System Security Plan



<System Name>

<Plan Version #.#>

<Date>

**Company Sensitive and Proprietary**

**For Authorized Use Only**

**LEVEL 3, RESTRICTED INFORMATION**

**DISTRIBUTION FOR OFFICIAL USE ONLY**

When system specific information is detailed within this document, all Level 3 statewide information security standards must be met. All copies must follow statewide protection and handling standards. Destroy by shredding.

# Executive Summary

The objective of system security planning is to improve protection of information system resources. All State of Oregon systems have some level of sensitivity and require protection as part of good management practice.

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place, or planned, for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.

Management authorization should be based on an assessment of management, operational, and technical controls.

## Security Plan Benefits

Accurate documentation of an organization’s security programs, processes and procedures, and documentation of compliance with them, provides five key benefits. Security plans:

* Facilitate adequate, cost-effective security protection by assessing the security controls during the development phase of systems and documenting the authorization given by management.
* Lead to institutionalization of security activities for consistency as employees leave the organization. Good documentation is a change management tool and helps effective practices outlast the person who developed them.
* Increase compliance with security measures. Rules are generally followed more closely when someone is looking and keeping records.
* Help IT staff determine where various security measures may need to be strengthened.
* Provide an important step in quality control.

## System Overview

[*Provide a high-level summary of the system*]

## Identified System Risks

[*Provide a summary of the risk identified in the table below.* *Describe any residual risk (portion of risk remaining after security measures have been applied[[1]](#footnote-2), the likelihood of occurrence, and (using the impact table on page 3) the impact of a security event to the business or system.* *When assigning an impact rating to a risk, assign the rating corresponding to the most serious consequence that could result should the vulnerability be exploited*.]

Provide the top 5 risks associated with the system:

|  |  |  |
| --- | --- | --- |
| Likelihood | Impact | Risk Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*{A summary table is provided for the Executive review, compiled from the information recorded in Section 3 (Oregon Standards Spreadsheet). Although not required, it is recommended as an overview of the control implementation status for each control family.}*

**Controls Status Summary Table**

|  | **Vendor** | | | | **Agency** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Control Family** | **In Place** | **Partially In Place** | **Not In Place** | **Not Applicable** | **In Place** | **Partially In Place** | **Not In Place** | **Not Applicable** |
| **AC - Access Control (43)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **AT - Awareness and Training (6)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **AU - Audit and Accountability (17)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **CA – Assessment, Authorization, and Monitoring (14)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **CM – Configuration Management (27)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **CP – Contingency Planning (23)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **IA – Identification and Authentication (27)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **IR – Incident Response (17)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **MA – Maintenance (10)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **MP – Media Protection (7)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **PE – Physical and Environmental Protection (19)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **PL – Planning (7)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **PS – Personnel Security (9)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **RA – Risk Assessment (11)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **SA – System and Services Acquisition (21)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **SC – System and Communication Protection (29)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **SI – System and Information Integrity (24)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **SR – Supply Chain Risk Management (12)** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Totals** | 0 | 0 | 0 | **0** | 0 | 0 | 0 | **0** |

1 GENERAL system Information

This System Security Plan provides an overview of the security requirements for the <**system name**> and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our state security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <**system name**> information system.

**Note:** Once the name and abbreviation for the system and all the system’s components is established in this section, use the exact same name and abbreviation throughout the SSP.

The security safeguards implemented for the <**system name**> system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Those items in square brackets (e.g. [ ], or < >) are intended for fill-in purposes. Those items in braces (e.g. { }) are for references purposes.

