epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

FISMA Gap Analysis of the U.S. Department of Justice's Collection of State Voter Registration List Data

This document provides an analysis of the U.S. Department of Justice (DOJ)'s compliance with the security requirements of the Federal Information Security Modernization Act of 2014 (FISMA) with respect to its ongoing collection and retention of voter registration list (VRL) data from states. Since May 2025, the DOJ has sought the VRLs of 47 states and Washington, D.C., including sensitive voter information such as Social Security Numbers.[1] While at least ten states have provided their VRLs, 24 states and D.C. have declined the DOJ's request and now face suit from the DOJ over their refusal to provide their VRLs.

To evaluate the adequacy of security protections in place for voter registration list data obtained (or that may later be obtained) by the DOJ, we—the Electronic Privacy Information Center (EPIC)—apply the baseline controls and security requirements set out by FISMA and related National Institute for Standards and Technology (NIST) privacy and security standards to the DOJ's publicly available representations about how such VRL data will be protected. We find that the DOJ's safeguards for VRL data are severely deficient, failing to impose the stringent security controls that FISMA requires due to the data's volume, sensitivity, and connection to the exercise of fundamental rights.

FISMA and NIST Standards

The Federal Information Security Modernization Act of 2014 (FISMA)[2] requires that agencies identify and provide information security protections for (1) information collected or maintained by or on behalf of an agency, and (2) information systems used or operated by an agency, or by a contractor or some other organization on behalf of the agency. 44 U.S.C. §§ 3554(a)(1)(A)(i)-(ii). These protections must be commensurate with the risk and magnitude of the harm resulting from "unauthorized access, use, disclosure, disruption, modification, or destruction" of the collected information or information system. 44 U.S.C. § 3554(a)(1)(A). To comply with said mandate, federal agencies must adhere to "minimum information security requirements" promulgated by the National Institute for Standards and Technology (NIST). 44 U.S.C. §3554(a)(1)(B)(i); 40 U.S.C. § 11331(b)(2)(A)(i).

---

[1] Kaylie Martinez-Ochoa, Eileen O'Connor, & Patrick Berry, *Tracker of Justice Department Requests for Voter Information*, Brennan Ctr. for Justice (last updated Feb. 13, 2026), https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information.

[2] The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this analysis, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

Security Objectives

FISMA defines "information security" to include the three objectives of protecting the confidentiality, integrity, and availability of information systems. 44 U.S.C. §§3552(b)(3)(A)-(C). NIST standardizes said objectives into three different security categorizations in FIPS 199.

The first security objective is **integrity**. A "loss of integrity is the unauthorized modification or disclosure of information."[3] The integrity security objective incorporates the statutory mandate for "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity[.]" 44 U.S.C. §3552(b)(3)(A).

The second security objective is **confidentiality**. A "loss of confidentiality is the unauthorized disclosure of information."[4] The confidentiality security objective incorporates the statutory mandate for "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information[.]" 44 U.S.C. §3552(b)(3)(B).

The third security objective is **availability**. A "loss of availability is the disruption of access to or use of information or an information system."[5] The availability security objective incorporates the statutory mandate for "ensuring timely and reliable access to and use of information." 44 U.S.C. §3552(b)(3)(C).

Security Categorizations

To help operationalize these security objectives into "minimum information security requirements," NIST has established three security categorizations for information and information systems.[6] These categorizations reflect what the potential impact on the statutory objectives of confidentiality, integrity, and availability would be if said information systems were jeopardized. Agencies must use these security categorizations whenever there is a federal requirement to provide such a categorization of information or information system.[7] The three security categorizations are "LOW," "MODERATE," and "HIGH."

The security categorization is "LOW" if the loss of the security objectives would have a "**limited adverse** effect on organizational operations, organizational assets, or individuals."[8] The security categorization is "MODERATE" if the loss of the security objectives would have a "**serious adverse** effect on organizational operations, organizational assets, or individuals."[9] The security categorization is "HIGH" if the loss of the security objectives would have a "**severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals."[10] The minimum security requirements for federal information and information

---

[3] *Id.*
[4] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, at 2 (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[5] *Id.*
[6] *Id.* at 1-3.
[7] *Id.*
[8] *Id*. at 2.
[9] *Id.*
[10] *Id.* at 2-3.

systems depend on what security category the information system is sorted into. For example, moderate-impact information systems must at a minimum adhere to the moderate baseline security controls highlighted in NIST Special Publication (SP) 800-53B. High-impact information systems similarly must at minimum adhere to the high baseline of security controls defined in NIST SP 800-53B.[11]

Security Categorization for Sensitive PII

NIST has two relevant publications that help determine the security categorization of sensitive personally identifiable information (PII) such as a full or partial Social Security Number (SSN) and driver's license number.

