SHEEO

State Higher Education
Executive Officers Association

State Postsecondary Data:

HOW DATA GOVERNANCE AND FUNDING INFLUENCE INNOVATION AND SUSTAINABILITY

Carrie Klein, Sean Baser, & Jessica Colorado

May 2024

TABLE OF CONTENTS

INDEX OF FIGURES

INTRODUCTION

Integrity, security, and sustained investment in data systems are critical for state agencies and stakeholders to effectively harness information to inform policy and decision-making in postsecondary education. Recognizing this crucial need, the State Higher Education Executive Officers Association (SHEEO) has led the charge with its State Postsecondary Data initiative — the definitive source for understanding the state of state[1] postsecondary data in the U.S. SHEEO's Strong Foundations surveys and Communities of Practice convenings are distinct yet interlinked components of that initiative that focus on state postsecondary student unit record systems (PSURSs). Strong Foundations documents the content, capacity, and growth PSURSs. SHEEO focuses on PSURSs because the data therein are the cornerstone to effective state postsecondary policy and decision making. The Strong Foundations 2023 survey's first report highlighted the use, evolution, and value of PSURSs.[2] In this report, SHEEO examines the ongoing efforts and challenges in safeguarding data integrity and privacy and promoting the sustainable growth of PSURSs to meet postsecondary educational needs, today and into the future.

Through PSURSs, state agencies gather and share unit record information across the P20W landscape – within and beyond their state borders – to advance student outcomes and state goals. As PSURSs have expanded across state agencies, so have the technologies that support them, including data-sharing platforms, enterprise resource planning systems, cloud computing, and artificial intelligence. These technologies allow innovative and synergistic data practices but can also pose potential threats to data security and privacy, as PSURSs contain personally identifiable information (PII). As a result, states are enhancing their security and privacy standards and practices[3] to better protect the PII within their PSURSs. However, in a fluctuating state funding environment,[4] the cost of developing, maintaining, and upgrading modern PSURSs can render their governance and sustainability uncertain and vulnerable.

To understand the influence of changing data governance and funding realities, in *Strong Foundations 2023*, SHEEO extended its examination into data privacy and security standards, building upon insights from the 2020 and 2018 surveys. SHEEO also created a new line of inquiry into funding and sustainability. Results from the 2023 survey indicate a continued commitment to protecting the security and privacy of PSURSs data, with all state agencies following established federal and state data handling standards. Further, state agencies adhere to established internal data policies to reduce the risk of data loss and privacy violations. They continue to have data breach protocols in place or comply with overarching state protocols. Recognizing robust protocols and infrastructures alone is not enough, state agencies are taking additional steps. They provide training to staff to ensure the appropriate use of data and PII; are building upon data governance councils to ensure data security and privacy standards are in place; and are creating Chief Data Privacy officer positions.

1. SHEEO includes the District of Columbia, Puerto Rico, and all U.S. territories and freely associated states when using the term "state."
2. Klein, C., & Colorado, J. (2024, January). *State postsecondary data: Evolving systems, improving insights, and enduring value.* State Higher Education Executive Officers Association. https://postsecondarydata.sheeo.org/wp-content/uploads/2024/01/SF2023Report.pdf
3. National Conference of State Legislatures (NCSL). (2020, February 14). *Data security laws/state government.* NCSL. https://www.ncsl.org/technology-and-communication/data-security-laws-state-government
4. State Higher Education Executive Officers Association (SHEEO). (2024, February 2). *SHEF grapevine fiscal year 2024.* SHEEO. shef.sheeo.org/grapevine

Given the need to continually update and sustain PSURSs and to protect the data therein, Strong Foundations 2023 also asked state agencies about current and planned technology priorities and the associated funding their agency or PSURSs had received to support and sustain those priorities. Results indicate that state agencies have a slate of planned technology priorities to improve PSURSs' impacts and processes and to reduce risk to those systems. State agencies reported the need to hire new staff or leverage current personnel to help improve capacity, governance, and use of their PSURSs in response to increasing demands by state stakeholders for targeted, real-time, and consumable data reporting. In instances where budgets are constrained and funding is limited, states have encountered challenges in their endeavors to innovate and modernize. The lack of financial stability hinders their ability to invest in essential infrastructure and personnel required for sustained modernization efforts. Despite these constraints, some states are finding innovative ways to modernize through creative data solutions. **Universally, state agencies noted the need for further investment in their PSURSs to stay economically competitive and to meet state objectives.**

As states seek to improve student outcomes and state goals, greater support of PSURS infrastructure, data, and personnel is vital. Enhancing PSURS capabilities ensures data accuracy and accessibility, key to informed decision-making and policy development. Fostering robust data governance and privacy standards and advocating for continued investment in resources, technologies, and personnel are essential to maintaining effective PSURSs as the cornerstone of effective state policy and practice.