## System Function or Purpose

*Get from charter or business case.*

The purpose of the <system name> system is to

## Contact information

Authorizing Official

The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The authorizing official has the following responsibilities related to system security plans:

• Approves system security plans,

• Authorizes operation of an information system,

• Issues an interim authorization to operate the information system under specific terms and conditions, or

• Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Information System Owner

The following individual is identified as the information system owner or functional proponent/advocate for this system. The system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.  The system owner has the following responsibilities related to system security plans:

• Develops the system security plan in coordination with information owners, the system administrator, and functional "end users,"

• Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,

• Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior, system and position-related),

• Updates the system security plan whenever a significant change occurs, and

• Assists in the identification, implementation, and assessment of the security controls.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Information Owner (a.k.a. Data owner)

The following individual(s) identified below is the agency official with the statutory or operational authority for the information processed, stored, or transmitted as part of this system and/or its functions and operation. The information owner has the following responsibilities related to system security plans:

• Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),

• Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,

• Decides who has access to the information system and with what types of privileges or access rights, and

• Assists in the identification and assessment of the security controls where the information resides.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Information Owner

System Administration

This system is managed by [*the <ORGANIZATION and Team>*]. List the Agency Primary and Secondary Administrators and the [*Vendor Administrators*]. Additionally list all groups, or individuals not in groups, that have administrative access to the system or its application.

Identify groups or individuals, if possible, responsible for administrative functions of the system:

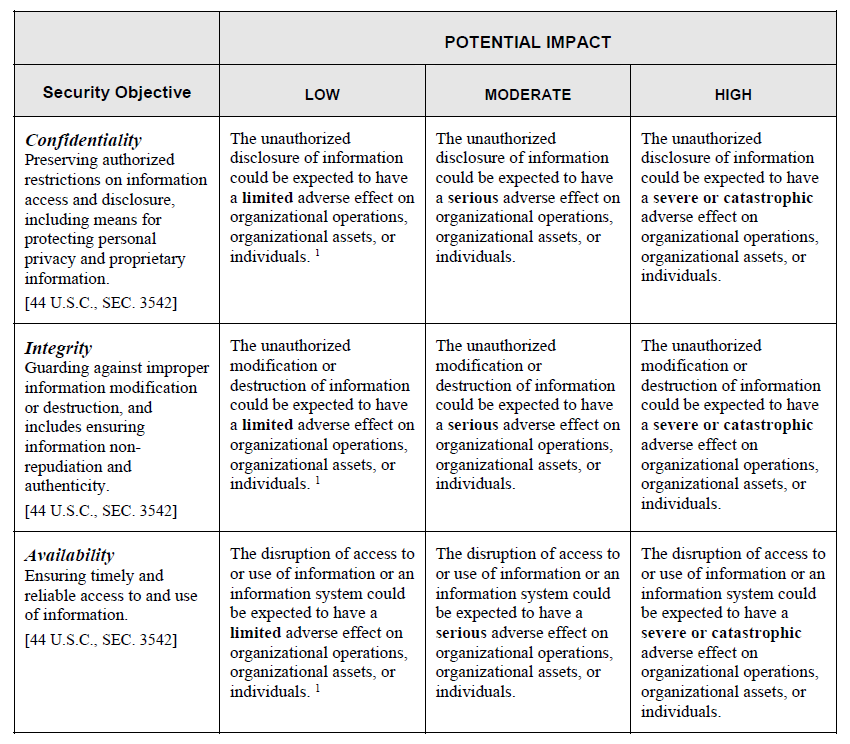
* *Group Name*
* *Name*
* *Name*

**Information System Business impact Assessment**

A potential impact assessment must be performed to determine the system categorization. An impact assessment considers the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the information system and/or its data. This section describes how the information system is categorized for confidentiality, integrity, and availability.

*{Working with the Authorizing Official, the Information System Owner, and the Information Owner, rate the potential impact to the business or system in the event of unauthorized disclosure, modification, or unavailability of this information and/or information system.}*

The tables (below) identifies the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and below from FIPS Pub 199 February 2004, Table 1: Potential Impact Definitions in Security Objectives.

