
- Indemnification
- Restrictions on disclosure, publication, notice
- Compliance with OCIO security policies
- Pass-through requirements to subcontractors
- Appropriate contract owners

Other resources

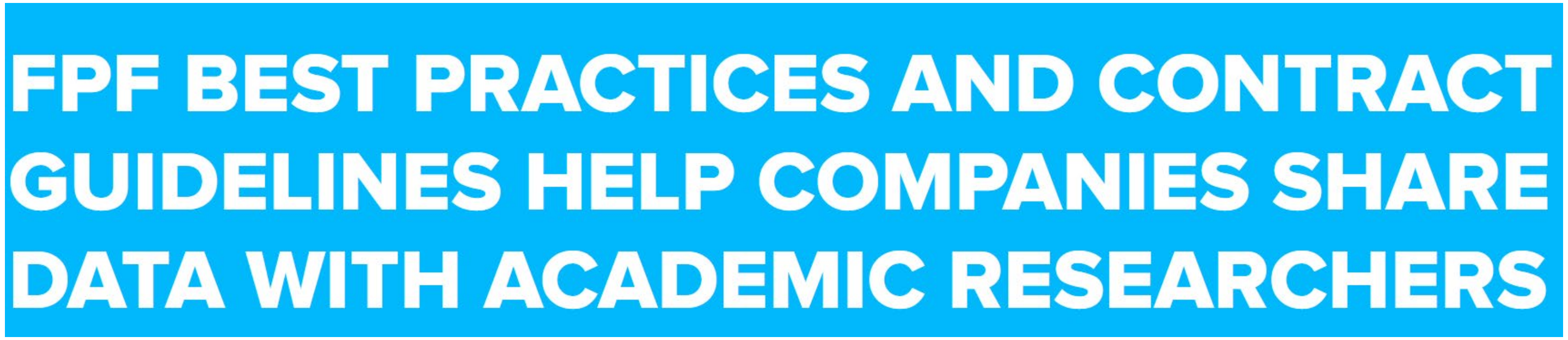


Performance Audit

Contract Assurances for Vendor-Hosted State Information Technology Applications

December 13, 2018

SAO report



FPF BEST PRACTICES AND CONTRACT GUIDELINES HELP COMPANIES SHARE DATA WITH ACADEMIC RESEARCHERS

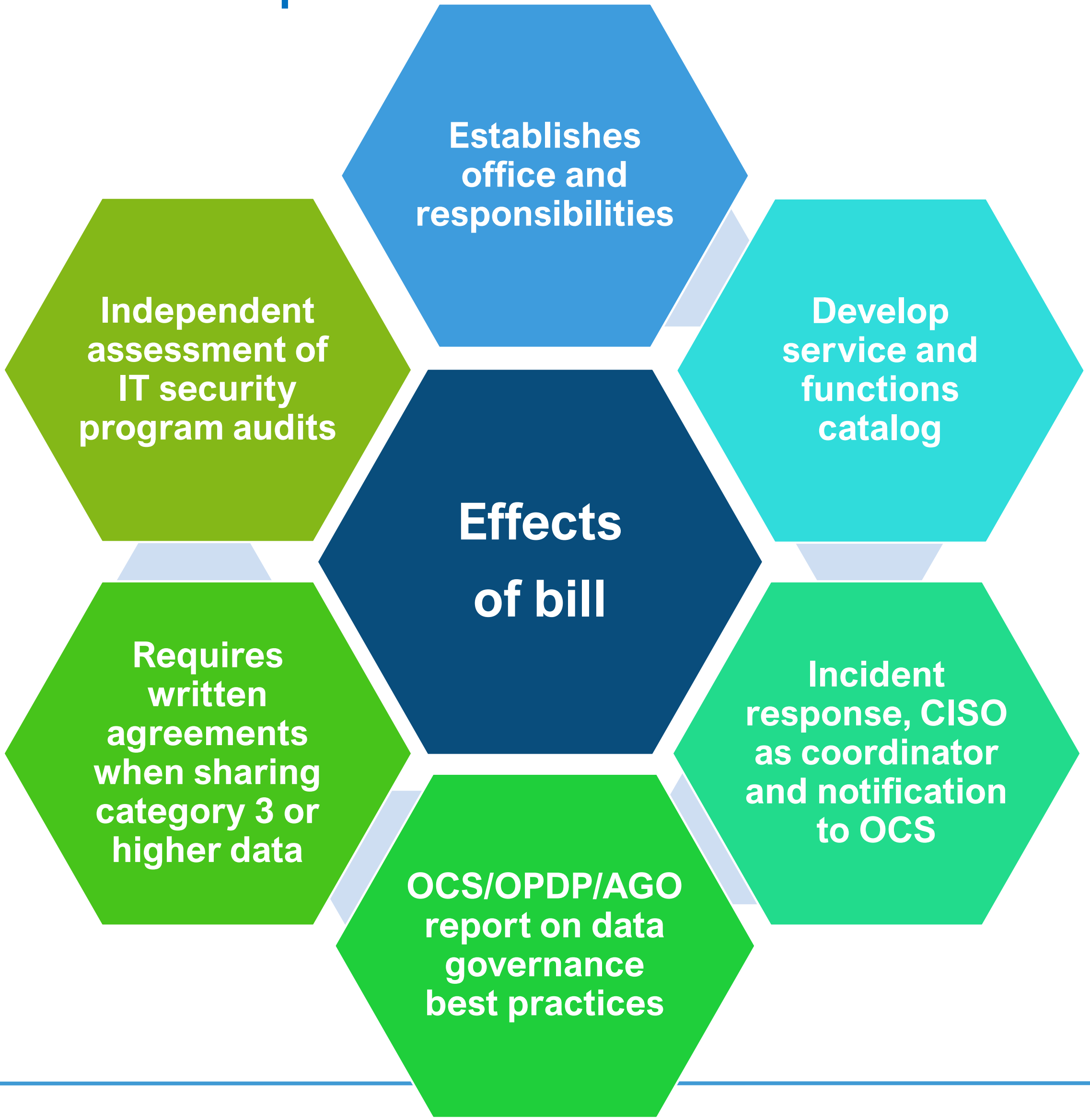
FPF guidelines

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Other cybersecurity workstreams

OPDP

ESSB 5432 impacts and requirements



Effects of bill

Establishes office and responsibilities

Develop service and functions catalog

Incident response, CISO as coordinator and notification to OCS

OCS/OPDP/AGO report on data governance best practices

