ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: SSNR – Standardize VA Enterprise Person Identifiers

Approved by the VA Chief Architect (OIT/OCTO) on 11/05/2025

Context

Efforts are underway across the VA to minimize operational use of SSNs across VA business lines to reduce risk of identity theft, improve data security/privacy, while maintaining or improving operational efficiency. This initiative is guided by federal laws, including the Consolidated Appropriations Act of 2024 and related mandates such as the Fraud Reduction and Data Analytics Act.

Whereas the law previously mandated removal of SSNs from all systems, the 2024 revision allows VA discretionary use of the SSN for identification, fraud prevention and data exchange, while still requiring VA to take steps to remove SSN "high risk" uses as a means of authentication and/or in veteran facing applications. The intent of this ADR is as follows:

- In accordance with VA Enterprise Social Security Number Reduction Guide – September 2025, this ADR prescribes an architectural requirement for all VA Systems that collect SSNs to standardize on the person identifiers they maintain. The systems listed in Table 1, and any future VA systems that meet the same criteria, are subject to this ADR.

- Table 2 provides a key summation of real-life examples to illustrate when VA may use SSN and when SSN must be remediated within VA systems.

System Scope

The systems listed in Table 1 were identified through VASI as systems that collect and store SSNs in support of benefit, healthcare, or other Veteran-facing service delivery missions. This list is not exhaustive. Any current or future VA system that collects and stores SSNs for these purposes must comply with this ADR.

For the purposes of this ADR, SSN use cases in VA systems may be classified as High Risk, Medium Risk, or Low Risk based on exposure, sensitivity, and access scope. These classifications are provided by the Architecture and Engineering Services (AES) team as working definitions to support system owners in prioritizing remediation activities under the SSNR initiative.

Final authority for data risk classification remains with the VA Privacy Service, the Office of Information Security (OIS), or other designated policy bodies. These definitions may be updated or superseded by future enterprise privacy or security guidance. Table 3 provides the SSN risk tier definitions and example use cases.

Decision

1. VA systems listed in Table 1, and any future systems meeting the same mission criteria, are authorized to continue collecting and using SSNs as an optional identity trait when necessary and when no adequate substitute identifier is available to administer benefits, verify identity, or prevent fraud. These systems shall also take steps to minimize exposure of SSNs in non-essential contexts, such as correspondence, self-service portals, and authentication processes, replacing SSN with ICN where possible.

2. The types of persons whose records are maintained in VA Systems include the following: current military members, former military members, veterans, dependents, caregivers, other associated persons (e.g., insurance beneficiaries), employees, contractors who may have their SSN collected and maintained for the purpose of establishing person identity, record exchange, and fraud prevention.

3. All VA Systems that contain SSNs shall maintain a compliant system-to-system integration with the VA Master Person Index (MPI) as a source for all identity management functions and authoritative identity traits including the Social Security Number (SSN) and the Identity Control Number (ICN). The Electronic Data Interchange – Person Identifier (EDI PI) may also be maintained where required.

4. All systems that contain SSNs can continue to maintain the Social Security Number (SSN) if no adequate substitute identifier is available or use the Identity Control Number (ICN) for all new and active person records. The Electronic Data Interchange – Person Identifier (EDI PI) may also be maintained where required.

5. All systems that contain SSNs shall subscribe to identity trait updates (including ICN, EDI PI, and SSN changes) published by the MPI and shall apply those updates to those affected person records as near real time as possible, but not later than 24 hours after receipt, unless business requirements dictate otherwise.

Rationale

Directly supports the VA SSNR initiative. By requiring each VA owner of a system that contains SSNs to complete a compliant integration with the VA MPI system, by requiring enhancement of each System to include ICN (and EDI PI where required) as alternative person identity traits, and by requiring these systems to subscribe to and apply MPI trait change updates, system owners can more easily adapt inter/intra VA exchanges to remove SSN usage potentially improving operational efficiency.

