

Privacy and Data Sharing Agreement Best Practices Report

December 16, 2021

Washington state lawmakers want to strengthen cybersecurity in Olympia after massive data breach

Feb. 9, 2021 at 5:26 pm | Updated Feb. 9, 2021 at 5:30 pm

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

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

O
P
D
P

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

O
P
D
P

Report Submitted December 1, 2021

Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report

- Findings and recommendations related to:
 - Cybersecurity
 - Privacy
 - Data sharing agreements

Data Sharing Agreement Implementation Guidance

Sample DSA for defined extract or system access

Sample DSA for multiparty relationship with broad sharing

O
P
D
P

Agenda

In-scope

Privacy Best Practices

Data Sharing Agreement Best Practices

Supplemental DSA materials

Out-of-scope

Cybersecurity findings and recommendations

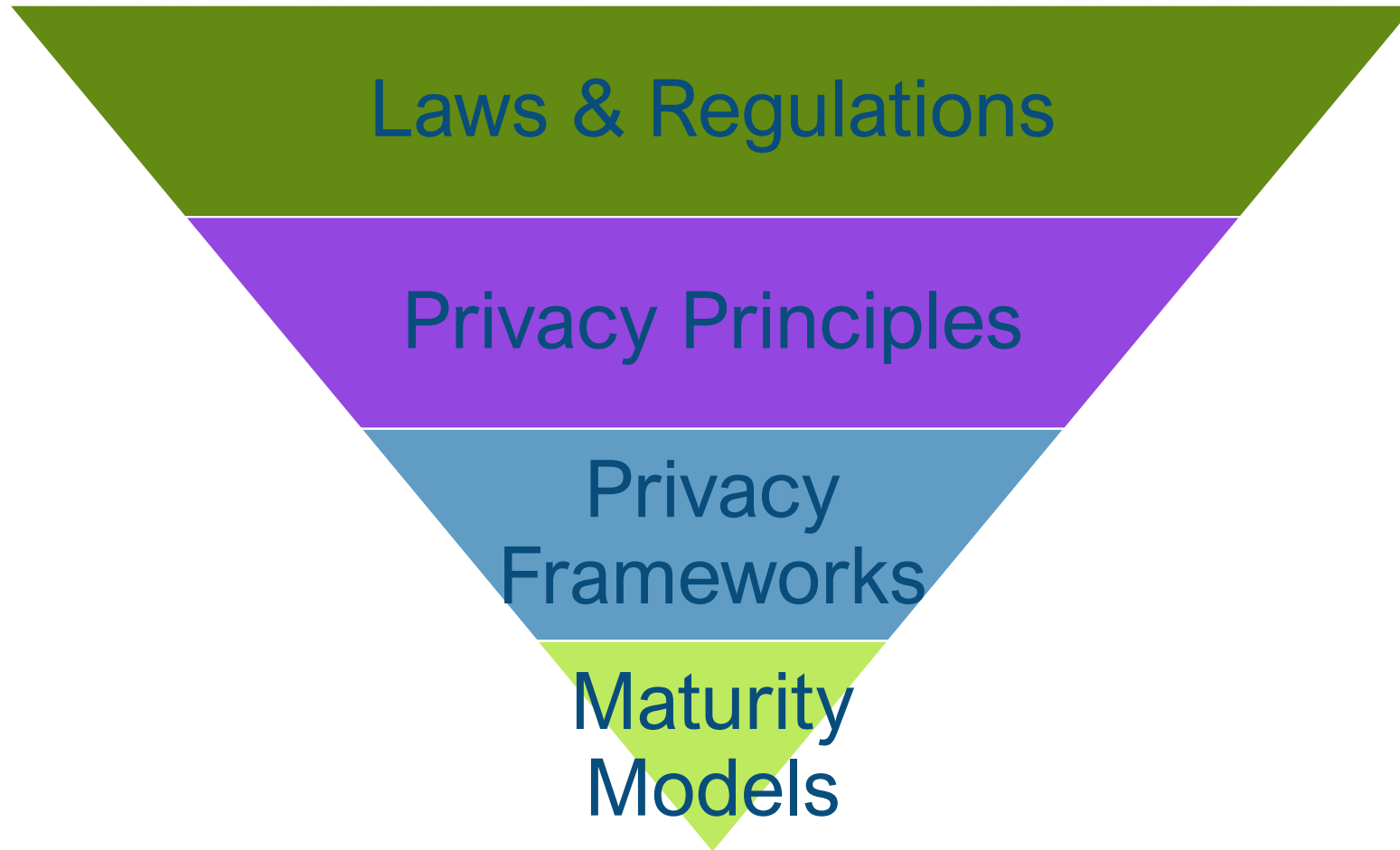
Reminder: This presentation and related materials are an informational resource and not provided for the purpose of giving legal advice. The information provided does not represent the legal opinion of any Washington state agency.