Requires written agreements when sharing category 3 or higher data

Independent assessment of IT security program audits

Existing requirements restated in new law

- Agency cybersecurity programs and adherence to security policy
- Independent compliance audits of cybersecurity programs
- Reporting of cybersecurity incidents to OCS

New requirements for OCS in law

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Develop catalog of enterprise services and functions

- Updated and published biennially

Create model incident response plan for agency adoption

- For incidents that impact multiple agencies, impact more than 10,000 citizens, involve a nation state actor, or are likely to be in the public domain.

Develop policy related to incident response

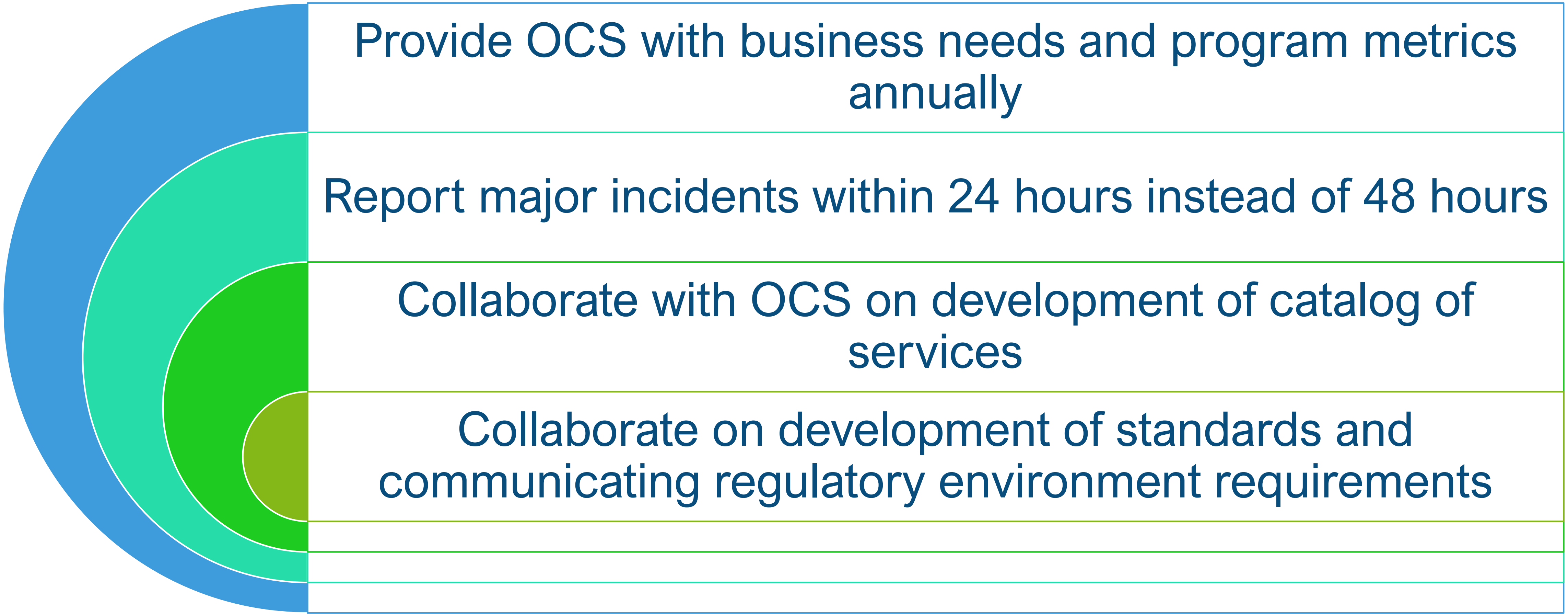
- Includes defining what constitutes a “major” cybersecurity incident.