METHODS

SHEEO developed Strong Foundations 2023 in the fall of 2022 in partnership with an advisory board composed of SHEEO staff, survey respondents from SHEEO member agencies, and postsecondary data experts. SHEEO administered the survey from February through March of 2023. Seventy-three SHEEO member and non-member state agencies[5] from all 50 states and the District of Columbia responded to the survey. Information on the Strong Foundations 2023 survey instrument, respondent list, and data can be found here. To protect sensitive data governance, planning, and funding details, SHEEO does not identify individual state agency respondents, except in cases where publicly available resources are available or referenced.

For more information on Strong Foundations, including past survey instruments, data downloads, and reports from current and past survey administrations, go to the Strong Foundations website.

5. Referred to as "state agencies" in this report, this term comprises state postsecondary governing boards, coordinating boards, and departments of education, and systems composed of two- and four-year and technical institutions. Respondents also included agency staff from P20W/SLDS agencies, whose responses were informed by the postsecondary data in their systems. While SHEEO received 73 total responses, because Arizona and Delaware do not have PSURSs, they provided written responses outside the parameters of the survey that indicated how their states use available postsecondary data. Thus, the figures within this report reflect the 71 respondent agencies that completed the full survey.

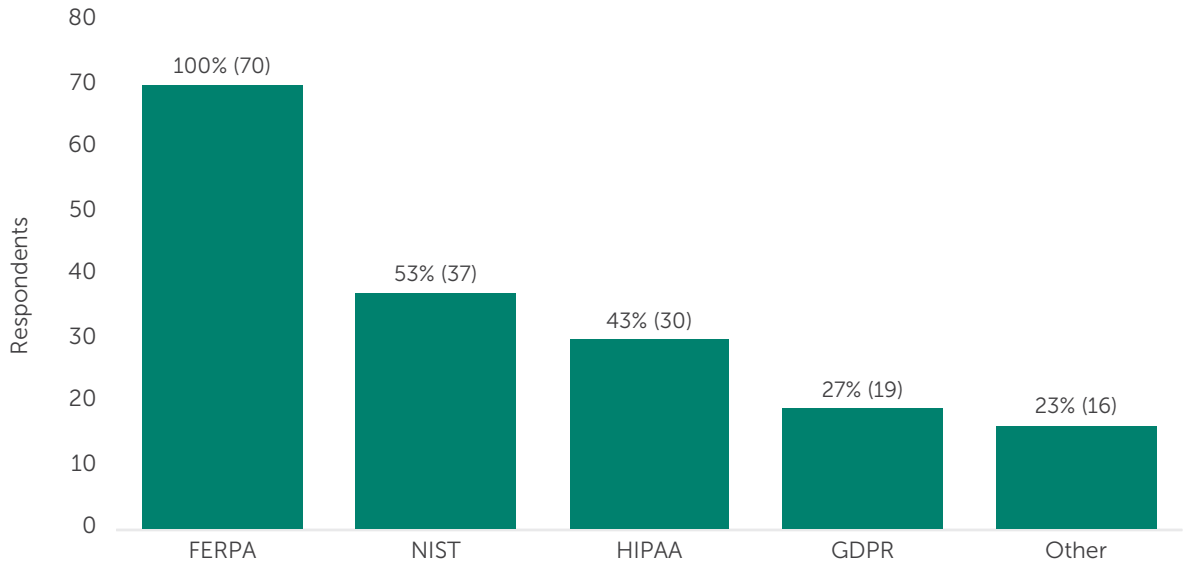
FOSTERING ROBUST PSURSS GOVERNANCE POLICIES, PRACTICES, & PERSONNEL

SHEEO ASKED STATE AGENCIES WHICH NATIONAL OR INTERNATIONAL PRIVACY STANDARDS, PROTOCOLS, REGULATIONS, OR LEGISLATION THEY USE TO DETERMINE PRIVACY AND SECURITY PROCEDURES.

Results from *Strong Foundations 2023* underscore the continued focus state agencies have on ensuring PSURSs data privacy and security standards (see *Figure 1*). Unsurprisingly, 100% of responding agencies indicated that they adhere to the Family Educational Rights and Privacy Act (FERPA) to guide their PSURSs data privacy standards. Additional national or international data security and privacy standards or frameworks state agencies follow include the National Institute of Sciences and Technology's Privacy Framework (NIST; 53%); the Health Insurance Portability and Accountability Act (HIPAA; 43%); the General Data Protection Regulation (GDPR; 27%); and other state or industry standards (23%). Other reported standards include those required by the Gramm-Leach-Bliley Act, the State Wage Interchange System (SWIS), Federal Student Aid; and the 1974 Privacy Act.