O
P
D
P

Privacy Best Practices – Where to Start?



O
P
D
P



Effective Privacy and Data Protection

O
P
D
P

Laws and Regulations

Privacy laws:

- Set baseline requirements
- Should be followed when applicable
- Offer relative certainty and predictability

Privacy laws are not:

- Privacy frameworks
- Maturity models
- Always detailed enough to effectively operationalize
- A guarantee of appropriate privacy and data protection

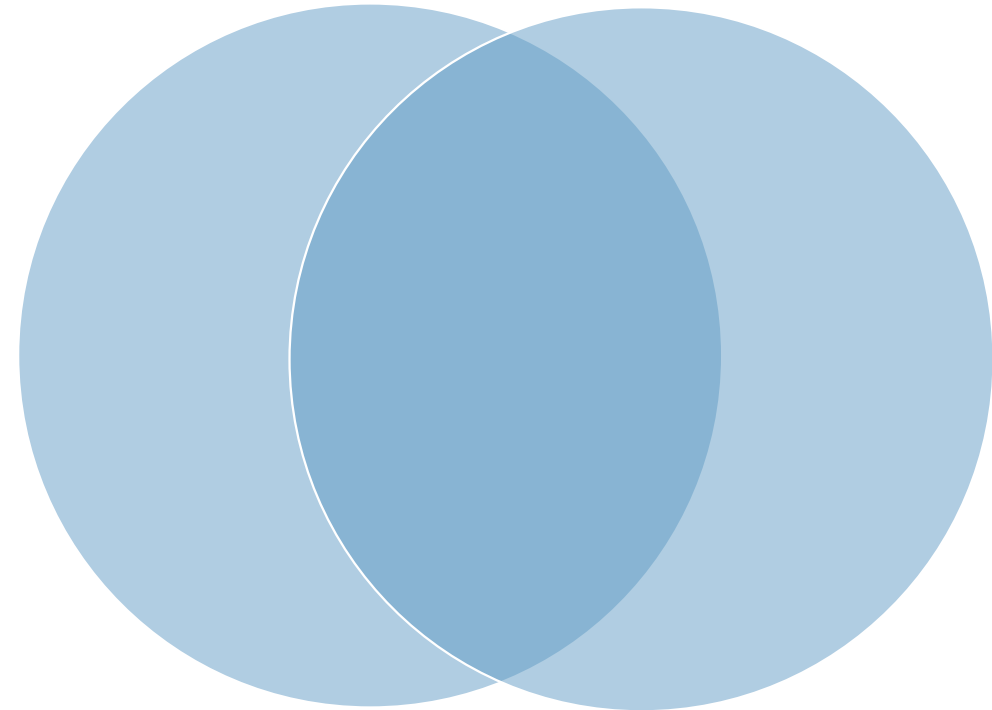
Laws and Regulations

Gaps may exist where laws:

- Do not establish strong enough protections to meet people's expectations
- Contemplate changes in technology and business practices
- Account for an organization's specific mission or cultural context

