



Department of the Secretary of State

Shenna Bellows
Secretary of State

JOINT STANDING COMMITTEE ON JUDICIARY

Testimony of Shenna Bellows, Secretary of State
Department of the Secretary of State

January 20, 2026

Testifying In Support

L.D. 2121, "An Act to Enhance the Safety of Judicial and Elected Officials, Constitutional Officers and the State Auditor by Allowing Certain Personal Information to Be Removed from Designated Public Records"

Senator Carney, Representative Kuhn and Members of the Joint Standing Committee on Judiciary, my name is Shenna Bellows and I am the Secretary of State. I am speaking today in support of L.D. 2121.

It is a sad truth about today's political and social environment that public servants are facing threats of violence – and actual violence – on a routine basis. Many of you have experienced this personally, like I have, or know colleagues who have. The mental and financial toll that this can take on an elected official or judicial officer can be incredibly burdensome for that person, as well as their family and friends. I am sure we all know people who have declined to run for reelection or even get involved on a higher level at all, because of this environment, and our communities are worse off for it.

That is why I am speaking today in support of L.D. 2121. The Department of the Secretary of State has experience managing public records with care as to what information should be public and what should be redacted or confidential and we have a strong track record of working with municipal and county officials regarding these types of records and decision-making processes. I believe we are well-suited to house a new Office of Information Privacy to carry out the state-level duties that would be assigned to the Department in this bill.

There are a few models – each with their own benefits and challenges – for public servant information privacy that the Committee should consider as you work this bill.

One version is the model that New Jersey has implemented. The New Jersey law covers judicial offices, prosecutors, law enforcement officers, child protective workers, and their immediate families in the same household. In this model, the state Office of Information Privacy trains designated redactors at the state, county and municipal level on the law and their responsibilities. Then, when covered persons apply through an online portal, the state notifies the relevant entities that redactions must be made. The redactions by government entities must be completed in 30 days. Once they are complete, the entity sends back to the state the list of redactions made, so that the covered person is aware. Additionally, the law has been amended in recent years to also cover non-governmental entities, which have 10 days after notification to complete their redactions.

The New Jersey model works there because the Office of Information Privacy has sufficient staff – an Executive Director, a staff person assigned to work with redactors from other government entities, a staff person assigned to work with covered persons, and a program assistant – and an online system to handle applications and notifications. Their ongoing appropriation is \$3,000,000. Covered persons must also sign off during the application process that they understand that certain rights, duties and obligations are affected as a result, including: receipt of certain notices from non-governmental entities; the ability to sign candidate or ballot question petitions; the eligibility or requirements to run for public office or be appointed to a public position; and selling or purchasing a home.

Another model the Committee could consider is offering paid subscriptions to a personal data removal service. This is a service that some states are adopting as part of their safe at home programs. In the first couple weeks of offering this service in Kentucky last year, the Secretary of State reported 15 participants signed up with 800 total listings and 4,500 PII removed. This model would need to be an ongoing subscription.

A different step the Committee may want to consider is a prohibition on publishing certain address and contact information on any maine.gov pages. For example, in places where legislator home address or personal phone numbers have been posted in the past, the contact information for their office here at the State House could be listed. Some legislators have long managed their own work-arounds on this by listing a P.O. Box or a phone number that receives voicemails as the way to contact them, rather than their home address or their cell or home phone numbers, but this could expand that idea for all legislators without any individual potentially standing out.

Finally, the Department of the Secretary of State manages the Address Confidentiality Program, which provides a designated address to survivors of specific circumstances including domestic violence, sexual assault, and stalking who have moved to a new location unknown to their abuser as well as free first-class confidential mail forwarding service. The success of this program relies on a few main components. Most importantly, the enrollee must be living at a new address that is unknown to the person who abused them. Enrollees come to ACP through partnership with trained advocates who consider each survivor's case and the known, specific threat they face. Department staff work one-on-one with them throughout their enrollment to assist with their interaction with state agencies and other entities as needed, in regard to confidentiality. Successful enrollment is very specific to each survivor's case and the known, specific threat that they face. Enrollees sacrifice a lot to be a part of the program, but doing so is an important component of staying safe. Because of the nature of this type of program, I would not recommend this model for public officials.

Thank you for the opportunity to testify in support of L.D. 2121 and I would be happy to answer any questions that the committee may have.