FIGURE 1

WHICH NATIONAL OR INTERNATIONAL PRIVACY STANDARDS, PROTOCOLS, REGULATIONS, OR LEGISLATION DOES YOUR AGENCY USE TO DETERMINE PRIVACY AND SECURITY PROCEDURES?



NOTES:

1. Respondents selected all responses applicable to the situation in their state.
2. One state agency did not respond to this question.
3. Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), National Institute for Standards and Technology (NIST) Cybersecurity Framework

SOURCE: State Higher Education Executive Officers Association

State agencies also reported complying with state legislative requirements and standards. Over the past five years, numerous states have enacted data security and privacy legislation[6] aimed at governing the use of personal information, several of which include the governance of postsecondary data.[7] This state privacy story played out in *Strong Foundations 2023*. SHEEO asked about changing state legislation and how those changes influenced data storage and analysis. **Eighteen percent of responding agencies noted that changes in state legislation in the last five years had affected how they store and analyze student unit record data.** Strong Foundations 2023 demonstrates state agencies' dedication to maintaining PSURSs data privacy and security using recognized standards and adhering to federal and state regulations.

INTERNAL POLICIES AND EXTERNAL NOTICES COMMUNICATE STANDARDS

81% OF RESPONDING STATE AGENCIES HAVE INTERNAL-FACING, EMPLOYEE-FOCUSED DATA PRIVACY POLICIES.

In addition to federal and state standards, state-level privacy policies[8] and notices[9] are also an important component of effective data governance. As such, **SHEEO wanted to understand how state agencies were communicating their collection and protection of PSURSs data to staff and stakeholders**. Eighty-one percent of responding agencies have internal-facing, employee-focused data privacy policies informed by state-level standards. These internal policies guide the practice and use of PSURSs data by state agency employees and often provide data protection protocols that go beyond federal standards. For example, one state agency highlighted the specificity and comprehensiveness of its internal policies, which include:

> *...risk and security assessments and audits; [adherence] to best practices for password conventions lock out and employee password disabling; require security and non-disclosure training; require employee non-disclosure statements; build firewalls; run intrusion software; maintain incident response plans; and so forth. These state requirements often go beyond FERPA and NIST [standards].*

Typical reported policies included restricted data access and sharing, appropriate and limited use of data for specific purposes, de-identification of records shared for research, and data storage on separate, secured servers. State agencies also noted that their internal privacy policies are continuously evolving as they respond to new information, contexts, and potential threats to data privacy and security. One state agency reported that its data governance handbook contains a data **"sensitivity classification system...and the data review committee assigns a data owner who, working with IT, legal, and other members of the data review committee, is responsible for data classification and protection."** This collective approach to data governance is vital to ensuring that PSURSs are not just protected, but also reflect ever-changing technological and legislative standards.

6. Folks, A. (2024, April 8). *US state privacy legislation tracker.* International Association of Privacy Professionals (IAPP). iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws
7. American Association of Collegiate Registrars and Admissions Officers (AACRAO). (n.d.). *State privacy legislation.* AACRAO. www.aacrao.org/advocacy/issues/state-privacy-legislation#resources
8. International Association of Privacy Professionals (IAPP). (n.d.). *Organizational privacy policies.* IAPP. iapp.org/resources/topics/organizational-privacy-policies
9. International Association of Privacy Professionals (IAPP). (n.d.). *Crafting a privacy notice.* IAPP. iapp.org/resources/topics/crafting-a-privacy-notice

In addition to creating or adhering to established data privacy and security policies for their organization, **43% of state postsecondary agencies reported having externally facing, stakeholder-focused data privacy notices**. These notices are used by state agencies to communicate with stakeholders how the data in their PSURSs are collected, protected, or used. The California State University system, the Colorado Department of Higher Education, and the University System of Maine have strong examples of state agency data privacy notices.

PROACTIVE PROTOCOLS, AUDITS, & ASSESSMENTS

85% OF RESPONDING STATE AGENCIES REPORTED ESTABLISHED DATA BREACH PROTOCOLS.

With data breaches increasing across industries,[10] including higher education institutions and agencies,[11] establishing effective and actionable breach protocols is of paramount importance. Eighty-five percent of respondents indicated having breach protocols in place. Those standards are established by the state agency or by a partner agency or organization. For example, one state agency noted that it has an incident response plan maintained by its information security officer, which **"outlines the ten incidence response teams, their roles, incident severities, incident categories, and the procedures for each type of data breach."** Others noted that they follow the data breach protocols legislated by their state. Given the connected nature of data between state agencies, higher education institutions, and other state entities, these protocols often include notification of breaches to those organizations. A respondent explained, **"We have a protocol to alert institutions and our IT partners in the department of treasury would alert us and tell us what records may have been compromised. We would contact institutions and alert them of the data breach within 24 hours of finding out about the potential data breach."** PSURSs do not exist in a vacuum. As such, data privacy and security protocols must span the ecosystem in which connected PSURSs data exist.