Legal Requirements

Effective Privacy Controls



O
P
D
P

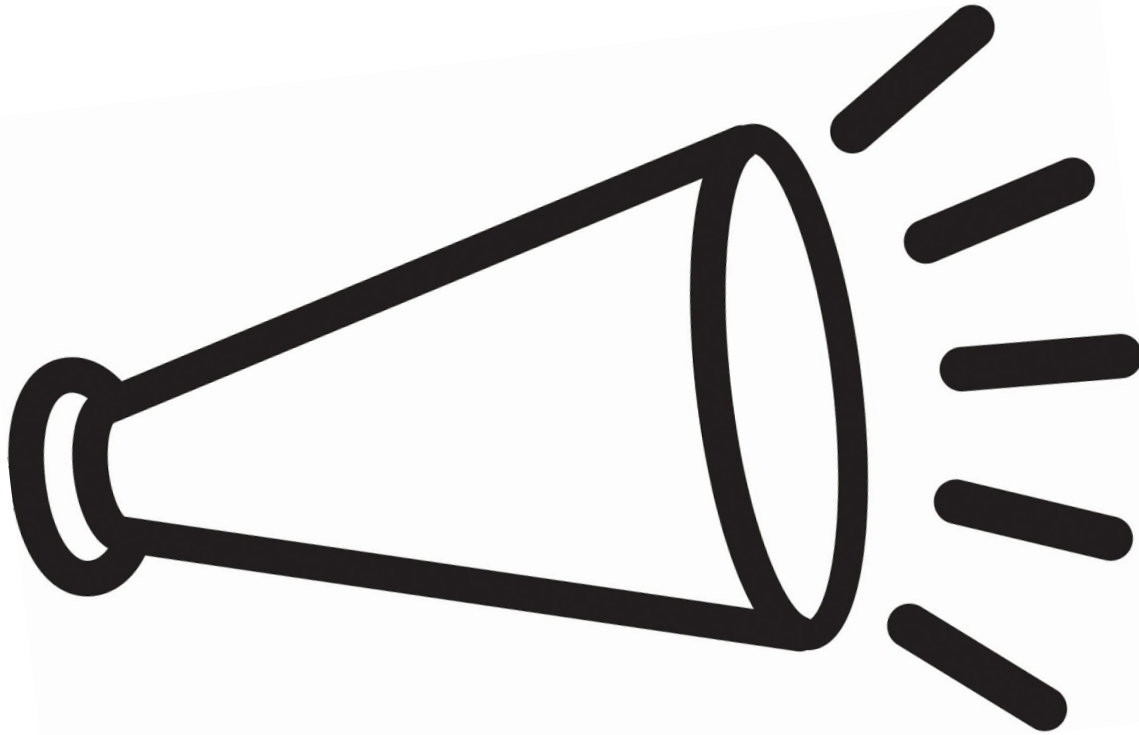
Privacy Principles

- Privacy principles = fundamental values to guide practices
- Fair Information Practice Principles articulated nearly half a century ago
- Variations adopted by federal agencies and international organizations
- Concepts incorporated in privacy laws
- No single, authoritative version



O
P
D
P

Adherence to Privacy Principles



- Talk about them
- Adopt formal policies
- Require training; conduct other awareness activities
- Promote workforce development
- Incorporate in other work

O
P
D
P

Privacy Frameworks

Frameworks:

