JOINT COMMITTEE ON GOVERNMENT AND FINANCE
WEST VIRGINIA OFFICE OF THE LEGISLATIVE AUDITOR

POST AUDIT DIVISION

POST AUDITS SUBCOMMITTEE
MEMBERS

SENATE MEMBERS	HOUSE MEMBERS
President, Craig Blair	Roger Hanshaw, *Speaker*
Mark Maynard	Brandon Steele
Stephen Baldwin	Chad Lovejoy

LEGISLATIVE AUDITOR'S INFORMATIONAL REPORT

September 14, 2021

State Government Entities Requiring Social Security Numbers for Initial Job Applicants

LEGISLATIVE AUDITOR'S STAFF CONTRIBUTORS

Aaron Allred ..... Legislative Auditor

Justin Robinson ..... Director
Melissa Bishop, CPA ..... Audit Manager

Issue 1: State Government Entities Have Been Requiring and Collecting Social Security Numbers for Initial Job Applicants Without a Defined Need to Do So, Increasing the Risk to the State and Those Applicants in the Event of a Data Breach.

In July 2021, it came to the attention of the Legislative Auditor that several state government entities requested or required job applicants to provide their social security number (SSN) when applying for employment with the state. This includes the Division of Personnel (DOP), the Supreme Court of Appeals of WV (the Court), and the State Auditor's Office (SAO). The Legislative Auditor contacted these entities to determine why the SSN was being collected on initial job applications and if doing so was necessary or practical given the sensitive nature of such information in light of the recent data breach of WorkForce West Virginia.

In response to the Legislative Auditor's questions, these entities all gave very similar answers. The practice of requesting SSNs on job applications has been a historical practice and the use of an applicant's SSN is primarily as a unique identifying number. Beyond that primary purpose, none of the responding entities cited any use of an applicant's SSN for any other purpose at the point of application. Each stated that the SSN is not necessary at the time of initial application to conduct background checks or credit checks as those actions are performed when an applicant is being offered a position, not at the point of application.

The concern that resulted in the Legislative Auditor's inquiry is the highly sensitive nature of SSNs and the risk of a data breach associated with a state entity unnecessarily requesting and maintaining such information for initial job applicants. This concern is especially true for the Division of Personnel, which functions as the central hiring entity for the majority of the Executive Branch agencies which in turn receives a significantly larger number of applications containing SSNs. Prior to the Legislative Auditor contacting the DOP concerning this issue, the instructions for applying through the Division of Personnel stated:

> *Social Security Number Required: Pursuant to Section 7 of the Privacy Act of 1974, your disclosure of your social security number is* ***mandatory****. We* ***require*** *social security numbers to verify your identity and confirm the information you provide in your application.* ***Failure to provide your social security number will result in rejection of your application.*** *(Emphasis Added)*

Further, located at https://personnel.wv.gov/Pages/privacy.aspx, the DOP stated:

> *REGARDING YOUR SOCIAL SECURITY NUMBER (SSN): As stated above, we do not automatically collect personal information just by visiting our website. If you choose to apply for jobs with us, we* ***require*** *you to provide us with your Social Security Number to verify your identity and confirm the information you provide on your application.* ***You will be required to provide your Social Security Number, pursuant to Section 7 of the Privacy Act of 1974. In addition, we have the authority to solicit your SSN for the purpose of verifying your identity pursuant to West Virginia Code § 29-6-1. Failure to provide your SSN will result in rejection of your application.*** *(Emphasis Added)*

In reviewing the Privacy Act of 1974 and W.Va. Code, Legislative Services attorneys cannot find any federal or state law that would allow the DOP, or any employer in the U.S., to require an individual to provide their SSN as a job applicant and subsequently reject an application for an individual failing to provide this information. Further, this practice would also preclude non-U.S. citizens who legally reside in the U.S. and are legally eligible to be employed in the U.S. from applying from DOP posted positions as these individuals do not have an SSN.

In response to an inquiry concerning the annual frequency that applications were rejected for failure to provide the SSN, the DOP stated that it did not reject any applications due to failure to provide an SSN on a job application, and applicants that did not provide their SSN would enter all ones, zeroes, or a made-up number sequence. This would be true for online applicants who cannot proceed with their online application without completing the entry field where the SSN is being requested. However, it is still unclear how this would have been treated for applicants filling out a paper application or if any potential applicants decided not to apply due to the requirements stated by DOP to provide the SSN under penalty of rejection.

