UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LEAGUE OF WOMEN VOTERS, *et al.*, *Plaintiffs*, *v.* U.S. DEPARTMENT OF HOMELAND SECURITY, *et al.*, *Defendants*.	Case No. 25-cv-03501

DECLARATION OF GINGER MCCALL
IN SUPPORT OF PLAINTIFFS' MOTION FOR A STAY AND A PRELIMINARY INJUNCTION

I, Ginger McCall, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am an attorney, barred in the District of Columbia. I am a 2009 graduate of Cornell Law School.

2. Nothing I am sharing in this declaration is confidential. The process I will describe is publicly known and results from public documentation that is available on the Department of Homeland Security (DHS) website and in the Federal Register.

3. My opinions and legal analysis expressed within this declaration are mine alone, and do not represent the official opinion of DHS, the Federal Emergency Management Agency (FEMA), or any other agency or employer. I am drafting this declaration in my personal capacity, as a private individual and attorney, based on my own personal expertise.

4. I have a decade and a half of experience working on issues related to information law, particularly privacy, cybersecurity, and public records law. Currently, I am a partner at a small law firm focusing on public records litigation.

5. I previously worked at the FEMA as the Deputy Associate Chief Counsel for Information Law. I held that position from November 2019 to March 2021 and again from May 2024 to February 2025, when I took the Deferred Resignation offer. From February 2025 to September 2025, I was on Administrative Leave per the guidelines of the Deferred Resignation Program.

6. In my role at FEMA, I supervised a team of five attorneys. I was responsible for providing legal counsel to the agency on matters related to privacy, the Freedom of Information Act, cybersecurity, and the Paperwork Reduction Act. I was frequently asked to advise the agency on matters related to the Privacy Act, including System of Records Notices (SORNs), Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), Computer Matching Agreements, Information Sharing Agreements, Authorizations to Operate, and Memoranda of Understanding/Agreement.

7. Prior to working at FEMA, I worked at the Department of Labor. There, I was an attorney advisor working on issues related to privacy, the Freedom of Information Act, and cybersecurity. I was responsible for shepherding the agency's 700+ page System of Records republication through internal clearance and the Notice and Comment Rulemaking Process.

8. In my experience at FEMA, a component of DHS, DHS has a strictly prescribed process[1] that is required when the agency decides to collect new personally identifiable information (PII), use existing PII in a new or different way, share existing information with a new partner, or merge its information with other databases (inside or outside of DHS).

[1] https://www.dhs.gov/compliance

9. Typically, if a DHS component is considering collecting new PII, or using PII that had been collected under an existing SORN in a new way, the agency begins by drafting a PTA.[2] That document requires the program to carefully consider what data it is collecting, how the data will be protected, how it will be used, and who it will be shared with. PTAs are submitted to the DHS Privacy Office for its review. The Privacy Office then reviews the PTA to determine if the program or system is privacy sensitive and if additional privacy compliance documentation, like a PIA or SORN, is required.

10. If the Privacy Office determines that a PIA is necessary, the program office must undergo a more intensive process. Title 6 U.S.C. § 142 of the Homeland Security Act and Section 208 of the E-Government Act require that DHS (and all federal agencies) conduct a PIA before developing or procuring information systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public.[3]

11. According to DHS Guidance, PIAs require the program to consider how to "incorporate[] privacy concerns throughout its development, design, and deployment of a technology, program, or rulemaking."[4]

12. A PIA can be triggered by either a new collection of PII or a change in an existing collection. Per DHS' website, the agency "conducts a PIA when developing or procuring any new technologies or systems that handle or collect information in identifiable form; creating a new program, system, technology, or information collection that may have privacy implications;

[2] https://www.dhs.gov/publication/privacy-threshold-analysis

[3] https://www.dhs.gov/privacy-impact-assessments

[4] https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

updating a system that results in new privacy risk and issuing a new or updated rulemaking."[5] The SAVE Program, for instance, was most recently the subject of a PIA in 2020.[6]

13. The PIA process typically involves subject matter experts within the program office, the Privacy Office of the component, and technical experts. This team discusses what information will be collected, how it will be used and protected, where the system will be stored, who will have access, and how long information will be retained.

14. PIAs require an explicit discussion of potential privacy risks posed by the system and the mitigation measures the agency is taking to reduce those risks. For instance, the 2020 SAVE PIA included the following:

> Privacy Risk: There is a risk that authorized user agencies could use the data for purposes inconsistent with the original collection.
>
> Mitigation: This risk is mitigated. SAVE's comprehensive audit trail tracking and maintenance functionality mitigates the risk of unauthorized use. Audit measures track and store information on users who submit queries, including: when the query was processed; what the response was; who receives the response; and when SAVE receives the response. The audit logs restrict access based on user roles. USCIS externalized these logs from system administration access methods and protected them from modification. USCIS periodically reviews the audit logs for monitoring user activity.[7]

15. When a PIA draft is complete, it is submitted to the DHS Privacy Office for that office's review. In my experience, there are often several rounds of drafting, during which program

[5] https://www.dhs.gov/privacy-impact-assessments

[6] https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis006c-save-july2020.pdf

[7] https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis006c-save-july2020.pdf

offices are asked to revise, clarify, or provide information. Occasionally, during this process, agency attorneys (like myself) are consulted in order to work through legal issues related to the collection.

