Student Privacy and Data Security

2017–19 Biennium Budget
Decision Package

Agency: 350 Office of Superintendent of Public Instruction
Decision Package Code/Title: AJ/Student Privacy and Data Security
Budget Period: 2017–19
Budget Level: PL

Agency Recommendation Summary Text:
OSPI systems contain confidential data and information, including student–related data, testing materials, investigative information, educator certification information, and staff employment data. These systems currently lack the infrastructure to protect OSPI's data and information, leaving confidential and secure information at risk for cyber–attacks. This request improves OSPI's security posture by acquiring an IDPS, a Data Loss Prevention (DLP) system, and adding .5 FTE to support the new systems. Total request for the 2017–19 biennium is $475,000.

Fiscal Summary: Decision package total dollar and FTE cost/savings by year, by fund, for 4 years. Additional fiscal details are required below.

Operating Expenditures	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
Fund 001–01	$340,000	$135,000	$135,000	$135,000
Total Cost	**$340,000**	**$135,000**	**$135,000**	**$135,000**
Staffing	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
FTEs	**.5**	**.5**	**.5**	**.5**
Revenue	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
Fund 001–01	0	0	0	0
Object of Expenditure	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
Obj. A	42,400	42,400	42,400	42,400
Obj. B	25,470	25,970	25,970	25,970
Obj. C	100,000	60,000	60,000	60,000
Obj. E	3,315	3,315	3,315	3,315
Obj. G	3,315	3,315	3,315	3,315
Obj. J	165,500	0	0	0
Obj. N	0	0	0	0

Package Description

Background:

OSPI is required to collect many data sets to perform national and state level reporting, manage and evaluate educational programs, certify educators, and finance schools. OSPI systems, therefore, contain confidential data and information, including student–related data, testing materials, investigative information, educator certification information, and staff employment data. Much of that data is made available on the OSPI website to the legislature, parents, districts, and other organizations for both

informational purposes and also to support data–informed decision making. OSPI also shares data with research partners, vendors, and other state agencies. The Every Student Succeeds Act (ESSA) includes many new opportunities for states to collect, report, and use data—and these powerful practices go hand in hand with safeguarding student privacy.

Within the past several years, there have been increased concerns across the nation and within the state of Washington about student privacy and systems security. Student–related data sets are regulated by the federal Family Educational Rights and Privacy Act (FERPA) and the Washington State Office of the CIO imposes additional security requirements.

In July of 2015, the Risk and Vulnerability Assessment done by the Department of Homeland Security's National Cybersecurity Assessments & Technical Services (NCATS) included the following observations:

- "Lack of Intrusion Detection/Protection System (IDS/IPS) and Security Incident/Event Management (SIEM) tool suit leaves OSPI blind to cyber–attacks.
- User base is the largest vulnerability to OSPI network security during this assessment"

An Intrusion Detection/Protection System (IDPS) is a network security appliance that monitors network and/or system activities for malicious activity. The main functions of an IDPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. A Data Loss Prevention (DLP) solution is a system that is designed to detect and prevent a potential data breach/data leak by monitoring, detecting, identifying and blocking certain actions to sensitive and confidential data (Category 2–4) while in–use, in–motion, and at–rest.

The Consolidated Technical Services Agency also reported in a Design Review Summary on June 16, 2015:

- OCIO Security Standards Compliance:
  The (OSPI) proposed solution has OCIO security standard controls for the majority of the overall standard. However, the proposed solution does not currently have an identified solution for Intrusion Prevention and Detection in the K–20 networks. This solution is therefore not compliant with the OCIO security standards (10.3 of the OCIO 141.10 standards).

  The agency must therefore fund and implement its own solution for this control to be compliant.

In an IT Security Audit of OSPI's fingerprint system for educator certifications, the U.S. Department of Justice's Criminal Justice Information Services Division could not assess intrusion detection tools and techniques (4.19) due to OSPI's lack of an IDPS.

Current Situation:

OSPI maintains an Information Technology security program that is updated at least annually. The program consists of annual security training, third–party risk assessments, security testing, and audits. OSPI's systems are updated regularly to prevent unauthorized access to our systems. OSPI's infrastructure consists of multiple routers/switches, firewalls, and Microsoft systems to protect our information and data from unauthorized access. Two FTEs currently provide support for these systems.