That ecosystem often extends beyond state agencies' organizational borders. State agencies reported contracting with third-party organizations or other agencies to maintain their data warehouse security or to ensure secure transfer of data from one entity to another, which also requires attention to breach protocols. As a respondent explained, their agency:

> ...contracts with [an outside organization] to maintain our data warehouse. Upon discovering any use or disclosure of confidential information, [that organization] will immediately notify [our agency] to identify... (a) the nature of the unauthorized use or disclosure; (b) the confidential information used or disclosed; (c) who made the unauthorized use or received the unauthorized disclosure; (d) what has been done or shall be done to mitigate any deleterious effect of the unauthorized use or disclosure; and (e) what corrective action has been taken or shall be taken to prevent future similar unauthorized use or disclosure.

10. Knight, K. (2023, April 20). *Why data breaches are increasing and what CISOs can do about it.* Forbes Technology Council. www.forbes.com/sites/forbestechcouncil/2023/04/20/why-data-breaches-are-increasing-and-what-cisos-can-do-about-it/?sh=6347d93547e9
11. Schwartz, N. (2023, September 27). *MOVEit breach hit nearly 900 colleges, says National Student Clearinghouse.* Higher Ed Dive. https://www.highereddive.com/news/move-it-900-colleges-breach/694835

Establishing clear areas of responsibility, action, and remediation across organizations is a core component of appropriate state agency data breach protocols.

In addition to data breach protocols, some state postsecondary agencies have purchased cybersecurity insurance to further mitigate harm after a breach. An agency noted the use of **"general liability and cyber liability insurance covering errors and omissions in its data processing and data storage operations in the amount of at least one million dollars ($1,000,000)."** As the costs associated with responding to the damages of data breaches continue to rise (average breaches can range from median costs of $60k to $1.87M[12]), investing in cybersecurity becomes essential for helping to cover liabilities and recouping losses. However, given the increase in attacks, according to recent reporting, insurance is becoming "more expensive and harder to get,"[13] especially for state and local governments.

With rising costs often placing insurance out of reach, audits and assessments become important mechanisms for improving PSURSs data security and privacy. **SHEEO asked how frequently PSURSs systems and processes are audited to ensure privacy and security standards are current. Respondents indicated that they audited their PSURSs annually (37%), every two years (6%), every three years (5%) or never (11%).** Forty-one percent of respondents marked 'other' indicating that either they or an entity outside of their department may be responsible for auditing their PSURSs within a time frame not listed in the survey.

State agencies engaged in the auditing of their PSURSs are using the process to assess data privacy and security standards, response, and reporting. One agency explained that its data governance group — which includes chief privacy officers from their governor's office and state administration and the overarching state chief privacy officer and the postsecondary agency privacy officer — not only have created breach response standards, including **"artifacts and templates designed to enhance the reporting factor in case of an incident" but have also created an assessment tool to measure the effectiveness of breach responses and reporting.** Use of these audits and assessments act as feedback mechanisms to improve future breach response.

12. Stone, A. (2022, April 20). *The pros and cons of cybersecurity insurance for municipalities.* StateTech. statetechmagazine.com/article/2022/04/pros-and-cons-cybersecurity-insurance-municipalities-perfcon

13. Martineau, P. (2021, October/November). *Is cybersecurity insurance out of reach for government?* Government Technology. www.govtech.com/security/is-cybersecurity-insurance-out-of-reach-for-government

FOCUSED DATA PRIVACY COUNCILS, PERSONNEL, & TRAINING

54% OF RESPONDING STATE AGENCIES HAVE INDIVIDUALS OR TEAMS RESPONSIBLE FOR PSURs DATA PRIVACY AND 33% HAVE CREATED CHIEF DATA PRIVACY OFFICER POSITIONS.

Collaborative and informed personnel, who work to set and ensure data governance standards and practices are maintained, are central to effective postsecondary data governance.[14] Protection of the PII that exists in PSURSs is a paramount priority for state agencies. Consequently, state agencies are convening data governance councils, often led by chief privacy or security officer positions, and implementing data privacy and protection training for broader state agency staff to ensure appropriate data privacy protections are in place for their PSURSs.

