

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

Basic Change :

Sponsors: Sen. Pitsch and Rep. S. Meeks

SB281 would amend the Arkansas Procurement Law, § 19-11-201 et seq., by requiring the use of tracking software in certain contracts awarded by or on behalf of a state agency or political subdivision. The requirement would apply to all contracts for services that have an annual contract amount of at least \$100,000. Such a contract must require the vendor to use software to verify hours billed for work on a computer and must specify that the state agency or political subdivision will not pay for hours worked on a computer unless the hours are verifiable by the required software. The software must allow real-time and retroactive access to the data collected. It must automatically gather data from the vendor by tracking total keystroke and mouse event frequency and by taking a screenshot at least once every three minutes. It must automatically provide the state agency or political subdivision with the real-time cost status of each task performed. It must protect confidential data concerning individuals to the extent such information is protected under state law. It also must allow the state agency or political subdivision to provide immediate feedback regarding any work in progress to the person who is performing the work.

Under the bill, data collected by the software becomes an accounting record that belongs to the person that is performing work under the contract. The person performing work under the contract must store the data collected by the software for at least seven years. The person performing the work must provide the state agency, political subdivision, or an auditor acting on behalf of the state agency or political subdivision with access to data that the software has collected. The person performing the work cannot charge a fee for use of the software or for retrieval of data collected by the software. The bill would require the person performing the work to procure the software from an independent third party.

Revenue Impact :

Unknown at this time.

Taxpayer Impact :

Tracking software would be installed on certain contracts awarded on or behalf of a state agency or political subdivision, which could capture confidential taxpayer information.

Resources Required :

Unknown at this time.

Time Required :

Unknown at this time.

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

Procedural Changes :

Contractors of state agencies and political subdivisions would need to be educated on the requirements to obtain and install tracking software.

Other Comments :

SB281 appears to be patterned upon legislation introduced in several other states that mandates that all state contractors use software to verify that the amount of time they are working on state business matches up with the amount of time they are billing the state for said business. The software automatically gathers verification data of all work performed by the contractor on a computer by tracking total keystroke and mouse event frequency, and by recording screenshots at least once every three minutes.

SB281 mandates all state contractors install tracking software that would enable the verification of the amount of time worked on state business to ensure it matches with the amount of time the contractor bills the state for the work. There are issues with using tracking software. This specific type of software outlined in the bill automatically gathers data of all work performed by the contractor on a computer by tracking the total keystroke and mouse event frequency and records screenshots at least once every three minutes. This creates a significant risk to privacy of state-owned data, as well as, issues with federal regulatory compliance. Additionally, using this type of tracking software would be effectively mandating the installation of third-party spyware/malware on both state-owned personal/private devices.

In 2018, similar bills failed in Rhode Island, Illinois, and Minnesota. Another bill recently failed in Mississippi, yet currently more have been filed in Rhode Island (again), Illinois (again), New Jersey, Minnesota (again), Washington, West Virginia, Kansas, Hawaii, Arizona, Nebraska, Maryland, Tennessee, and South Dakota, all of which have no resolution to date. Presently, DFA is unaware if this legislation has passed any state legislature.

Privacy/Security Concerns

- The provisions in this bill create significant issues with privacy and federal regulatory compliance.
- It is not possible to take a screen shot every three minutes and not capture individual and personal data.
- Key logging software would record everything including passwords, healthcare, and other personal information with no mechanism for redaction before being recorded or stored by the tracking software.
- Meeting the requirements of the legislation would effectively be mandating the installation of third-party spyware on state-owned devices for the sole purpose of reclassifying sensitive data to be time-keeping (accounting records). (*pg. 2, lines 35-36*)
- This bill requires real-time and *retroactive access* of personal data by a third party. Additionally, the bill would allow Arkansas to have access to non-Arkansas owned personal data.
- This bill does not have explicit provisions on how to protect private information.