Student Privacy and Data Security

For OSPI's student, educator, and finance systems—which include close to 50 individual systems—school district and state personnel gain access to those systems through OSPI's Education Data System (EDS) single sign–on security portal, which was developed in–house nearly nine years ago. The system has nearly 182,000 active user accounts and in 2015, averaging about 350,000 user logins per month from state staff, school district personnel, and individual educators.

OSPI's security infrastructure lacks an Intrusion Detection/Protection System and Security Incident/Event Management tool which leaves OSPI, and the data that is stored here, blind to cyber–attacks.

Proposed Solution:

OSPI will competitively acquire an Intrusion Detection and Protection System (IDPS), a Data Loss Prevention (DLP) system, add .5 FTE to support these systems, and hire a contractor to begin the investigation and planning phase for OSPI to migrate from our current EDS security portal to a commercial grade system.

By loading OSPI policy and business rules into DLP software we will better protect sensitive and confidential data and information so that end users cannot accidentally or maliciously share data whose disclosure could put OSPI at risk. For example, if an employee tried to forward an email outside OSPI or upload a file with student information to a consumer cloud storage service like Dropbox or write it to an un–encrypted USB drive, the employee would be denied permission. DLP tools can also be used to filter data streams containing Category 2–4 on the OSPI network. The new hardware and software will compliment and integrate well within the existing infrastructure with no system latency.

Contact person

- Peter D. Tamayo, Chief Information Officer, 360-725-6134

Base Budget: If the proposal is an expansion or alteration of a current program or service, provide information on the resources now devoted to the program or service.
OSPI current has one network administrator and one system administrator (2 FTE). We are asking for .5 FTE to support the additional security hardware and software.

Decision Package expenditure, FTE and revenue assumptions, calculations and details:
Expenditures are based on prior quotes received to do this work. FTE assumptions are based on the expected level of maintenance required using our experience managing similar devices.

Decision Package Justification and Impacts

What specific performance outcomes does the agency expect?
OSPI expects several areas of improved performance.

1) Improved data privacy and data security governance and support
2) Increased enforcement of and compliance with state and agency security policies
3) Reduced risk and exposure by detecting and protecting OSPI system from security threats
4) More advanced notification of potential data breaches and leaks
5) More secured access for authorized users to OSPI systems

Performance Measure detail:
The Agency will use data privacy risk and data security policy compliance audits and include regular risk and vulnerability assessments of OSPI's system as performance measures. The system will be responsive

to existing and emerging data privacy and data security policies, a risk assessment and policy compliance framework, and compliance measurement processes. OSPI will review access and security logs, perform periodic compliance audits and search OSPI systems for improperly secured Category 2–4 data and information to ensure the systems are operating correctly and effectively.

Fully describe and quantify expected impacts on state residents and specific populations served. The solution described above is to reduce the negative impacts on state residents and the populations we serve. OSPI systems contain confidential information on educators and K–12 students. With the approval of this decision package, OSPI would better comply with state security standards and better secure personally identifiable information (PII) and other sensitive and confidential data and information rated as Category 2, 3, and/or 4 according to state and OSPI policy and standards. These improvements will improve security and enforce state and agency privacy policies thereby reducing negative impacts on state residents and the populations we serve.

Distinction between one–time and ongoing costs:

- The Contracts for the implementation of the IDPS and DLP and the initial purchase price of the IDPS and DLP are one–time (40,000+163,00) $203,000 for fiscal year 2018.
- Salary and Benefits for the FTE expenditure and Goods and Services for the annual maintenance fees for the IDPS and DLP are ongoing in future biennia. Cost are $77,00 for .5 FTE and $60,000 for contracts and maintenance fees, total of $137,000 fiscal year 2018, and $135,000 for on–going cost.

What are other important connections or impacts related to this proposal?