First, **NIST Special Publication 800-60 Volume II Revision 1** provides guidelines for "appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or loss of availability of the information or information system."[12] These guidelines apply to all information security systems to which FISMA applies. Under 800-60, Personal Identity Information is categorized as MODERATE impact across all security objectives.[13]

Second, **NIST Special Publication 800-122 for Personally Identifiable Information** creates further standards for PII. Agencies must determine PII disclosure impact levels by looking at factors such as how easily PII can be used to identify specific individuals, the quantity of records in question, the sensitivity of the PII data fields together, the context for which the PII was collected, as well existing obligations to protect confidentiality and the nature of access/storage location of the PII.[14]

<u>The Applicability of FISMA to the VRL Data Collected by the DOJ</u>

DOJ has sought voter registration lists from 47 states and the District of Columbia. At least ten states have provided their VRLs to the agency, including the sensitive and identifying information of over 37 million registered voters. The DOJ has also brought suit against 25 jurisdictions to obtain their VRLs.

VRL data merits a HIGH security categorization in light of the factors laid out in NIST SP 800-122. Nearly 200 million individuals were registered to vote as of 2024.[15] VRLs include the records of each of these voters, including information such as SSNs and driver's

[11] NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* at 6 (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.
[12] *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST SP 800-60 Vol. II Rev. 1, at vi (Aug. 2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.
[13] *Id.* at 53.
[14] NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST SP 800-122, at 3-3, 3-5 (April 2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.
[15] United States Census Bureau, *Voting and Registration in the Election of November 2024, Table 1, Reported Voting and Registration, by Sex and Singer Years of Age: November 2024* (accessed Feb. 2, 2025), https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-587.html.

license numbers which make identifying voters exceedingly easy. Taking all PII data fields together, VRLs are replete with sensitive information.

At minimum, DOJ seeks a voter's full name, date of birth, residential address, state driver's license number, or partial SSN. However, VRLs often include other information. In California, for example, DOJ sought (and failed to obtain) voter participation history and political party registration.[16] This information was collected to aid individuals in exercising their right to fundamental right to vote—a right so foundational that it has been recognized by the Supreme Court as a right "preservative of all rights."[17] Despite the strong potential for abuse and misuse of sensitive information to suppress voting rights and intimidate lawful voters, DOJ is demanding (and in some cases obtaining) complete and unredacted VRL data.

Finally, states bear an obligation to protect the confidentiality of VRL data and the privacy of voters, as does DOJ once it receives and aggregates VRL data into federal information systems.[18] For these reasons, the standard security controls for PII are insufficient to protect VRL data. Instead, VRL data merits HIGH security controls in addition to the baseline controls established in NIST SP 800-53B.[19]

Analysis of the Security Controls DOJ Has Established for VRL Data

Based on our analysis of the DOJ's representations as to how it will maintain VRL data, we find that the DOJ's security controls are severely deficient and cast serious doubt on the agency's compliance with FISMA. We find that DOJ's publicly available statements fail to specify adequate controls for who may access VRL data and under what conditions; how information systems containing VRL data will be protected and how access to those systems will be audited; and what procedures are in place should those systems be breached.

To conduct our analysis, we compared the NIST and FISMA standards detailed above to the data safeguards described by DOJ in its draft Memorandum of Understanding (MOU) sent to Colorado.[20] The MOU, which Colorado declined to sign, would require the state to deliver its VRL to DOJ and remove registered voters named by DOJ.

The security controls articulated in the MOU are severely deficient. The MOU is littered with generalized recitations of compliance with DOJ's obligations—far short of the

---

[16] Order Granting Defendant's Motion to Dismiss and Intervenor's Motion to Dismiss at 5, *United States v. Shirley Weber*, No. 2:25-cv-09149 (C.D. Cal. Jan. 16, 2026), ECF No. 128.
[17] Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886).
[18] While DOJ may not be directly bound by a state's law that protect the confidentiality of VRLs, its aggregation of VRL data into federal information systems does violate the confidentiality protections of those state laws. Further, the Privacy Act of 1974 imposes additional obligations on DOJ once it accepts and aggregates VRL data. 5 U.S.C. § 552a (1974).
[19] NIST, *Control Baselines for Information Systems and Organizations*, NIST SP 800-53B, at 6 (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf [hereinafter NIST SP 800-53B]. Explanations of the security controls are available at NIST, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Sep. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [hereinafter NIST SP 800-53r5].
[20] Colorado Memorandum of Understanding, (Dec. 1, 2025), https://www.brennancenter.org/media/14806/download/2025-12-01-doj-mou-to-colorado.pdf?inline=1.

particularized security controls that an agency must establish under FISMA to adequately protect data as sensitive as unredacted voter registration lists.