16. Once a PIA is completed, it is generally published on DHS' website.

17. Under the Privacy Act, when an agency creates a new System of Records, the agency must undergo the formal SORN process.

18. The SORN process typically begins with internal clearance, which means that the agency shares the draft SORN revisions with relevant stakeholder offices within the agency. After internal comments are integrated, then the agency must notify the Office of Management and Budget (OMB) and Congress. No less than thirty days after that, the agency can begin the public notice and comment portion of the SORN process, which includes publication of the draft SORN in the Federal Register, 30 days for public comment, agency consideration of comments, then – if the comments necessitate changes – republishing the final SORN in the Federal Register.

19. A SORN revision is triggered if there is a significant change to the SORN, including – but not limited to – changes regarding what PII is collected, who it is shared with, and new routine uses.[8] In that instance, an agency would typically go through the same notice and comment process described again.

20. The PIA and SORN process serves several important policy purposes. First, it forces program offices to limit data collection. The PIA process is time-consuming and onerous. Because of this, program offices are disincentivized from over-collection of information.

21. The PIA and SORN process also forces program offices to be transparent about what PII they are collecting, why, and how it is shared and protected. Program offices are required

[8] https://perma.cc/N9QK-SDLE

to answer to the DHS Privacy Office for their PII collection. And, in my experience, during the time that I worked at FEMA from 2019 to 2021 and from May 2024 to February 2025, the DHS Privacy Office exercised significant, meaningful oversight over PII collection, often requiring components to redo portions of PIAs and PTAs, provide more information, and clarify existing information.

22. The PIA and SORN process also forces program offices to consider the risks of collection and actively work to mitigate them. This helps to prevent inadvertent breaches and oversharing of PII.

23. I have reviewed the complaint and other publicly available documentation related to this case. The following observations are made based on the facts described in the complaint. I have no direct personal knowledge of the SAVE system or any of the systems feeding into it.

24. It is my opinion, as a former government official with a decade and a half of experience in this subject area, and with specialized experience working within a DHS component on privacy-related issues – including PTAs, PIAs, and SORNs – that the changes to the SAVE Program (as described in the complaint) should have triggered a PIA and SORN revision and republication.

25. Per OMB guidelines, a revised SORN is required when there is a significant change in an existing SORN. That includes "[a] substantial increase in the number, type, or category of individuals about whom records are maintained in the system."[9] There were several significant changes to the SAVE system that, under any ordinary circumstances, would have caused DHS to revise the SORN and PIA.

[9] https://perma.cc/N9QK-SDLE

26. First, the decision to begin using or collecting the information of United States Citizens was a departure from the existing SORN. The existing SORN had only allowed for collection of PII about "naturalized and certain derived citizens"[10] – not all citizens. Per Paragraph 110 of the complaint, the agency has made public representations that the system would not, in fact, be used for any kind of verification of natural born citizens, nor would it verify citizenship status using a Social Security Number (SSN).

27. The new ability to search by an entirely different personal identifier — a SSN — is also a very significant change which, under any normal circumstances, would have caused DHS to embark on a revised and republished PIA and SORN. The current SORN specifies that SSNs will only be used "in very limited circumstances."[11] Adding SSNs as a searchable personal identifier is a significant departure from that.

28. The purpose and uses of the SAVE system also changed significantly. As the complaint indicates, the SAVE system was previously being used in a more limited way to do voter verification. Even that should have triggered a SORN revision and republication, because when members of the public look at the stated purpose and uses of the existing SORN, they would likely never contemplate that this system would be used for voter verification.

29. The existing SORN reads, "[t]he purpose of this system is to provide a fee-based service that assists Federal, state, tribal, and local government agencies, benefit-granting agencies, private entities, institutions, and licensing bureaus for any legally mandated purpose in accordance with an authorizing statute to confirm immigration and naturalized and certain derived citizen status information, and to otherwise efficiently administer their programs, to the extent that such

[10] https://www.federalregister.gov/documents/2020/05/27/2020-11390/privacy-act-of-1974-system-of-records

[11] https://www.federalregister.gov/documents/2020/05/27/2020-11390/privacy-act-of-1974-system-of-records

disclosure is necessary to enable these agencies and entities to make decisions related to (1) determining eligibility for a Federal, state, tribal, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; or (5) any other lawful purpose. This system is also used for USCIS bond management purposes under sec. 213 of the Immigration and Nationality Act."[12]

30. Already, voter verification would not fit neatly into any of those uses. But the changes since approximately April of 2025 have been more significant, still. The SAVE system was not intended to be used to determine voting eligibility or, worse, potential criminal liability. Neither the PIA nor the SORN contemplates that – nor should they, because this system was not built to be reliable enough to be the basis of such serious determinations. OMB guidance indicates that a revision is necessary when there is, "[a] change that modifies the purpose(s) for which the information in the system of records is maintained."[13]

31. The PIA and SORN also do not specify that the backend of the SAVE system is actually a database that belongs to another agency entirely – the Social Security Administration. That is a very significant change that ought to have triggered a revised and republished PIA and SORN. OMB guidelines specify that a SORN should be republished when there is "[a] change that modifies the scope of the system. For example, the combining of two or more existing systems of records."[14] That is a fair description of what DHS has done here – pulling in an entirely new system on the backend, without ever informing the public about that.