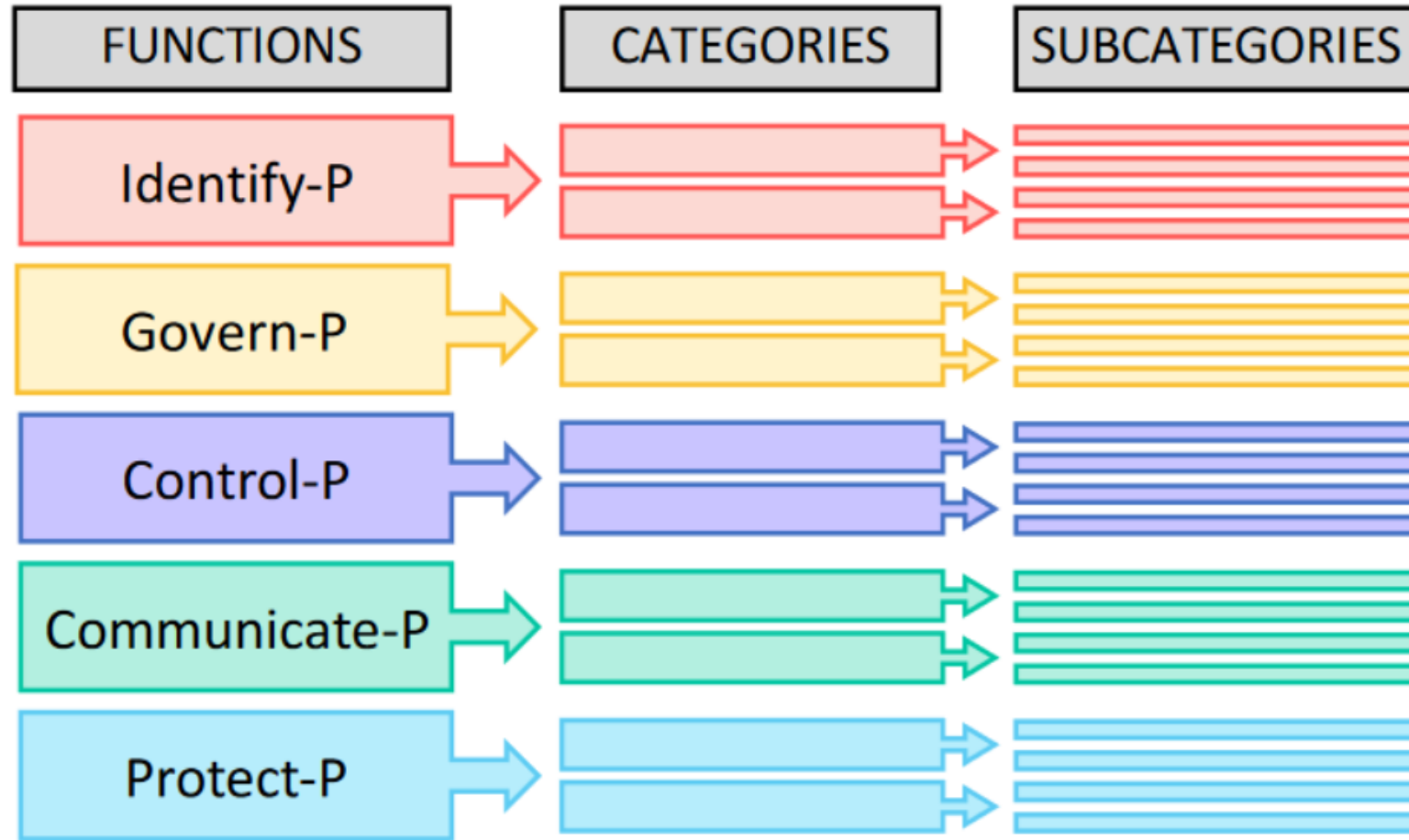
- Are NOT about requirements
- But can be mapped to legal requirements
- Provide the structure and basis to implement privacy practices and operationalize privacy program
- Can be applied in part to account for types of information, risk profile, resources, culture and current maturity

Flexibility is a key strength, but can be applied in a way that is:

- Too lenient, which leads to ineffective practices
- Too conservation, which leads to inefficient practices