Fifty-four percent of state agencies have individuals or teams responsible for PSURSs data privacy. As a respondent noted, they **"have a data governance committee and a data stewardship committee. The individuals [in these committees] review policy and practices to ensure standards are met and relevant over time."** Another agency noted that its data governance is established, **"Through a combination of data services, information technology, and general counsel."** These collaborative approaches promote stronger, more effective data governance as they include a variety of data perspectives, needs, and experiences to help inform and improve data governance processes. For those agencies who do not have a data governance committee because data are not housed in their agency, they adhere to the data standards of their partner agencies. For example, a respondent noted that they collaborate with those entities to **"borrow resources from our universities, including the flagship university in the state, which manages the databases needed for the agency's data warehouse."**

State agencies are also hiring or assigning individuals to lead their data governance efforts. **Thirty-three percent of respondents indicated that a chief data privacy officer on their staff filled this role.** These individuals typically work in information technology or research and policy shops. They are often part of (or lead) larger data governance committees, but their primary role is to focus on issues of data privacy, protection, and the appropriate handling of PII. While not all agencies have an official data privacy officer, other individuals on their staff fill this data stewardship role. For example, a state agency explained, **"The director of information technology functions as chief security officer, and the director of data, research, and planning functions as data owner or data steward for many of the large datasets possessed. Some duties are shared, along with other data owners or stewards."** Other reported individual positions responsible for data privacy and security standards include: the directors of data governance, chief information officers, data ethics and compliance officers, chief information technology officers, data strategists, and leaders of data, analysis, and policy departments. Regardless of where these positions exist or what they are called, state agencies are actively working to ensure current data privacy standards are in place at their agency.

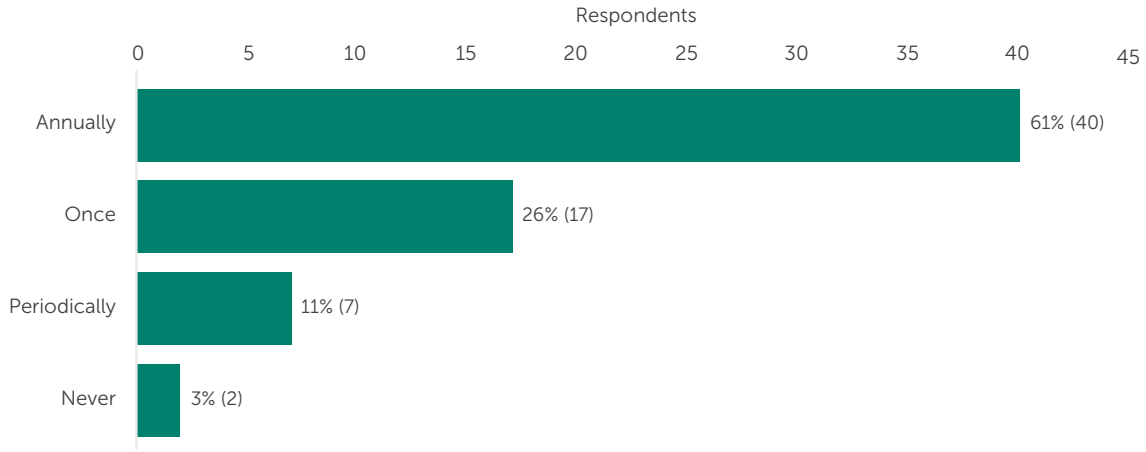
14. Robert, J., & Reinetz, B. (2023, March 6). *2023 EDUCAUSE horizon action plan: Data governance.* EDUCAUSE. library.educause.edu/resources/2023/3/2023-educause-horizon-action-plan-data-governance?m_i=G3eGP_tgP16dhfMfnikW0%2BQ_1AHflvFmRHRDX0GXt00tj5K%2BGzBC7rwLjjcSfFX0VYCHYUZ3CrwCPxZZwW2W5R63kQP8mouGGK&M_BT=87754733647

Chief privacy officers and data governance teams are useful for creating the vision for appropriate use and protection of data; however, this responsibility extends to all data stakeholders. When asked about who bears the responsibility for ensuring data security and privacy standards, one respondent noted: "**Simply everyone! Anyone providing or requesting data must ensure data privacy."** To ensure that reality, data privacy and security training is an important component of a state agency's data governance strategy to equip all personnel with the necessary skills for effectively managing, securing, and using data with privacy in mind. SHEEO asked how often state agency employees received formal training for ensuring data privacy, security, and confidentiality of student-level data (see *Figure 2*).

Eighty-five percent of responding state agencies indicated that they provided data privacy and security training for their employees. Of those, 40 state agencies provide annual training, 17 provide training once (e.g., during onboarding), and seven provide periodic training. Three percent indicated that no training was provided.

FIGURE 2

HOW OFTEN DO EMPLOYEES IN YOUR AGENCY RECEIVE FORMAL TRAINING FOR ENSURING PRIVACY, SECURITY, AND CONFIDENTIALITY OF STUDENT-LEVEL DATA?



NOTES:

1. Three respondents noted more than one response choice applied to their situation: they conduct initial training when onboarding employees and then provide additional training annually or periodically.
2. Three respondents, not included in the figure, do not formally provide training, are planning to, or use webinar-style training available through outside organizations.
3. Five state agencies did not provide a response to this question.