This decision is aligned with the Consolidated Appropriations Act of 2024, which provides VA discretion to retain SSN use for identification, fraud prevention, and data exchange. Eliminating SSNs entirely from these core systems would introduce operational and interoperability risks. This ADR documents VA's decision to maintain SSN as an optional trait for these systems while advancing SSN reduction through standardized use of ICN and minimization of high-risk uses.

Impact(s)

How this affects system owners:

System owners will need to plan for integration with the Master Person Index (if not already connected), subscribe to and apply MPI updates, and ensure their data models include the required identifiers. They are also expected to identify and reduce high-risk uses of SSN in correspondence, self-service portals, and call center processes by replacing SSN with ICN wherever possible. These steps may require adjustments to interfaces, data exchanges, or templates but do not mandate removal of SSN from core records where its use remains justified.

Enterprise outcomes:

- Standardize the identity traits available from VA Systems for system and application developers.
- Establish a standard set of person identifiers (other than SSN) in each system as a baseline requirement for the enterprise.
- Facilitate API development and system integrations.
- Provide alternative identifiers for person record matching, external facing applications, correspondence to enable business owners to reduce "high risk" and "medium risk" uses of SSN.
- Facilitate completion of the SSNR initiative, minimize disruption to VA OIT operations, and improve data exchange efficiency.

- Reduce SSN operational use between VA business line systems and with external partners such as DoD.
- Support replacement of SSN within Veteran-facing correspondence, email, letters, and self-service applications.

For questions or further clarification, contact the Enterprise Architecture team at ea@va.gov.

BASSAM KALDAWI

Digitally signed by BASSAM KALDAWI
Date: 2025.11.05 09:50:43 -08'00'

Sam Kaldawi
Chief Architect
Office of the Chief Technology Officer (OCTO)

**Disclaimer: The Architecture and Engineering Services (AES) team's recommendation in this ADR is provided solely as an architectural guidance and does not imply AES ownership of operational, licensing, or cost responsibilities associated with the adoption of the recommended tool.*

This ADR does not establish the recommended tool as the exclusive solution for the defined use case. Other tools that meet VA requirements may continue to be used or evaluated as part of VA's enterprise technology strategy. Cost considerations, licensing agreements, and operational support for any tool remain the responsibility of the respective program offices and stakeholders.

Table 1: List of VA Systems with SSNs

System Acronym	VASI ID	Product Line
BOSS-E	1069	Memorial Benefits and Services
CRP	1153	Benefits Integration and Administration
VETSNET	1712	Compensation and Pension
VBMS	1728	Compensation and Pension
VEFS	3023	Compensation and Pension
CAPRI	1130	Compensation and Pension
LIPAS	2404	Insurance
EIN	2296	Insurance
LGY	1489	Loan Guaranty
MBMS	3269	Memorial Benefits and Services
VD3	2120	Benefits Integration and Administration
eFolder Express	1698	Appeals **Component of VBMS*
LGYA	2719	Loan Guaranty
VALERI- R	2227	Loan Guaranty
SAHSHA	1862	Loan Guaranty
BEP - CSS	1898	Benefits Integration and Administration
FCMT	1929	Education Veteran Readiness and Employment
eMPWR- VA	2602	Education Veteran Readiness and Employment
Caseflow	2114	Appeals
BVA VACOLS	1721	Appeals
BIP	2295	Benefits Integration and Administration
MEL	2113	Memorial Benefits and Services
CCFT	3262	Community Care

DCPS/DDE	2450	Financial Management
DM2	1909	VHA Finance
EDR	3077	N/A* *Product Line not assigned for this system in VASI*
ePerformance	2344	Human Capital Management
F&L	3040	Patient Care Services
FMBT	2546	Financial Management
GRB	2219	Human Capital Management
iFAMS	2202	Financial Management
OHRS	1467	Healthcare Environment and Logistics Management
PayVA	2307	Financial Management
S/WIMS	2799	Human Capital Management
VEIS	2405	Veteran Relationship Management
VHALWD	1863	Human Capital Management
VistA	1973	Health Informatics
VSSC	1769	Data and Analytics
WC-OSH	1868	Human Capital Management
AcuStaf	2214	VHA Front Office
CCRMS	1109	Human Capital Management
CDW	1152	Data and Analytics
CommCare-CRM	2033	Veteran Relationship Management
DIP	2825	Platform Management
DSS	1174	VHA Finance
EHRM MAP	2536	Electronic Health Record Modernization
FMS	1277	Financial Management
HCM-DW	2904	Human Capital Management