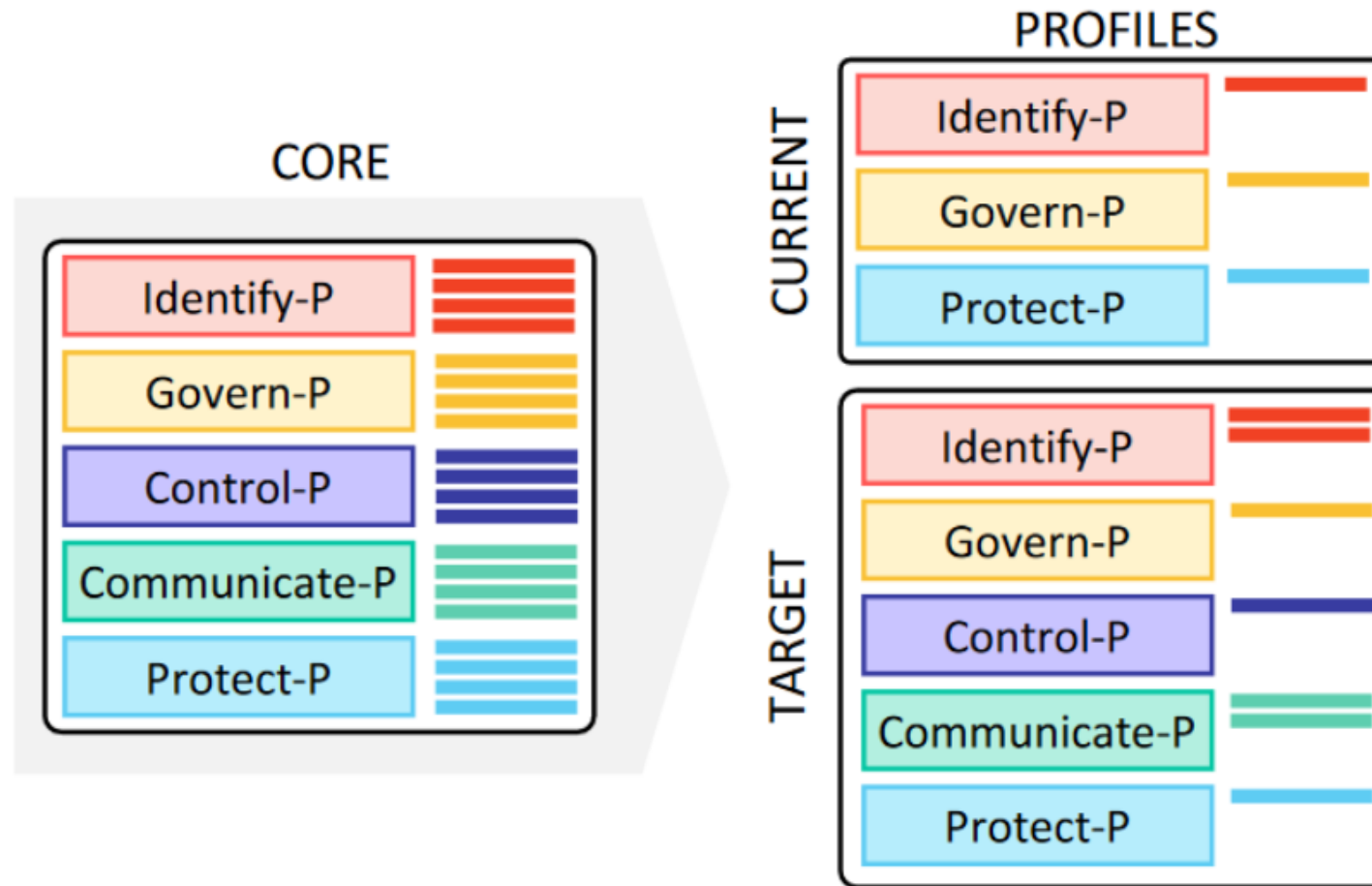
O
P
D
P

NIST Privacy Framework



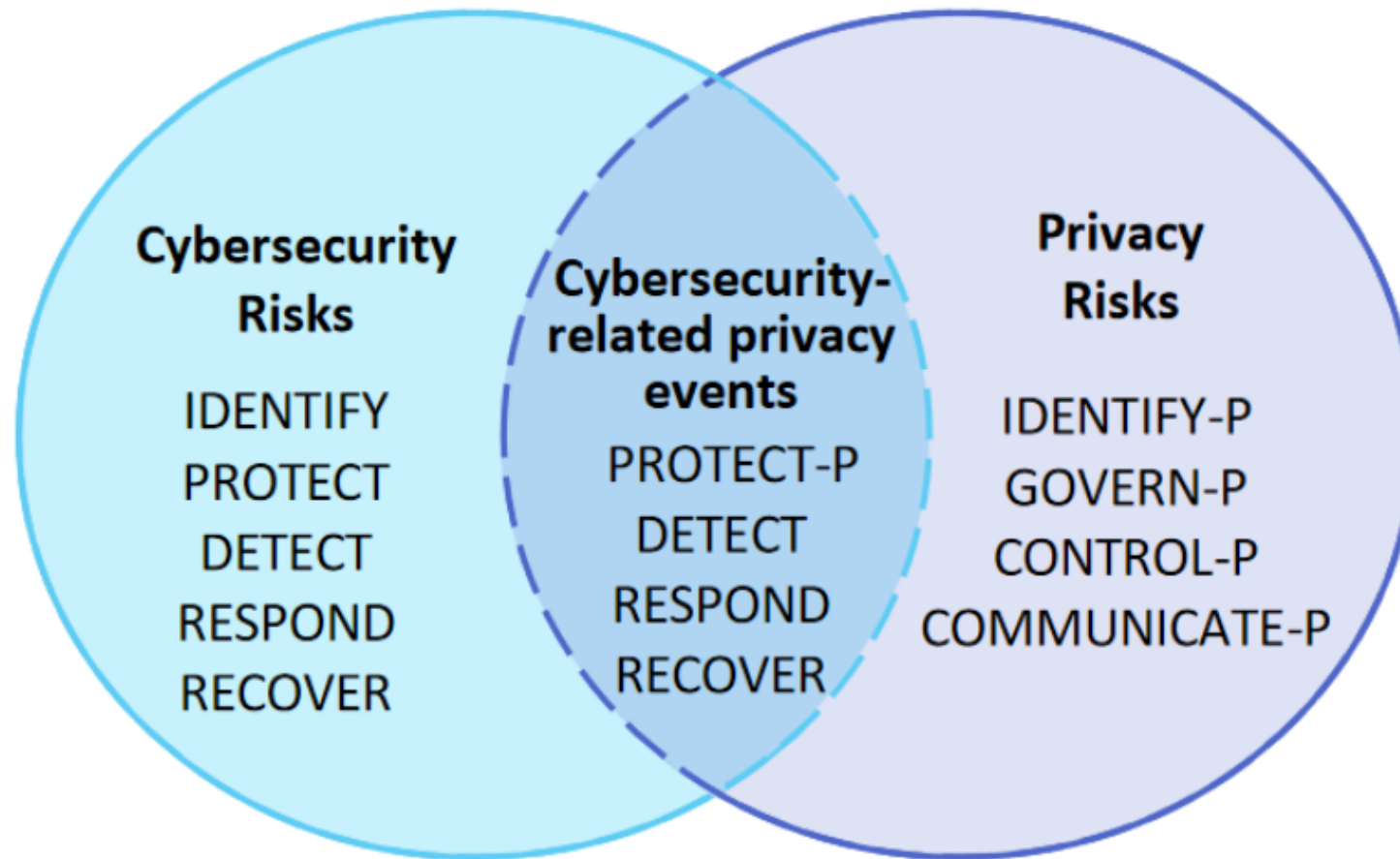
O
P
D
P

NIST Privacy Framework



O
P
D
P

NIST Privacy Framework



O
P
D
P

Maturity Models

Laws = what you have to do

Frameworks = what you need or want to do

Maturity model = how well you're doing it

O
P
D
P

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|--|--|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| MANAGEMENT (14 criteria) cont. | The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures. | | | | | |
| Personal Information Identification and Classification (1.2.3) | The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures. | The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information. | Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information. | All personal information collected, used, stored and disclosed within the entity has been classified and risk rated. | All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification. | Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification. |

Misc. Privacy Recommendations

OPDP should:

- Develop additional training and awareness tools
- Tailor resources to address the greatest privacy risks
- Incorporate WSAPP in new resources, such as privacy impact assessments
- Promote workforce development
- Publish privacy impact assessment templates for major IT projects that involve personal information

Agencies should:

- Continue to invest in their privacy programs
- Designate privacy contacts, even if privacy is not that person's full-time job
- Make training mandatory for some or all staff
- Implement formal privacy policies that incorporate privacy principles



Data Sharing Agreements

O
P
D
P

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

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 Security Standard #141.10

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

O
P
D
P

Other benefits

- Document all data flows
- Ensure appropriate protections to prevent incidents and misuse
- Outline responsibilities and mitigate impacts when an incident does occur
- Creates a gate to vet data sharing relationships

O
P
D
P

How are we doing?

O
P
D
P

Steps to implementation



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

O
P
D
P

← 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.