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

- There is a risk of state and non-state sensitive data being comingled and accessible by unauthorized individuals which would constitute a breach.
- The bill is an unwarranted mandate for spyware to be installed on the state's secure network, and a possible back door for state security systems. This type of software is one that the state was actively trying to prevent hackers from installing.
- The bill would introduce an unnecessary risk to the most sensitive data of citizens.
- The bill requires that ownership of this data be transferred to the contractor and stored off-site with no guarantees that state-owned information would be stored inside the boundaries of the United States. (*pg. 2, line 35*)
- There are other solutions rather than passing this bill, including transparency provision in the contract itself or include transparency in the RFP process.
- There are no industry standards regarding the number of keystrokes/mouse events in a given time window and how it equates to the amount of work being performed or billed under a state contract. (*pg. 2, lines 11-14*)
- This bill will require the third-party administrator of the Employee Benefits Division of the Department of Finance and Administration (EBD), to potentially expose to disclosure to the vendor and its employees/agents all of the State and Public-School Employee Health Information transmitted to it by EBD. EBD's data is Protected Health Information (PHI) and is therefore protected by both the Health Insurance Portability and Accountability Act, Pub.L. 104-191 (HIPAA) and Family Educational Rights and Privacy Act, (FERPA). These federal privacy laws include requirements that data disclosures be limited to the minimum amount necessary. Although the disclosures required by this bill would be permissible under HIPAA and FERPA, the required transmissions will necessitate that EBD, as a covered entity under HIPAA enter into a Business Associate Agreement with the vendor. Similar requirements will be necessary to comply with FERPA.
- This bill could create an increased risk of wrongful uses and disclosures of EBD PHI for which there can be a substantial penalty under federal law. In addition, the software will include "taking a screenshot at least one (1) time every three (3) minutes;" These screenshots are also PHI under HIPAA and their contemplated storage raises similar issues as stated above.
- It is also possible that the requirements of this bill are not technically possible for EBD's third-party vendor due to the complex nature of its work which includes it's computers working with data that is not EBD PHI but which belongs to another health plan. This "cross walking" of data within Health Advantage's systems would require that Health Advantage ensure the security of the non-EBD PHI making the use of the software required under this bill not feasible.

Other Concerns

- This legislation may be so narrowly defined in scope that only the software from a specific vendor would meet the requirements, thus creating a barrier to entry for all but the largest of contract vendors.
- There is a lack of limitation for the use of such a tool to state owned computers.
- The language of the bill implies a requirement incumbent upon a signatory contractor but mixes personal use of a tool with the requirement. (*pg. 2, lines 8-10*).
- The bill does not include any limitations as to when a contract was established with respect to compliance with these requirements.

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

- The bill does not provide any limitations or requirements as to the accommodation for visual assistance tools (ex. speech to text) in use by the non-sighted worker.
- The bill would create a barrier to entry for all but the largest of contract vendors.
- The bill does not account for legitimately billed work that does not occur on a computer.
- The software will capture information from non-state, contracted jobs. In order to redact this information, state employees must use their time and resources to redact personal information.
- There are other solutions rather than passing this bill, including transparency provision in the contract itself or include transparency in the RFP process.
- The confidential provisions of this bill do not explicitly mention protection of trade secrets, attorney-client privileged information, and proprietary accounting records.
- Independent contractors are extensively vetted through background checks, yet this bill allows the contractors to choose a third party that was not extensively vetted to track sensitive data.

For example, contracts this bill would impact include without limitation:

- Contractors that work on AASIS (access to social security number and tax information), and other contractors assigned to the Department of Human Services, Arkansas Department of Health, and other agencies.
- UAMS/physicians who provide OB/GYN services for high-risk pregnancies and HIV treatment for the Arkansas Department of Health.
- EBD third-party contractors.

Legal Analysis :

This bill raises significant privacy and security concerns. For example, in lines 21-23, page 3, subsection (f), the bill requires the person performing the work to procure the required software from an independent third party. As a result, to the extent that the person performing the work has access to confidential information, the third-party software vendor also will have access to that information. The bill does not require the third-party vendor to have a direct contractual relationship with the state agency or political subdivision. The bill does not require the third-party vendor to be registered to do business in the State of Arkansas. In the event of a data security breach, the state agency or political subdivision may have no legal recourse against the third-party vendor.

There is a national trend in software agreements away from the selling or licensing of software and toward "service agreements" under which the software company permits the use of its software, often remotely through a secure internet connection. Such agreements also may provide for remote data storage. If the customer defaults or allows the agreement to expire, the customer may lose access to the data. Here, this bill does not specify what would happen if the person performing the work loses access to the required data prior to the expiration of the seven-year retention period. In the event that only the third-party software vendor has access to the data, the state agency or political subdivision may not have a cost-effective way to compel the third-party vendor to produce the data.

The bill does not specify whether data collected under the bill's requirements would be subject to FOIA. The FOIA provides access to "public records," which § 25-19-103(7)(A) defines to include "electronic or computer based information, or data compilations in any medium required by law to be kept or otherwise kept that constitute a record of the performance or lack of performance of official functions

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

that are or should be carried out by a public official or employee, a governmental agency, or any other agency or improvement district that is wholly or partially supported by public funds or expending public funds." Arguably, data collected under this bill would constitute a "public record" subject to FOIA as a record of the performance or lack of performance of official duties. The requirements of the Arkansas FOIA would then apply to the records and costs of this third party service provider to the extent it is intertwined with and performing a governmental function.