HRIS	1340	Human Capital Management
HR-PAS	2302	Human Capital Management
IAM	2350	Identity Access Management
MHV	1820	Digital Experience
Payer EDI TAS	2625	Community Care
TMS 2.0	2136	Human Capital Management
VA MPI	1406	Identity Access Management
VA USA PIV	2274	Human Capital Management
VA-CABS 2.0	2907	Human Capital Management
VATAS	1677	Financial Management
VEMS	1735	Acquisition and Property Management
VERA	1737	Financial Management
VetPro	1756	Human Capital Management
VIEWS CCM	2619	Sec VA / Congressional / Legal Affairs
VPS	1752	Digital Experience
WC-OSH/MIS	1868	Human Capital Management

Table 2: Summary of Relevant Federal Guidance

Table 2A: Consolidated Appropriations Act of 2024

Acceptable Use	Description	Example
Non-VA Source	SSN needed to exchange info with outside agencies.	Treasury payments, DCSA investigations
Legal Requirement	Law/regulation/court order explicitly requires SSN.	Specific statutes requiring SSN
Anti-Fraud	SSN used to detect/prevent fraud.	Fraud data matching
No Substitute	SSN required where no alternate ID exists.	Assigning ICN in VA MPI

Table 2B: Fraud Reduction and Data Analytics Act (FRDAA)

Exemption	Description	Example
Required by Law	SSN inclusion mandated by statute.	HUD housing applications
Other Legal Mandate	SSN needed to meet other legal mandates.	SSA misuse notification
No Substitute	SSN required if no alternate ID exists.	NOT permitted if Receivable ID available
Compelling Need	SSN needed for urgent, mission-critical tasks.	FOIA response, health record delivery

Bottom Line

The Consolidated Appropriations Act of 2024 and the Fraud Reduction and Data Analytics Act provide VA the statutory basis to retain SSN use where required for identification, fraud prevention, and data exchange. They also require continued progress toward reducing unnecessary or high-risk SSN use in Veteran-facing and administrative processes. These laws collectively underpin the direction established in this ADR.

Table 3: SSN Risk Tier Definitions

Risk Tier	Definition	Examples
High Risk	SSN is used or exposed in Veteran-facing interfaces, transmitted to external parties, or appears in unprotected outputs. Includes any SSN usage that could reasonably result in identity theft or privacy breach if mishandled. Also includes any use of SSN for authentication, such as using the full or partial SSN (for example, the last four digits) as a verification factor or credential to grant access to information or services. SSN may aid in identification when no adequate substitute exists but must never be used as an authenticator	•SSN in outbound correspondence (mail, email) •SSN in self-service portals or contact-center ID proofing questions •SSN in interfaces with external partners (e.g., DoD, SSA) •SSN in publicly accessible logs or reports •Use of SSN or last four digits as an authentication factor (for example, "confirm last four of SSN" during call-center verification)
Medium Risk	SSN is stored or processed internally but not exposed externally or to end users. Often present in back-office systems or operational data exchanges. Risk is moderate and limited to internal misuse or internal breach.	• SSN stored in internal reports or databases • SSN used in batch processing or system integrations • SSN available to VA staff through UI but not surfaced to Veterans
Low Risk	SSN is retained in archival systems or only accessed under strict conditions. No frequent usage, low exposure surface, and very limited access. May exist for records retention or compliance.	• Archived claims files • Read-only legacy data repositories • Encrypted backups with restricted access