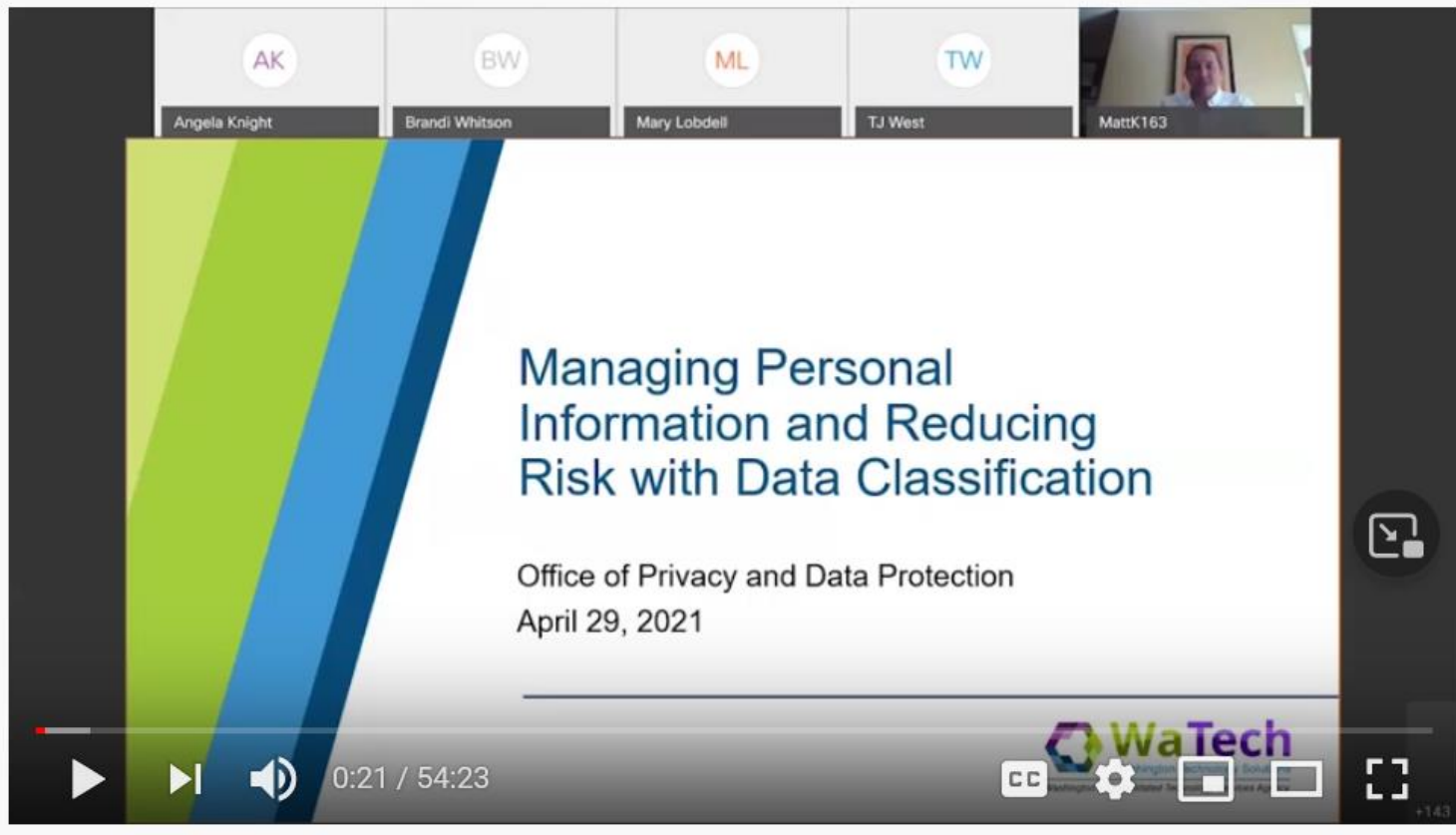
Category 3 – Confidential Information

... 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]

O
P
D
P



AK BW ML TW
Angela Knight Brandi Whitson Mary Lobdell TJ West MattK163

Managing Personal Information and Reducing Risk with Data Classification

Office of Privacy and Data Protection
April 29, 2021

0:21 / 54:23

WaTech

Available on [OPDP's Government Agency Resources](#) page

OPDP

Identify – What is data sharing?

Making data available to third parties.

O
P
D
P

Identify – What is data sharing?

Making data available to third parties.

Types of sharing include:

- Data transmissions
- Data hosting
- System access

Functions include routine sharing necessary for an agency to perform core functions, such as sharing with:

- Contractors
- Service providers
- Other public agencies

O
P
D
P

Identify – Controls and processes

- Consider all ways third parties access information
- Log and track data sent outside of systems
- Build safeguards into existing processes
 - Contracting
 - Data product development
- Create common intake tools
- Develop approval requirements
- Policies to require data sharing agreements

O
P
D
P

Implement – What is a DSA?