Further, the MOU includes expedited timelines for the transfer of VRL data, raising added concern that the security controls in place at the time of transfer will be insufficient or nonexistent. Section IV of the MOU, for example, asks that the Agreement be signed within seven (7) days of the DOJ having presented it. The same Section further presses for Colorado to act as quickly as possible, stating that "no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL" to the DOJ for analysis. These statements cast serious doubt on the DOJ's commitment to protecting the VRL data it obtains, particularly considered against the backdrop of recent data security violations by federal agencies involving the wrongful disclosure of personal data from thousands of individuals.[21]

In Appendix A of this analysis, we set out in greater detail the crucial security and privacy[22] controls that ought to govern VRL data under FISMA and the NIST Standards; the ways in which the controls set out in the DOJ's MOU falls short of those requirements; and the potential consequences of these gaps in security protection. As the Appendix makes clear, the controls identified in the MOU are woefully insufficient and suggest numerous ways in which the DOJ has failed to comply with its FISMA obligations with respect to the VRL data it is collecting from states.

Conclusion

Voter registration lists contain vast quantities of sensitive personal information. To the extent that a federal agency may lawfully collect bulk VRL data to begin with, FISMA requires that such data be protected by strict security controls. Based on our analysis of the DOJ's publicly available representations as to how it will protect the VRL data it obtains, we conclude that the DOJ has failed to establish numerous critical security controls in apparent violation of FISMA.

[21] *See* Notice of Corrections to the Record, *Am. Fed'n of State, Cnty. And Muns. Emps., AFL-CIO v. Soc. Sec. Admin*., No. 1:25-cv-00596 (D. Md. Jan. 16, 2026), ECF no. 197 (admission by government that DOGE employees circumvented agency procedures for data sharing and used unauthorized third-party servers to share Social Security data); *See* Defendant's Corrected Notice on Status of Requests for Return Information, *Centro de Trabajadores Unidos, et al., v. Bessent*, No.. 1:25-cv-00677 (D.D.C. Feb. 11,2026), ECF no. 73 (admission by government that IRS used a faulty automated verification system to improperly share the sensitive information of thousands of taxpayers).

[22] Although NIST's Privacy Control Baseline is not directly required by FISMA, it is unlikely that an agency would be able to comply with the confidentiality requirements of FISMA if that agency were not already compliant with the privacy controls.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control[1]	NIST Requirements	MOU Deficiency	Analysis
Access Control				
AC-2: Account Management	**MODERATE**	Audit records are defined, reviewed, analyzed, and reported.	The MOU does not require that access be reviewed.	The ability to detect unauthorized access facilitates timely response when a breach does occur. Failure to regularly review access allows for (and increases the likelihood of) unauthorized access. This leads to a loss of control over information, diminished transparency, and a loss of public trust.

[1] This indicates the *minimum* level of potential impact on confidentiality, integrity, or availability (per FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, (2004) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf) that requires implementation of the security baseline control. So, a "Moderate" value in this column would mean that the baseline control would be legally necessary if the potential impact were "Moderate" or "High," and would not be necessary *only* if the potential impact is "Low." As a practical matter, implementing the control may still be advisable, even if not strictly required. We re-iterate that the potential impact level represented by the DOJ MOU is MODERATE because of the inclusion of PII, though, as we argue in the analysis, NIST guidance would classify the MOU as HIGH impact. NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST SP 800-122, at 3-3, 3-5 (Apr. 2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf. Privacy baseline controls apply regardless of impact level. *See* NIST SP 800-161r1-upd1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* at 15 (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf (noting that in SP 800-53B the privacy baseline should be "applied to systems irrespective of impact level") ["NIST SP 800-161 Rev. 1"]. The list of controls and associated impact levels can be found in NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* at 16-54 (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
AC-3: Access Enforcement	**MODERATE**	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Section VI of the MOU limits access based on user, with each user having their own defined permissions.[2] Staff members are "assigned a specific identification code" to access the stored information, however "a section may decide to allow its employees access to the system."	DOJ cannot guarantee that access is limited to those with an actual need. Of course, no user could demonstrate a legitimate need to access VRL data, as DOJ has no authority to demand it outside the context of non-discrimination. The MOU does not specify how individuals with a legitimate need to access the information will be identified or vetted, including vendors and contractors. This increases the risks of illegitimate access and loss of control.