SOURCE: State Higher Education Executive Officers Association

For agencies that do provide data privacy training, that training ranges from **"informal and ongoing discussions with new and current staff on expectations regarding the use of the [data] system"** to more formal processes that require staff to **"complete annual trainings and sign acknowledgments before gaining access"** to the data system.

Attention to the crucial areas of data privacy, security, and training remains an important aspect of modern PSURSs governance. State agencies must ensure that PSURSs containing PII are protected against external threats. That assurance is reliant on the investment of modernized and sustained PSURSs.

IMPACTS OF FUNDING ON MODERNIZING & SUSTAINING PSURSS

Twenty years ago, the federal government began to invest in the development of state longitudinal data systems (SLDSs).[15] Through over $700 million in funding between 2005-2016,[16] this funding supported state capacity to build and connect large data sets, like PSURSs. Yet despite this initial investment and recent pandemic-era funding,[17] respondents noted that adequate state funding is still often lacking. Agencies struggle to appropriately support evolving state data systems, including PSURSs' associated emerging technologies (e.g., enterprise resource planning systems, data storage systems, and artificial intelligence), and personnel to leverage the data therein. As such, SHEEO wanted to understand the funding, priorities, and sustainability associated with modern PSURSs. Unsurprisingly, responses were highly varied depending on the data maturity of a state agency's PSURS and how the system was funded.

64% OF RESPONDING STATE AGENCIES RECEIVED NO FUNDING TO BUILD OR DEVELOP THEIR PSURSs AND 60% HAVE RECEIVED NO FUNDING TO MAINTAIN OR IMPROVE THEIR PSURSS.

SHEEO asked if, since 2013, state agencies had received any funding specifically earmarked to build or develop PSURSs systems (see *Figure 2*). Sixty-four percent of responding agencies have received no funding to build or develop their PSURSs. Twenty percent of agencies reported receiving grants or state appropriations to fund their PSURSs, while 6% of agencies have received in-kind or other means of support. We also asked if state agencies had received any funds to maintain or improve their PSURSs (see *Figure 3*). Sixty percent of state agencies received no funding to maintain or improve their PSURSs, while 26% received state appropriation funding, 18% received grants, 3% received in-kind support, and 6% reported other means of support.

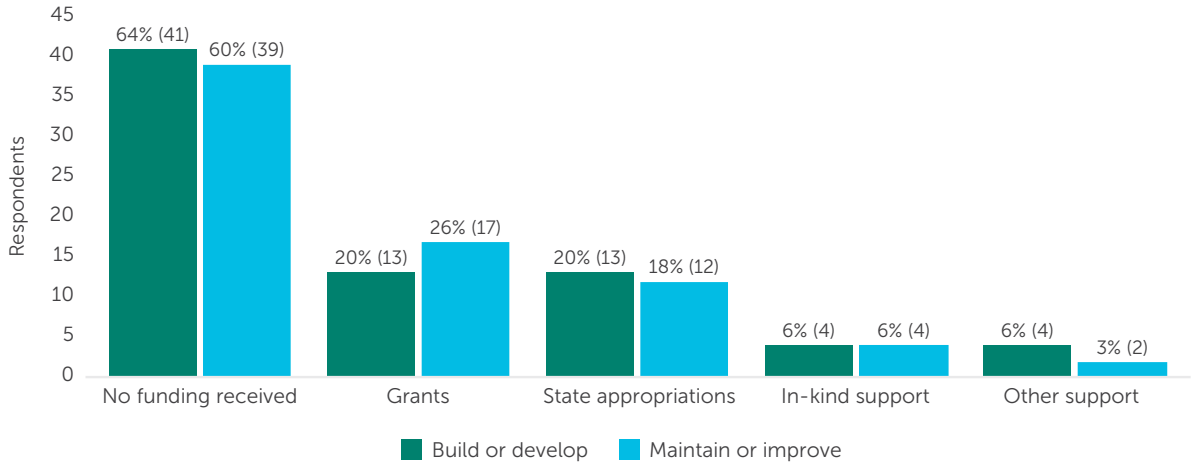
15. Education Commission of the States (ECS). (2021, December). *State longitudinal data systems 2021. ECS.* reports.ecs.org/comparisons/statewide-longitudinal-data-systems-2021-08

16. Armstrong, J., & Zaback, K. (2016, May). *Assessing and improving state postsecondary data systems.* State Higher Education Executive Officers Association & Complete College America. sheeo.org/wp-content/uploads/2019/02/state_postsecondary_data_systems.pdf

17. State Higher Education Executive Officers Association (SHEEO). *Grapevine fiscal year 2024.* SHEEO. shef.sheeo.org/grapevine

FIGURE 3

SINCE 2013, HAS YOUR AGENCY RECEIVED ANY FUNDING SPECIFICALLY EARMARKED TO BUILD, DEVELOP, MAINTAIN, OR IMPROVE YOUR PSUR SYSTEM?



