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/.