CISO as the point of contact for major cyber incidents

- Applies to major incidents and may be delegated at CISO’s discretion.

OPDP

New requirements for agency programs



Provide OCS with business needs and program metrics annually

Report major incidents within 24 hours instead of 48 hours

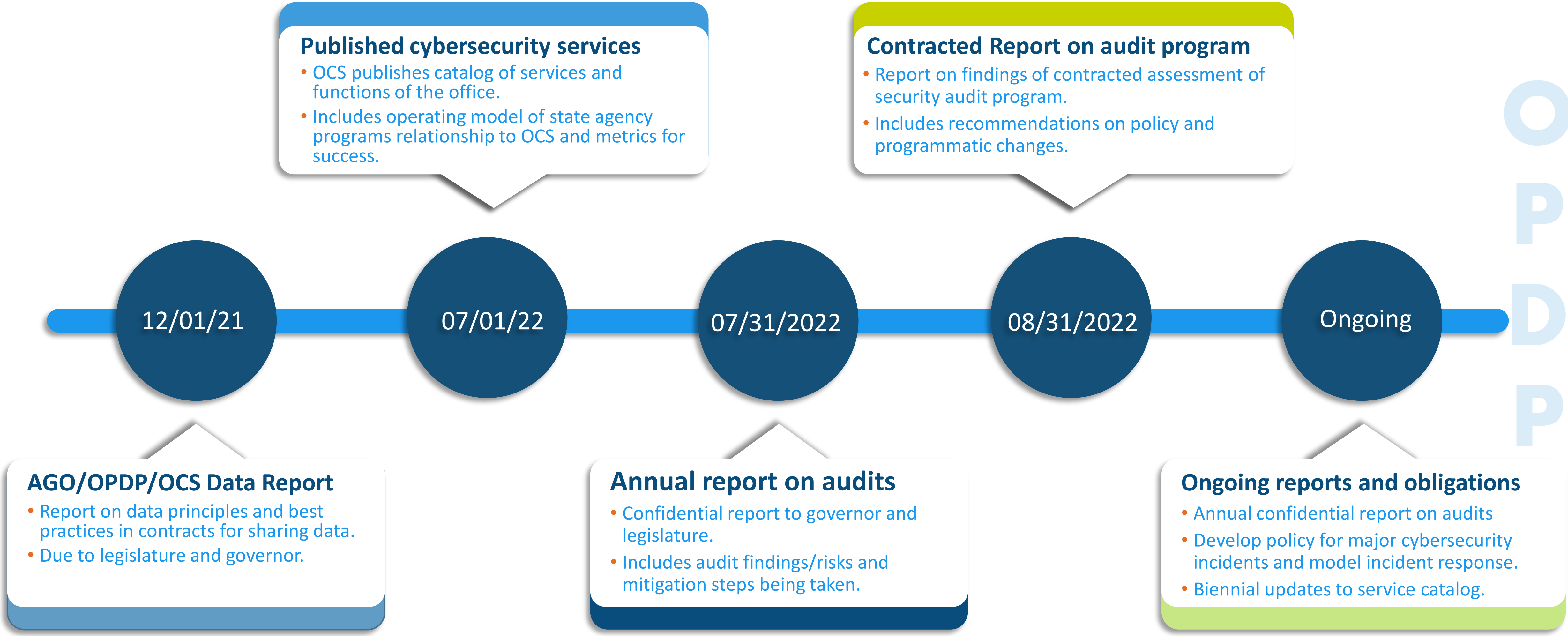
Collaborate with OCS on development of catalog of services

Collaborate on development of standards and communicating regulatory environment requirements

Required workstreams and deliverables

- Collaborative report with AGO/OPDP/OCS on data principles/contracts
- Published catalog of services and functions and report on metrics, services, and operating model of state agency security programs.
- First annual report on cybersecurity audit findings/risks and mitigation steps.
- Report on findings of contracted security assessment related to cybersecurity audits in the state.
- Develop policy related to major cybersecurity incidents and incident response.
- Create a model incident response plan for agency adoption.
- Confidential report on cybersecurity risks and their mitigation.
- Update and publish cybersecurity catalog, functions, and metrics.

Deliverables of ESSB 5432 in chronological order



12/01/21

AGO/OPDP/OCS Data Report

- Report on data principles and best practices in contracts for sharing data.
- Due to legislature and governor.

07/01/22

Published cybersecurity services

- OCS publishes catalog of services and functions of the office.
- Includes operating model of state agency programs relationship to OCS and metrics for success.

07/31/2022

Annual report on audits

- Confidential report to governor and legislature.
- Includes audit findings/risks and mitigation steps being taken.

08/31/2022

Contracted Report on audit program

- Report on findings of contracted assessment of security audit program.
- Includes recommendations on policy and programmatic changes.

Ongoing

Ongoing reports and obligations

- Annual confidential report on audits
- Develop policy for major cybersecurity incidents and model incident response.
- Biennial updates to service catalog.

Thank you

Questions?

OPDP

www.privacy.wa.gov

www.cybersecurity.wa.gov