NOTES:

1. Respondents selected all responses applicable to the situation in their state.
2. This figure combines two survey questions (Q34 & Q35).
3. Seven state agencies did not provide a response to the first question with regards to funding for building or developing their PSURS (N = 64), and six state agencies did not provide a response to the second question with regards to funding for maintaining or improving their PSURS (N=65).

SOURCE: State Higher Education Executive Officers Association

Examples of reported funding included a mix of federal, state, philanthropic, or other funding and ranged from the tens of thousands to a few million dollars. These funds are being used to bolster participation in and development, maintenance, or improvement of P20W/SLDSs; create data dashboards and visualizations; implement enterprise resource planning systems (ERPs); employ cloud-based or subscription-based services; modernize financial aid and credential registry systems; expand data collections, including collection of non-credit data; build data warehouses; hire database and platform administrators, developers, hardware, and software; improve quality control and standards; and contract third-party platforms.

BALANCING INNOVATION & COST

SHEEO ASKED WHAT TECHNOLOGIES OR INNOVATIONS STATE AGENCIES WERE CONSIDERING AND THE IMPACT OF MODERNIZATION EFFORTS ON CURRENT AND FUTURE PSURSS BUDGETS.

SHEEO was interested in understanding the interplay between evolving technology and innovation and the costs of developing and maintaining PSURSs. Modern technologies have helped state agencies access new tools, improve data security and reporting, and employ innovative practices. These developments have included server and system upgrades, the creation of data warehouses and lakes, and the implementation of data visualization tools and cloud- and subscription-based solutions. However, alongside these technologies comes a rise in associated costs. As a state agency explains, **"Evolving reporting needs are increasing the costs related to data extraction (such as data visualization tools) and the need for storing and transforming multiple related**

data streams." Yet even with rising costs, state agencies are seeing a value in the expense. For example, a state agency noted that their move to **"cloud and subscription-based solutions creates more operating costs, these are offset (at least in part) by the gains in efficiency from enterprise solutions and pricing, as well as reduced staff time needed for maintenance and upgrades."** As technologies evolve, they create the potential for improved capacity and output, but state agencies must plan for associated expenditures.

State agencies repeatedly noted the cost of modernization. Notably, state agencies underscored that modernization expenses encompass more than just the costs of technology; they also include expenditures for infrastructure and personnel. For example, one state agency noted that, **"Cloud-based computing has made some things easier and cheaper, but we do not have the infrastructure to completely benefit from it."** While the potential exists for these agencies to leverage modern data systems, the potential is often strained by current infrastructure. Staffing to employ modern data systems is another important balancing point for state agencies. Another respondent noted that, **"Evolving technology offers more choices when evaluating possible solutions, which requires skilled staff who can evaluate the implications and communicate decision points to key stakeholders. Other environmental factors [like staffing] and not specifically evolving technology, have the more significant impact on budget."** Responding state agencies said the rapid pace of innovation was both a boon and a detriment to their efforts and budgets given the associated expense.

Even if the technology is somewhat more affordable, often it is not enough to offset the operational costs of deploying it: **"The majority of the candidates are subscription services, that would only slightly reduce our personnel costs, while incurring significant new operational costs and conversion costs. The value proposition remains poor for all the alternatives at this time."** Budget realities and capacity constraints are real limitations for state agencies' efforts to modernize their PSURSs.

UNINVESTED INNOVATION DEMANDS CAN HINDER SUSTAINABILITY & GROWTH

DEMANDS WITHOUT INVESTMENT HAMPERS MODERNIZATION EFFORTS AND THE POTENTIAL OF PSURSS.

State agencies are facing external (and even legislated) pressures to modernize. As a state agency noted, **"Per state law, we are moving our student/employee database into the cloud which involves many factors."** And, even when not legislated, the need to modernize is ever-present, even in the face of limited resources. As a respondent explained, **"In general, the public's expectations are higher, while resources remain the same."** Another respondent explained, **"While budgets remain static, the pressure to eventually migrate to a new system continues to mount. The current options are lukewarm at best, and all come at a significant cost."** The pressure and need to modernize becomes increasingly challenging to implement and sustain when the funding and personnel needed to make those changes are in flux.