32. The ability to bulk upload records is also another significant change that ought to have resulted in a revision of the PIA and SORN. Under OMB guidelines, a SORN revision is

[12] https://www.federalregister.gov/documents/2020/05/27/2020-11390/privacy-act-of-1974-system-of-records
[13] https://perma.cc/N9QK-SDLE
[14] https://perma.cc/N9QK-SDLE

appropriate when there is "[a] change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system."[15]

33. As the complaint describes, there is a reason why a system cannot simply be transformed in the way SAVE has been. First, the purpose of SORN publication is so people know where their data is, how it is being protected and used, and who is using it. But the Privacy Act also includes another important right: the right to correct inaccuracies. This right is core to the Act and the Fair Information Practice Principles it was built on.

34. Because the existing SAVE documentation never indicates that U.S. Citizens could have data collected, used, stored, or shared by the SAVE system, no citizen would have any reason to know their information is in that system, so they would have no way to identify what system needs correction if, in fact, they are wrongly denied the right to vote based on the SAVE system.

35. Moreover, because the SAVE system is using a Social Security database on the backend, without disclosing that in the SORN or PIA, even if a citizen knew what system was used to create the query that resulted in the denial of voting rights, they would not know what underlying Social Security database was actually used to make that decision and needs to be corrected. Nor would they know who to reach out to demand that correction. This is the reason the drafters of the Privacy Act did not want life-altering decisions to be based on secret databases of PII.

36. The Privacy Act also requires that agencies ensure the quality of the data they are using, which is not happening here. The reliability problems with Social Security's databases have been well-documented. Those systems should not be operating as the back end of another agency's voter verification system.

[15] https://perma.cc/N9QK-SDLE

37. Privacy Act protections also help to ensure the security of the data that is being handled. DHS, like all agencies, has specific policies that govern the handling of sensitive PII, like SSNs. The DHS Handbook for Safeguarding Sensitive PII specifies when sensitive PII can be collected, how sensitive PII may be transferred, and what security precautions must be in place if it is stored.[16]

38. The Handbook expressly states that "DHS programs shall only collect, use, maintain, and disseminate SSNs when required by statute or regulation, or pursuant to a specific authorized purpose."[17]

39. In my years of working as a privacy attorney in FEMA and DOL, I never saw either agency engage in the kind of bulk SSN collection and processing that the SAVE program is now engaging in. No law has authorized, let alone required, DHS to engage in this collection and use of sensitive PII. There is a reason for that: because the collection and use of sensitive PII – like SSNs – creates significant security vulnerabilities that require time, money, and expertise to mitigate. That mitigation is the entire point of the PIA and SORN process.

40. The privacy documentation for the SAVE program has been amended several times for lesser changes. For example, the PIA was revised and republished when transitioning from a paper form to a paperless one,[18] to add the use of SAVE information for administering bonds,[19] and to add a photo matching tool.[20]

---

[16] https://www.dhs.gov/sites/default/files/2024-03/17_1204_priv_handbooksafeguardingsensitivepii_rev3_047-01-007.pdf

[17] https://www.dhs.gov/sites/default/files/2024-03/17_1204_priv_handbooksafeguardingsensitivepii_rev3_047-01-007.pdf

[18] https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis006c-save-july2020.pdf

[19] https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis006c-save-july2020.pdf

[20] https://www.dhs.gov/sites/default/files/publications/privacy-pia-%20uscis-save-20130419.pdf

41. At FEMA I saw numerous SORN revisions. That was a regular part of my work and the work of the FEMA and DHS Privacy Offices. I also participated in the revision and republication of DOL's entire SORN catalogue. In those instances, the changes that triggered SORN revisions were far less significant than the changes that have been made to the SAVE program.

42. I am aware of no facts indicating that DHS undertook its statutorily-required privacy processes. On the contrary, the agency's website indicates that the 2020 PIA was the most recent PIA related to the SAVE program.[21] The agency's online SORN list indicates that the most recent SORN for the SAVE program was published in May 2020.[22] This is an extraordinary departure from ordinary DHS policy and practice and will create serious risks for both individuals who are potentially wrongly purged from voter roles, as well as everyone whose sensitive PII is being saved in an untested, potentially unsecured system.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on October 6, 2025, in Arlington, VA.

_____/s/_____
Ginger McCall

[21] https://www.dhs.gov/publication/systematic-alien-verification-entitlements-save-program

[22] https://www.dhs.gov/system-records-notices-sorns