Subsequent to the Legislative Auditor's inquiries and discussions with the DOP, the Court, and the SAO, all entities stated they would cease the practice of requesting and collecting full SSNs for initial job applicants and would move to requesting just the last 4 digits. Further, the DOP stated the instructions requiring applicants to provide their SSN have been removed from their website and applications.

The Society for Human Resource Management provides guidance to employers stating that employers should generally **not** request SSNs on an employment application as the SSN is not directly related to the applicant's ability to perform a specific job and applications are often viewed by individuals who do not have a need to know the applicant's SSN. This guidance to not collect SSNs is due to identity theft and general privacy issue concerns.

While the practice of collecting SSNs for applicants may have been in place for decades within state government, the current environment we operate in presents far more opportunities for such information to be exploited by those who wish to obtain and use the identities of others for fraudulent or criminal activities. This issue has recently affected WV state government with the WorkForce WV data breach impacting users of its Job Seekers portal. While there is a necessity for employers to request and require SSNs as part of the hiring process and for individuals that are or who have been employed by the state, it is the opinion of the Legislative Auditor that collecting and maintaining SSNs for job applicants is unnecessary and increases the potential damages that may result from a data breach of the systems where such information is maintained.

Social security numbers are arguably the most sensitive piece of private information about an individual. They are used to secure loans, file taxes, apply for government assistance, housing, health care, and a myriad of other important uses. Along with your name, address, date of birth, and some other common personal information, your social security number could be used by a fraudster to do serious financial damage or commit identity theft. The SSN itself is comprised of three groups of numbers. The first three digits are the "area number". Area numbers assigned before 1972 reflect the state where you applied for your number; otherwise, they are based upon the Social Security card application mailing address zip-code. In 2011, a new randomized

assignment method was employed for the area number. The second two digits are the group number, and the last four digits are the "serial numbers". These last four digits are the only unique digits to an individual within an area and group number.

While the decision by the DOP, the Court, and the SAO to move to requesting just the last 4 digits of an applicant's SSN does reduce the risk of damages resulting from someone improperly accessing this information, the need to properly secure this information from unauthorized access is still critical to reducing the risks associated with a potential data breach. Many institutions used by the public request the last 4 digits of an SSN to gain access to an account, along with other more commonly accessible information such as name, address, telephone number, and date of birth. As almost all this information is typically requested on a job application, by including the last 4 digits of an applicant's SSN there remains a heightened risk associated with maintaining this information. Therefore, it is critical these entities, and all state entities which collect SSNs or other personally identifiable information, follow best practices that will ensure this information is properly protected and secured from improper access. These best practices include but are not limited to:

- Identification of personally identifiable information (PII) received and maintained;
- Classification of PII in terms of sensitivity;
- Proper maintenance of PII data and deletion of PII no longer needed;
- Segregation of PII within a data system;
- Encryption of PII within a data system;
- Establishing and employing policies, procedures, and organizational standards for accessing, recording, receiving, and storing PII, as well as for assessing and mitigating the risk of data breaches and a response plan to potential data breaches.
- Restriction of access to certain PII maintained based on defined need for access by the users of such PII within an organization; and
- Training of staff and all users of PII within the organization on the acceptable use and access of PII, the importance of protecting PII, and how to report suspicious activity or potential issues concerning PII to management of the organization.

While the above list of best practices concerning PII is not comprehensive, it exemplifies the key areas an organization should be focused on in order to properly protect PII it maintains and mitigate the risk associated with maintaining it within the organization. As a result of the information described in this report and the issues concerning PII collected and maintained by state agencies, including SSNs or the last 4 digits of an SSN, the Legislative Auditor makes the following recommendations to all state entities.

Recommendations

1. The Legislative Auditor recommends all state government entities cease the practice of requesting or collecting full social security numbers from all job applicants on initial job applications. The collection of a social security number by any state entity should only be done when there is a defined need for this information to further the application process when an applicant is being offered a position. Further, when such information is collected,

it should be properly protected and secured from improper access by employing processes and procedures that encompass the best practices described in this report.

2. The Legislative Auditor recommends that the Legislature consider enacting legislation that would prohibit state government entities from requesting or requiring an applicant provide their social security number as a part of the initial application for employment. However, exemptions should be recognized for state government entities that possess a legitimate need for a social security number at the initial application phase or for compliance with other laws. The Legislature should also consider legislation that requires state government entities protect and secure job applications from improper access, as they contain personally identifiable information that may include social security numbers.