Impact(s) To:		Identify / Explanation
Regional/County impacts?	**Yes**	**Identify:** The systems identified here protect students and educators statewide and other data received from school districts.
Other local gov't impacts?	**Yes**	**Identify:** The systems identified here protect students and educators statewide and other data received from school districts
Tribal gov't impacts?	**Yes**	**Identify:** The systems identified here protect students and educators statewide and other data received from school districts
Other state agency impacts?	**No**	**Identify:**
Responds to specific task force, report, mandate or exec order?	**No**	**Identify:**
Does request contain a compensation change?	**No**	**Identify:**

Student Privacy and Data Security

Does request require a change to a collective bargaining agreement?	**No**	**Identify:**
Facility/workplace needs or impacts?	**No**	**Identify:**
Capital Budget Impacts?	**No**	**Identify:**
Is change required to existing statutes, rules or contracts?	**No**	**Identify:**
Is the request related to or a result of litigation?	**No**	**Identify lawsuit (please consult with Attorney General's Office):**
Is the request related to Puget Sound recovery?	**No**	**If yes, see budget instructions Section 14.4 for additional instructions**
Identify other important connections		

Please provide a detailed discussion of connections/impacts identified above.
OSPI receives confidential data and information from school districts statewide, including tribal schools. In addition, educators from across the state enter confidential information into our systems. The purpose of this budget decision package is to secure all the statewide data and information we receive and minimize educator, parent and student concerns about the security and privacy of their data and information.

The agency is bound by FERPA which is complex in both its interpretation and implementation. Other state and federal data and information security laws cover many of the data types with in OSPI. The Washington State WaTech requires agencies to have a Security Program and implement a variety of security and privacy policies and regulations. The WaTech agency also conducts regular security design reviews and houses the security operations center for state agencies.

What alternatives were explored by the agency and why was this option chosen?
Developing an IDPS and DLP system using in–house state staff was not chosen. State staff do not have the deep knowledge of security systems to develop a robust commercial grade IDPS or DLP. Also existing staff are assigned to other projects and systems. Doing a competitive acquisition for off–the–shelf products is a better alternative.

What are the consequences of not funding this request?
If this package is not funded, threats to OSPI's data and information are more likely to be successful. Further, OSPI's compliance with state security standards is also at risk. OSPI is unable to enforce existing security policies through the implementation of its information security technology. The probability of accidental or malicious data leaks would remain high.

How has or can the agency address the issue or need in its current appropriation level?

Student Privacy and Data Security

OSPI has been able to partially address the issue by purchasing some of the licenses needed to operate the systems. However, the system is still incomplete.

Other supporting materials: N/A

Activity Inventory:

Activity Inventory Item	Prog	Staffing			Operating Expenditures		
		FY 2018	FY 2019	Avg	FY 2018	FY 2019	Total
A002	010	.5	.5	.5	$340,000	$135,000	$475,000
Total Activities					$340,000	$ 135,000	$475,000

Information technology: Does this Decision Package include funding for any IT–related costs, including hardware, software, services (including cloud–based services), contracts or IT staff?

☐ No 

☒ Yes Continue to IT Addendum below and follow the directions on the bottom of the addendum to meet requirements for OCIO review.)

Student Privacy and Data Security

2017-19 IT Addendum

Part 1: Itemized IT Costs

Please itemize any IT–related costs, including hardware, software, services (including cloud–based services), contracts (including professional services, quality assurance, and independent verification and validation), or IT staff. Be as specific as you can. (See chapter 12.1 of the operating budget instructions for guidance on what counts as "IT–related costs")

Information Technology Items in this DP (*insert rows as required*)	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**
IT Staff Salary and Benefits .5 FTE	68,000	68,000	68,000	68,000
Contracts and maintenance fees	60,000	60,000	60,000	60,000
Equipment	163,000			
IT Contracts for Implement	40,000			
Total Cost	**331,000**	**128,000**	**128,000**	**128,000**

Part 2: Identifying IT Projects

If the investment proposed in the decision package is the development or acquisition of an IT project/system, or is an enhancement to or modification of an existing IT project/system, it will also be reviewed and ranked by the OCIO as required by RCW 43.88.092. The answers to the three questions below will help OFM and the OCIO determine whether this decision package is, or enhances/modifies, an IT project:

1. Does this decision package fund the development or acquisition of a new or enhanced software or hardware system or service? ☒Yes ☐ No
2. Does this decision package fund the acquisition or enhancements of any agency data centers? (See OCIO Policy 184 for definition.) ☐Yes ☒ No
3. Does this decision package fund the continuation of a project that is, or will be, under OCIO oversight? (See OCIO Policy 121.) ☐Yes ☒ No

If you answered "yes" to *any* of these questions, you must complete a concept review with the OCIO before submitting your budget request. Refer to chapter 12.2 of the operating budget instructions for more information.