[2] Although not required by NIST SP 800-53B, Role-Based Access Controls (RBAC) can make it easier to manage authorized access and detect unauthorized access, as opposed to the MOU's more individualized user-based access rules.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
AC-6: Least Privilege	**MODERATE**	Grant users privilege levels no higher than necessary to accomplish assigned organizational tasks.	The MOU does not define how privilege is assigned and allows for section-level assignment. It does not provide for review of user privileges or access and has no discussion of least-privilege enforcement.	Because there is no review of user privileges, unnecessary access privileges will not be identified and revoked. This can make data breaches harder to detect, especially breaches caused by insider threats. Users may be granted greater privileges than necessary without least-privilege enforcement. DOJ cannot guarantee that access is limited to authorized personnel, and DOJ has not earned trust for enforcing this.
Audit & Accountability				
AU-6: Audit Review, Analysis, & Reporting	**LOW** (applies to all risk levels)	Explicit ongoing integrated audit review, analysis, and reporting are crucial. Ongoing review provides situational awareness of whether there are any deficiencies in the process.	Section IX of the MOU "activates audit logging," but includes no provisions for integrated audit review and analysis.	This is a critical deficiency. Without explicit meaningful audit review, audit logs are functionally useless, like the proverbial tree falling in the forest with no one to hear it, constituting mere "security theater."

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
AU-9: Protection of Audit Information	**LOW** (applies to all risk levels)	Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals.	There is no discussion of how audit logs will be protected or how alerts will be sent, beyond "the Department will activate audit logging" in Section IX of the MOU.	Especially given the woefully deficient security practices of DOGE employees across multiple federal agencies, the integrity of audit logs must be preserved.
AU-12: Audit Record Generation	**LOW** (applies to all risk levels)	Allow designated personnel to select event types that are logged by specific components.	Section VII and IX of the MOU taken together suggest that only the Civil Rights Division will be notified about audit logs tracking usage on computers, servers, and/or devices containing the VRL/data.	Each State would have no way to know about misuse of voter data, despite each State's responsibilities to do so under HAVA, per 52 U.S.C. § 21083(a)(3).

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
Identification & Authentication				
IA-2: Identification & Authorization (Organizational Users) [Multi-factor authentication (MFA)]	**LOW** (applies to all risk levels)	Uniquely identify and authenticate organizational users and associate unique ID with processes acting on their behalf. Many suggested fixes entail MFA, also required by OMB and Executive Order (EO) 14028.	Section IX of the MOU permits access using only a non-default, unique, complex password. Where two-factor authentication is deployed, there is no discussion as to whether SMS-based MFA is deemed acceptable.	MFA protects against the risk of a bad actor gaining unauthorized access to data immediately after obtaining (or correctly guessing) an authorized user's username and password. EO 14028 (Improving the Nation's Cybersecurity)[3] requires MFA, but the MOU does not. DOJ standard practice is to use a Personal Identity Verification card for MFA, but this is not specified in the MOU and there is no reason to trust this DOJ will implement it without oversight. Such trust is unearned by this Administration,[4] and states should not be required to accept a facially illegal security posture. We further note that SMS-based MFA is no longer adequate.[5]

[3] Executive Order 14028, *Improving the Nation's Cybersecurity* (2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[4] *See, e.g.*, Gregory Korte and Erik Larson, *DOGE Staffer Broke Treasury Rules Transmitting Personal Data*, Bloomberg (updated Mar. 15, 2025), https://www.bloomberg.com/news/articles/2025-03-14/doge-staffer-broke-treasury-rules-in-transmitting-personal-data; Letter from Reps. Trahan, Brown, and DelBene to Deputy Inspectors General Sciurba and Erickson (Apr. 3, 2025), https://trahan.house.gov/uploadedfiles/trahan_treasury_gsa_oig_letter_doge_spreadsheet_v2.0.pdf.