 **[[2]](#footnote-3)**Answers to the following questions may help in the evaluation process:

1

* How can a malicious adversary use unauthorized disclosure, disruption of access, modification, or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
* Would unauthorized disclosure, disruption of access, modification/destruction of elements of the information type violate Federal or State laws, executive orders, OAR’s, or agency regulations?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **SYSTEM-WIDE POTENTIAL IMPACT** | | |
| **Security Objective** | **Low** | **Moderate** | **High** |
| Confidentiality |  |  |  |
| Integrity |  |  |  |
| Availability |  |  |  |

***Information System-wide Impact Assessment***

agency DISASTER RECOVERy AND bUSINESS cONTINUITY

Does this system have a disaster recovery plan?  No  Yes

Please provide a reference to related documents (storage location and file name) and a brief description of your disaster recovery requirements, including recovery time objective/recovery point objective requirements. If no plan has been created, explain why.

Click here to enter text.

Does a Business Continuity Plan include this system?

No  Yes

Please provide a reference to related documents (storage location and file name) and a brief description of your business continuity requirements. If no plan includes this system, explain why.

Click here to enter text.

VENDOR DISASTER RECOVERy AND bUSINESS cONTINUITY

Does this system have a disaster recovery plan?  No  Yes

Please provide a reference to related documents (storage location and file name) and a brief description of your disaster recovery requirements, including recovery time objective/recovery point objective requirements. If no plan has been created, explain why.

Click here to enter text.

Does a Business Continuity Plan include this system?

No  Yes

Please provide a reference to related documents (storage location and file name) and a brief description of your business continuity requirements. If no plan includes this system, explain why.

Click here to enter text.

**Data Classification**

What level of data will the system be processing, storing, or transmitting – according to the Statewide Information Asset Classification Policy?

|  |  |
| --- | --- |
|  | Data Classification |
|  | Level 1 - Published |
|  | Level 2 - Limited |
|  | Level 3 – Restricted |
|  | Level 4 - Critical |

If Level 3 or Level 4 data classifications are checked, please indicate the type of data the information system will be processing, transmitting, or storing that requires this classification:

Click here to enter text.

**Regulatory compliance**

Oregon Consumer Identity Protection Act (As defined in ORS 646A.602)

Criminal Justice Information System (CJIS)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry-Data Security Standard (PCI-DSS)

Federal Information Security Management Act (FISMA)

Federal Tax Information (FTI)

Social Security Administration (SSA)

Other regulatory compliance (e.g. specific data-regulating ORS,)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If any regulatory compliance boxes were checked, refer to the appropriate regulatory document to determine if information types are required to be documented (otherwise, N/A). Information types are defined by the organization or in some instances, by a specific law. Examples of specific categories of information include privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

| Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- |
| Privacy (PII) | Moderate | Moderate | Low |
|  |  |  |  |
|  |  |  |  |

**Information System Operational Status**

The system is currently in the life-cycle phase noted in the table that follows. (Only operational systems can be granted an ATO).

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: |

***Table 7- 1. System Status***

**Shared responsibility model**

If this is a cloud system, document the shared responsibility model/s associated with the solution. If different services in the solution have different shared responsibilities, also document them below.

2 TECHNICAL System Description

This section includes a general description of the <system name>.

## Types of Users

Employees (or contractors) of [ORGANIZATION] are considered Internal Users. All other non-vendor users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

| Role | Internal, External or Vendor | Authorized Privileges and Functions Performed | Approximate # of users |
| --- | --- | --- | --- |
| Admins | Internal | Admin | 5 |
| Users | Internal/External | User | 100 |
|  |  |  |  |

Table 9- 1. User Roles and Privileges

## User identity management and authentication

Times New Roman

| User Type | Managed By | Identity Provider | Authentication Method |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 9- 2. User Identity and Authentication

## Operational RACSI

Modify and expand the RACSI to cover the activities required to operate and support the system and identify who (which Organization and Team or Position) has what role in that activity. The below entries are just examples.