The bill requires the software to collect data such as once-per-three-minute screenshots that may contain both confidential and non-confidential information. The bill does not specify who would be responsible for redacting the confidential information. This responsibility likely would fall on the state agency or political subdivision.

Lines 35-36, page 2, subsection (d)(1) provides that data collected by the software required by the bill "is an accounting record belonging to the person that is performing work under a contract awarded by or on behalf of a state agency or a political subdivision." There is no exemption under FOIA for "accounting records" and as noted above, this could create a significant administrative concern. If it is the intent to exclude from FOIA the data that the software collects as required by this bill, § 25-19-110 requires the enacted statute to state that "the record is exempt from the Freedom of Information Act of 1967, § 25-19-101 et seq."

By classifying the data collected by the required software as "an accounting record of the person performing the work," the bill appears to give the person performing the work a property interest in confidential data collected by a state agency or political subdivision (e.g., screenshots that include confidential taxpayer information). An unintended effect of this bill may be the reclassification of otherwise confidential information as timekeeping or accounting records. It is unclear whether or not the protection against commercial usage or exploitation of an individual's likeness would apply to the retention and usage of the pictures taken if it captures the individual contractor.

In lines 31-33, page 1, the phrase "to verify the hours worked on a computer as part of a public contract to prevent abuse and overbilling" likely should read "to verify the hours worked on a computer and to prevent abuse and overbilling as part of a public contract."

This bill would apply to contracts for "services," which is a defined term under the Arkansas Procurement Law. § 19-11-23 defines "services" as "the furnishing of labor, time, or effort by a contractor, not involving the delivery of a specific end product other than reports which are merely incidental to the required performance." "Services" do not include "employment agreements, collective bargaining agreements, exempt commodities and services, or architectural or engineering contracts requiring approval of the Building Authority Division of the Department of Finance and Administration or higher education." This bill only would apply to the types of services defined by the statute.

In line 8, page 2, the phrase "require a person to use software to verify the legitimacy of the hours billed" could be ambiguous. Instead, "require a contractor to use software that enables the state agency or political subdivision to verify the number of hours billed" would limit the application in a more specific manner.

The bill refers throughout to "the person providing the services." This could be ambiguous, since the

Department of Finance and Administration

Legislative Impact Statement

Bill: SB281

Bill Subtitle: TO REQUIRE VERIFICATION OF THE HOURS WORKED ON A COMPUTER IN PERFORMING WORK UNDER CERTAIN CONTRACTS OF A STATE AGENCY OR A POLITICAL SUBDIVISION.

"person providing the services" could mean the contractor, a specific employee of the contractor, or another person. The Arkansas Procurement Law uses the term "contractor," which § 19-11-23 defines as "any person having a contract with a state agency." Thus, replacement of the phrase "the person providing the services" with the term "contractor" would make the bill consistent with the rest of the Arkansas Procurement Law and would limit the application in a concrete manner. For further clarity, the bill could include a provision that reads, "For the purposes of this section, the term "contractor" means any person having a contract with a state agency or political subdivision of the state."

In lines 29-30, page 2, subsection (c)(3) requires the software to protect all confidential data concerning individuals that is protected under state law. Neither the bill nor the Arkansas Procurement Law defines the term "individuals." The bill is silent as to whether the software also must protect confidential data concerning entities that are not "individuals" (e.g., a corporation's trade secrets, which may be excepted from public disclosure under the Arkansas FOIA statute, § 25-19-105(a)(9)(A)).

In lines 29-30, page 2, subsection (c)(3), the bill only requires the software to protect confidential information that is protected under state law. It does not require the software to protect confidential information that is protected under federal laws, including the United States Constitution.

In lines 13-20, page 3, subsection (e) prohibits the person performing the work from charging a fee to the state agency or political subdivision for access to or use of the software and access to or use of the data collected by the software. In practice, it is likely that bidders will factor the cost of obtaining the software and the cost of data storage into their proposals. This could have the unintended effect of increasing the cost of contracts for services that are over \$100,000.

The bill does not prohibit the person performing the work or the third-party software vendor from providing the data obtained by the software to third parties, either for free or for profit.

Lines 21-23, page 3, subsection (f) requires the person performing the work under the contract to procure the required software from an independent third party. It is not clear whether the person performing the work also must follow state procurement laws in selecting a software vendor.

The bill will create additional recordkeeping duties for the DFA Director.

The bill does not specify whether it applies to public contracts already in effect on the bill's effective date.

This bill does not include a specific effective date. Therefore, the bill would become effective on the earlier of the ninety-first day after sine die adjournment of the session at which the bill was enacted or the ninety-first day of a recess. See *Fulkerson v. Refunding Board*, 201 Ark. 957, 147 S.W. 2d 980 (1941).