[5] "Multi-Factor Authentication", NIST Small Business Cybersecurity Corner (updated Jan. 5, 2026), https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
IA-8: Identification & Authorization (Non-Organizational Users)	**LOW** (applies to all risk levels)	Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information.	Per IA-2 above, the passwords allowed by Section IX of MOU are not sufficient. Secure access includes robust, secure authentication of users.	All users should be authenticated before accessing a federal database containing voter data. To the extent that contractors are not treated as organizational users, they should be subject to authentication as non-organizational users.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
Incident Response				
IR-4: Incident Handling	**LOW** (applies to all risk levels); also **Privacy Control Baseline** (not required but applies to all risk levels)	Implement and regularly reassess an incident response plan, including preparation, detection & analysis, containment, eradication, and recovery. See also OMB M-17-12.[6]	Section X of MOU only requires DOJ to make "reasonable and timely efforts" to notify state-provider of a breach. It does not define timeline nor forensic reporting requirements.	This is a critical deficiency. Because of the sensitivity and volume of data aggregated in this dataset, the risk of identity theft is likely and severe. DOJ's intention to share this data with contractors and other downstream entities, and DOJ's lack of a defined incident response plan, means both that it is more likely that a data breach will occur and that the federal government will not be able to contain the problem when a breach occurs. "For federal agencies, an incident that involves personally identifiable information is considered a breach."[7]

[6] *See Preparing for and Responding to a Breach of Personally Identifiable Information*, Memorandum for Heads of Executive Departments and Agencies (Jan. 3, 2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf ["M-17-12"].
[7] NIST SP 800-53r5 at 152.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
IR-6: Incident Reporting	**LOW** (applies to all risk levels); also **Privacy Control Baseline** (not required but applies to all risk levels)	Personnel must report suspected incidents within a specified period of time to specified officials. Recommended use of automated reporting.	Section X of MOU only requires DOJ to make "reasonable and timely efforts" to notify state-provider of a breach. It does not define any timeline or forensic reporting requirements.	Breaches must be reported within a defined, rapid timeframe, in order to effectively mitigate the severity of harm resulting from the breach. This also violates M-17-12, which requires reporting within one hour.[8]

[8] *See* M-17-12 at 45 ("FY 2014 FISMA Reporting and Privacy Management Guidance for the requirement that agencies report to US-CERT cyber-related (electronic) incidents with confirmed loss of confidentiality, integrity, or availability within one hour").

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
System & Communication Protection				
SC-12: Cryptographic Key Establishment & Management	**LOW** (applies to all risk levels)	Establish and maintain cryptographic keys in accordance with key management requirements for generation, distribution, storage, access, and destruction.	The MOU notes that records, files, and data containing VRL/data will not be copied to unencrypted external storage, but it does not explicitly state that the database itself will be encrypted.	This is a critical deficiency. Unencrypted data, if exposed to unauthorized parties, is easily readable. There is no discussion of encryption in the MOU, apart from external storage.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
SC-13: Cryptographic Protection	**LOW** (applies to all risk levels)	Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography.	No explicit internal encryption, per SC-12 above.	This is a critical deficiency. Unencrypted data, if exposed to unauthorized parties, is easily readable. In addition, methods of encryption that were once considered adequate can become obsolete as technology and tactics for decryption become more sophisticated.[9] There is no discussion of encryption protocols.
SC-28: Protection of Information at Rest	**MODERATE**	Information at rest refers to the state of information when it is not in transit and is located on system components (e.g. in a database).	The MOU includes no explicit internal encryption, per SC-12 above.	This is a critical deficiency. Unencrypted data, if exposed to unauthorized parties, is easily readable. "The focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information."[10]

[9] *See, e.g.*, NIST SP 800-131Ar3 ipd, *Transitioning the Use of Cryptographic Algorithms and Key Lengths* (Oct. 2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf.
[10] NIST SP 800-53r5 at 316 (PDF p. 343/492).