* (R)esponsible: (Doer) Position or team who actually works on the activity
* (A)ccountable: (The Buck Stops Here) Position with the actual authority over the activity.
* (C)onsult: (In the Loop) Position or team who is consulted prior to the activity moving forward. This is a 2-way communication.
* (S)upport: (Here to Assist) Position or team who provide information, resources, or other help required.
* (I)nform: (Notified) Position or team who is notified as the activity moves forward and doesn’t stop the process. This is a one-way communication.

*Example – An ficticious SaaS system using Enterprise Azure AD for employee SSO but no other interconnections or integration and the Agency is the Vendor Customers; Areas of Responsibility vs the Teams or Position Involved*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Vendor Customer Support** | **Vendor [Team, may need to be multiple columns]** | **Agency Program** | **Agency SaaS System Administration** | **Agency Device Administration** | **Agency CIO** | **DCS Cloud Identity** | **CSS SOC** | **Data Owner** | **System Owner** | **Authorizing Official** |
| **Agency User Device Management** |  |  | C | C | R | A |  |  | C | C | C |
| **Agency Customer Account Management** | S | S | C | R |  | C |  |  | AC | C | C |
| **Agency Customer Authentication Management** | S | S | C | R |  | C |  |  | AC | C | C |
| **Agency Customer Access Management** | S | S | C | R |  | C |  |  | AC | C | C |
| **Agency Employee Account Management** |  |  | C | R |  | C | S |  | AC | C | C |
| **Agency Employee Authentication Management** | S | S | C | R |  | C | C |  | AC | C | C |
| **Agency Employee Access Management** | S | S | C | R |  | C | S |  | AC | C | C |
| **Agency-specific Configuration** | S | S | C | R |  | C |  |  | C | AC | C |
| **Agency-specific Monitoring and Log Review** | S | S | C | R |  | C | S | S | C | AC | C |
| **Vendor User Device Management** |  | RA |  |  |  | I |  |  | I | I | I |
| **SaaS Services Operations & Maintenance** |  | RA | CI | CI |  | I |  |  | CI | CI | CI |
| **Hosting Provider Management** |  | RA |  |  |  | I |  |  | I | I | I |
| **Vendor 3rd Party Assessment** |  | RA | I | I |  | I |  |  | I | I | I |
| **Assessment Review** |  | I | C | C |  | C |  |  | C | C | AC |
| **Business Continuity Planning and Testing** | S | RS | RC | RC | CI | CI |  | S | C | C | AC |
| **Disaster Recovery Planning and Testing** | S | RS | RC | RC | CI | CI |  | S | C | C | AC |
| **Security Incident Response, Planning and Testing** | S | RS | RC | RC | CI | CI |  | CS | C | C | AC |
| **Backups** |  | RA | CI | CI |  | I |  |  | C | C | C |
| **Data Restore (e.g. Logs and Data)** |  | RA | CI | C |  | I |  |  | C | C | C |

## Software Inventory

The following table lists the principle software components for <**system name**>**.**

| Hostname | Function | Version | Patch Level | IP Address | Virtual (Yes / No) |
| --- | --- | --- | --- | --- | --- |
| <system name>.oregon.gov | Operating System | Windows Server 2012 R2 | Service Pack 1 | 255.255.255.255 | Yes |
| <system name>.oregon.gov | IIS | ASP .Net 4.5 |  | 255.255.255.255 | Yes |
| <system name>.oregon.gov | Application Software | <system name> |  | 255.255.255.255 | Yes |
| <system name>.oregon.gov | Database SQL Server | MS SQL 2016 |  | 123.45.678 | Yes |
| <system name>-testing.oregon.gov | Operating System | Windows Server 2012 R2 | Service Pack 1 | 123.45.678/23 | Yes |
| <system name>-testing.oregon.gov | IIS | ASP .Net 4.5 |  | 123.45.678/23 | Yes |
| <system name>-testing.oregon.gov | Application Software | <system name> |  | 123.45.678/23 | Yes |
| <system name>-testing.oregon.gov | Database SQL Server | MS SQL 2016 |  | 123.45.678 | Yes |