- Not defined in statute or OCIO policy
- Focus on appropriate data sharing language
- No requirement to have a document called a “Data Sharing Agreement”
- No requirement that DSA be a separate document

O
P
D
P

Implement – Flexibility required

- Not one, single version of model terms appropriate for all circumstances
- Consider:
 - Number of parties
 - Direction of sharing
 - Relationship between the parties
 - Method of sharing
 - Purpose of sharing
 - Frequency of sharing
 - Scope of sharing

O
P
D
P

Implement – Flexibility required

Flexible, not lackadaisical

O
P
D
P

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) Storage and disposal of data no longer required.
- (8) Backup requirements for the data if applicable
- (9) Other applicable data handling requirements.

| Should Include | |
|---|---|
| Purpose and specific authority for sharing. | Backup requirements if applicable. |
| A description of the data, including classification. | Incident notification and response. |
| Authorized uses. | Monitoring and enforcement. |
| Authorized users or classes of users. | Awareness and/or training. |
| Protection of the data in transit if the arrangement involves transmission. | Compliance with additional relevant OCIO security requirements based on the type of data sharing. |
| Secure storage for data maintained outside the agency. | Any other requirements imposed by law, regulation, contract or policy. |
| Data disposal. | |

O
P
D
P

| Might Include |
|--|
| Term and termination. |
| Off-shore prohibition. |
| Cyber liability insurance. |
| Indemnification. |
| Third party requests. |
| Restrictions on disclosure or publication. |
| Other widely applicable contract terms. |

O
P
D
P



Data Sharing Agreement Implementation Guidance

December 2021, v.1

O
P
D
P

Should include – Authorized uses

Describe how the information may be used, including prohibited uses. When the agreement is with a contractor performing functions on behalf of an agency, authorized uses should typically be limited to those functions.

Examples

| | |
|--|--|
| General limitation on permitted uses | This Agreement does not constitute a release of Confidential Information for the Receiving Party's discretionary use and may be accessed and used only to carry out the purposes described in this DSA. Any ad hoc analyses or other use of the data, not specified in this DSA, is not permitted without the prior written agreement of [AGENCY]. |
| General limitation on permitted uses for non-vendors | The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose, justification, and permitted uses of this DSA, except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Data. |
| General limitation on permitted uses for vendors | The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except: (1) as provided by law; or, (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information. |
| Prohibition on commercial or personal use | Receiving Party shall not access or use the Confidential Information for any commercial or personal purpose. |
| Prohibiting data linkage | The Confidential Information shared under this DSA may not be linked with other data sources without prior written agreement of [Agency]. |
| Allowing data linkage | The Confidential Information shared under this DSA may be linked with the following data sources: <i>[list sources]</i> <i>[When allowing data linkage, consider possible impacts such as whether the combined data will be shared with other parties, and whether Agency data will remain identifiable after combination]</i> |
| Prohibition on data modifications | The Receiving Party is not authorized to update or change any Data in [Agency system], and any updates or changes will be cause for immediate termination of this DSA. |

Might include – Off-shore prohibition

Include a prohibition on storing or sharing information outside of the United States when prohibited by law, contract or policy. Even when not formally prohibited, before allowing information to be stored outside of the United States consider the ability to protect the information and seek recourse in a foreign jurisdiction. Also consider the criticality and sensitivity of the information, including the impact of the loss of confidentiality, integrity or availability.

Examples

| | |
|---------------------|---|
| General prohibition | Receiving Party must maintain all hardcopies containing Confidential Information in the United States. Receiving Party may not directly or indirectly (including through Subcontractors) transport or maintain any Data, hardcopy or electronic, outside the United States unless it has advance written approval from [Agency]. |
|---------------------|---|

Using implementation guidance

- For each type of term, there may be multiple appropriate terms or none.
- Be ready to add content and narrative.
- Some terms overlap – one contract clause can cover multiple concepts
- Only exercise flexibility when appropriate for specific relationships
- Only exercise flexibility when appropriate for specific terms

O
P
D
P

Agreement for system access or pre-defined extract

- More appropriate for DSA when greater specificity is possible
- Includes alternative language for data sharing through system access transmitting data extract
- Contemplates sharing multiple types of information with one party
 - General requirements laid out in DSA, with new exhibits for each data sharing arrangement
- Includes sample data disposal certification document

Overarching agreement for multi-party relationship

- More appropriate when there are multiple parties sharing with each other and/or the nature of the relationship makes specificity impossible
- Although more general, include at least purpose, authority and the types of information shared with as much detail as possible

O
P
D
P

Monitor



- DSA inventory
- Assign responsibility
- Contemplate compliance measurement
- Include enforcement controls
- Certify disposal

O
P
D
P

Thank you

Questions?

O
P
D
P

privacy@ocio.wa.gov

www.watech.wa.gov/privacy