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
Additional Deficiencies				
PL-8: Security and Privacy Architectures	**MODERATE**; also **Privacy Control Baseline** (not required but applies to all risk levels)	Develop security and privacy architectures (including requirements and approach to minimize risks of processing and retention).	MOU suggests data may be archived rather than destroyed.	By archiving VRL data, it becomes subject to National Archives and Records Administration (NARA) retention schedules, meaning a permanent record of voter data is created that cannot be deleted.
PT-3: Personally Identifiable Information Processing Purposes	**Privacy Control Baseline** (not required but applies to all risk levels)	Restrict processing of personally identifiable information to only that which is compatible with the identified purpose(s), and monitor changes.	The purpose of the VRL, a creation of the HAVA, is to ensure non-discrimination; there is no discussion of non-discrimination whatsoever in the MOU.	The MOU creates unnecessary risks by allowing the data to be shared beyond what could ever be considered necessary. Data minimization is the data privacy and data security principle that limits risk by limiting the collection, processing, and retention of data to only what is necessary. Exceeding the stated purpose of the VRL, including sharing it with third party entities, contravenes data minimization principles.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
PT-6: System of Records Notice (SORN)	**Privacy Control Baseline** (not required but applies to all risk levels)	Keep system of records notices (SORNs) accurate, up-to-date, and scoped in accordance with policy.	Categories of records only includes name, address, telephone number, and voting areas, not driver's license number (DLN), or last 4 digits of social security number (SSN). Purposes are limited to ensure non-discrimination.[11]	SORNs are necessary for transparency and accountability about what data the federal government is collecting, how that data will be used, and for what purposes. It is also a violation of the Privacy Act, to state that "[t]his system contains no information about any individual other than as described in Categories of Records above"[12] when DOJ intends to imminently include DLN and SSN data.

[11] *See* Privacy Act of 1974; Systems of Records – JUSTICE/CRT-004, 68 Fed. Reg. 47610, 47614 (Aug. 11, 2003), https://www.govinfo.gov/content/pkg/FR-2003-08-11/pdf/03-20342.pdf.
[12] Id. at 47615. *See also* DOJ Systems of Records – CRT-004 *Registry of Names of Interested Persons Desiring Notification of Submissions Under Section 5 of the Voting Rights Act*, https://www.justice.gov/opcl/doj-systems-records (updated Dec. 19, 2025).

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
RA-8: Privacy Impact Assessments	**Privacy Control Baseline** (not required but applies to all risk levels)	Conduct Privacy Impact Assessments (PIA) before initiating a new collection of personally identifiable information.	There is no indication that the Civil Rights Division conducted a PIA at all, let alone one that was approved by the DOJ Office of Privacy and Civil Liberties.	The Civil Rights Division has not published a PIA related to its collection of VRLs.[13] It is common sense that a government agency did not adequately evaluate the privacy risks entailed in a new collection of personal information if it did not conduct even a baseline Privacy Impact Assessment. Further, no other DOJ division has updated a publicly available PIA to reflect the aggregation of VRL data. Congress has also made it a violation of the E-Government Act of 2002 to fail to conduct and publish a PIA before collecting the data.

[13] For a complete list of published PIAs completed by all DOJ components, see *DOJ Privacy Impact Assessments*, DOJ.gov (last accessed Feb. 22, 2026), https://www.justice.gov/opcl/doj-privacy-impact-assessments.

Appendix A

Baseline Control	*Minimum* Impact Level *Requiring* Listed Baseline Control	NIST Requirements	MOU Deficiency	Analysis
Cybersecurity Supply Chain Risk Mgmt. (C-SCRM)[14]	NIST SP 800-161 notes that 800-53 Controls should also be applied to C-SCRM, as relevant[15] (for example, vendors managing databases such as list maintenance).	Must establish contractor security requirements and conduct due diligence checks.[16] Must ensure that sharing occurs within formal structures.[17]	Section IX of the MOU permits a DOJ contractor to access VRL data without any vetting framework.	This is a critical deficiency. Third party contractors are a major source of data breaches.[18] The MOU contains no explicit language to bind contractors to the same controls as DOJ, leaving VRL data exposed to undefined risk.

[14] NIST SP 800-161 Rev. 1.
[15] *See id.* at 64 (PDF p. 78/325).
[16] *See id.* at 38.
[17] *See id.* at 42-43 (noting that this information sharing is described by NIST SP 800-150, *Guide to Cyber Threat Information Sharing*).
[18] Up to 30% of breaches are caused by third parties, by some estimates. *See, e.g.*, Connor Jones, *Your vendor may be the weakest link: Percentage of third-party breaches doubled in a year*, The Register (Apr. 24, 2025), https://www.theregister.com/2025/04/24/security_snafus_third_parties/ (reporting on statistics from Verizon's most recent Data Breach Investigations Report). This is no less true in the context of contractors handling sensitive data for the federal government. *See, e.g.*, Sean Lyngaas, *Customs and Border Protection subcontractor hack exposes traveler photos, license plates*, CyberScoop (June 10, 2019), https://cyberscoop.com/cbp-hack-subcontractor-hack-exposes-traveler-photos-license-plates/.