While some responding state agencies have been able to access grant funds or other special one-time budget allocations beyond annual state appropriations to improve technologies, sustaining those efforts is challenging without continued investment. A state agency explained, **"Evolving technology has made it easier to develop applications and provide transparent reporting,**

but each new effort must be sustained. While we try to implement sustainable solutions requiring the least human intervention, staff are still required to maintain and protect these technology systems." Without ongoing investment, implementation and leveraging of modern technologies and data systems can be hampered. For state agencies with smaller budgets, the cost to purchase, implement, and support modern technologies can be so prohibitive that it can stall modernization efforts altogether. For example, one state agency noted that their **"budget is small. There hasn't been space for improving technology."** Another noted that their fixed budget impacts modernization efforts, **"Due to budget constraints, funds allocated to the data warehouse has remained the same over the past several years."** By constraining budgets, state agencies are often caught in a technological and budgetary Catch-22, needing to modernize but lacking the funds to invest in the systems and personnel to leverage that modernization.

Investment in skilled personnel is increasingly important as state agencies grapple with the need to effectively tackle new data challenges. As one respondent said, **"A higher level of interest for on-demand data, reports and data visualization...has reinforced the need for additional staff to keep up with the demand."** Advancements in data and technologies have resulted in a subsequent need to leverage, develop, retain, and attract new talent to state agencies with modern data reporting skills. Some state agencies have been able to fund hiring specialized personnel to improve infrastructure, capacity, and reporting, like data strategists, analysts, and architects. These personnel, as another respondent noted, **"support data modeling for improved reporting and analytics; the implementation of Power BI; the implementation of Navigate to supplement the PSURS; and statewide course catalogue and alignment with [our community college system]."** By investing in personnel, in addition to technology, this agency has been able to meet evolving reporting needs. Yet not all state agencies have access to the funds to support these critical data positions. For example, a state agency noted that despite their efforts to **"get additional funding for a programmer with IBM Cloud-Pak experience" their request was denied.** Funding to support appropriate staffing levels was a repeatedly noted challenge related to PSURSs budgets. To effectively implement modern, data-informed policy and decision making, PSURSs and their personnel must be financially supported.

A state agency explains the challenges of modernizing and sustaining their PSURSs in a constrained funding environment:

"There is never enough funding of the budget it seems. Due to evolving technology, it is challenging to keep up and stay current. In our case, our budget will need to accommodate enhancements needed to streamline processes. Several of our processes are still based on older technology and replacing an interface platform will require a decision as it relates to a continued home-grown system that can be supported internally versus the potential of outsourcing by contracting talent to leverage innovative technology with maintenance attached. Adapting to new tools will require additional training. Increased and enhanced security efforts will change data management styles and, in some cases, necessitate a new position. All of these factors will impact our budget."

CONCLUSION

PSURSs are a valuable state resource, and, as such, must be invested in. This investment should include not only the funding required to modernize the technologies associated with PSURSs but also the support for PSURSs infrastructure, personnel, and governance. In the absence of additional funds, state agencies are working collaboratively to make the most of their data, capacity, and personnel. States continue to attend to data privacy and security standards and to create positions, councils, and partnerships to effectively govern and utilize their PSURSs. These actions are increasingly important as PSURSs modernize and as postsecondary data flows between state agencies and across state borders to inform student success and state outcomes. State agencies are committed to and working actively for advancing the use of PSURSs data to inform policy and practice. Funded commitment to those agencies and their PSURSs should follow.

ACKNOWLEDGEMENTS

This paper is based on research funded in part by the Bill & Melinda Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect the positions or policies of the Bill & Melinda Gates Foundation.

SHEEO would like to thank the survey respondents for their insights and the following Strong Foundations 2023 Advisory Board members for their contributions to the development of the survey.

- Kate Shirley Akers, Senior Advisor of Policy Implementation and Best Practices, Data Quality Campaign
- Jinann Bitar, Director of Higher Education Research and Data Analytics, The Education Trust
- Ernest Ezeugo, Strategy Officer for Federal Policy, Lumina Foundation
- Meredith Fergus, Scholarship and Financial Aid Analyst, University of Minnesota
- Jeremy Kintzel, P20W Research Director, Missouri Department of Higher Education & Workforce Development
- Patrick Lane, Vice President of Policy, Analysis, And Research, Western Interstate Commission for Higher Education
- Amanda Roberson, Senior Director of Strategic Engagement, Planning, and Operations, Institute for Higher Education Policy
- Jonathan Turk (survey consultant), Assistant Professor of Higher Education, Saint Louis University

SHEEO would also like to thank the SHEEO staff members who contributed to Strong Foundations 2023 survey development and reporting: Gloria Auer, Jessica Duren, Kelsey Heckert, and Christina Whitfield.

SUGGESTED CITATION:

Klein, C., Baser, S., & Colorado, J. (2024). *State postsecondary data: How data governance and funding influence innovation and sustainability.* State Higher Education Executive Officers Association (SHEEO). postsecondarydata.sheeo.org/strong-foundations