Table 10- 1. Software Components

## Remote Services (other than web services)

Will users or administrators connect to the system using any of the following services?

|  |  |  |  |
| --- | --- | --- | --- |
|  | Remote Management Services Questions | | |
|  | FTP |  | VNC |
|  | SFTP |  | RDP |
|  | Telnet |  | Citrix |
|  | SSH |  | Other (such as VPN): Click here to enter text. |

## hardware, network and data flow diagrams

<Insert Network and Data Flow Diagrams>

## Ports, Protocols and Services

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations. Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). (See [3.4.6](#_3.4_Configuration_Management))

In the table below, lists the Ports, Protocols, and Services enabled in this information system.

*{On the Hardware, Network, and Data flow diagrams are ports and protocols documented and color coded?}*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ports  (TCP/UDP) | Protocols | Services | Purpose | Used By (Function or System Name) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Ports, Protocols, and Services

## System Interconnections and integrations

*Instruction: List all interconnected systems – these are systems external to the System in this plan. Provide the IP address and interface identifier (eth0, eth1, eth2) that provides the connection to the external system. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted.*

<System name> Environment

| IP Address and Interface on the System | External Organization Name and IP Address of External System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) | Data Direction (incoming, outgoing, or both) | Information Being Transmitted | Ports or Circuit # |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

System Interconnections

**Benchmarks, Configuration, and Installation Guides**

This section is for listing the benchmarks and guides used to create and maintain the baseline and operational configurations. [CIS Workbench](https://workbench.cisecurity.org/) and [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks) are available at no cost to all State, Local, Tribal, and Territorial (SLTT) agencies and offer valuable tools for tailoring and customizing to fit your specific environment. Depending on the requirements for regulated data, some systems might need a more stringent secure configuration baseline.

**List CIS Benchmarks Used with this System**

<System> All operating systems used by the system

<System> All database servers used by the system

<System> All Web Servers used by the system

<System> All browsers used by the system

**Other artifacts:**

Regulated data rules or standards (example)

<System> Server – FTI Security Guidelines

<System> CJIS (Criminal Justice Information)

Documented deviations for all of the above

Baseline Configuration Compliance Scan for all the above

Below table is an example of the minimal CIS profile level for the most common used baselines.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Used By | Software, Application or Device | Technology Type | Secure Configuration Baseline | |
| CIS Benchmark | Profile |
| Vendor | Windows Server 2019 | Operating System | CIS Microsoft Windows Server 2019 Benchmark | Level 1 - Member Server |
| Vendor | Microsoft SQL Server | Database | CIS Microsoft SQL Server 2022 Benchmark | Level 1 - Database Engine |
| Vendor | Windows IIS 10 | Web Server | CIS Microsoft IIS 10 Benchmark | Level 1 |
| Vendor | GitHub | Code Repository | CIS GitHub Benchmark v1.0.0 | Level 1 + Multi-Factor Authentication (MFA) |
| Vendor | Windows 11 Enterprise | Operating System | CIS Microsoft Windows 11 Enterprise Benchmark | Level 1 + BitLocker (BL) |
| Agency | Windows 10 Enterprise | Operating System | CIS Microsoft Windows 10 Enterprise Benchmark | Level 1 + BitLocker (BL) |

# 3 Control Descriptions

Fill out the Oregon Standards Spreadsheet per the Instructions tab in the spreadsheet. Include the spreadsheet as part of this SSP.

[Add link to the filled out Standards Spreadsheet.]

1. NIST Computer Security Resource Center Glossary, csrc.nist.gov/glossary/term/residual\_risk [↑](#footnote-ref-2)
2. Adverse effects on individuals may include, but are not limited to, loss of privacy to which individuals are entitled under law. [↑](#footnote-ref-3)