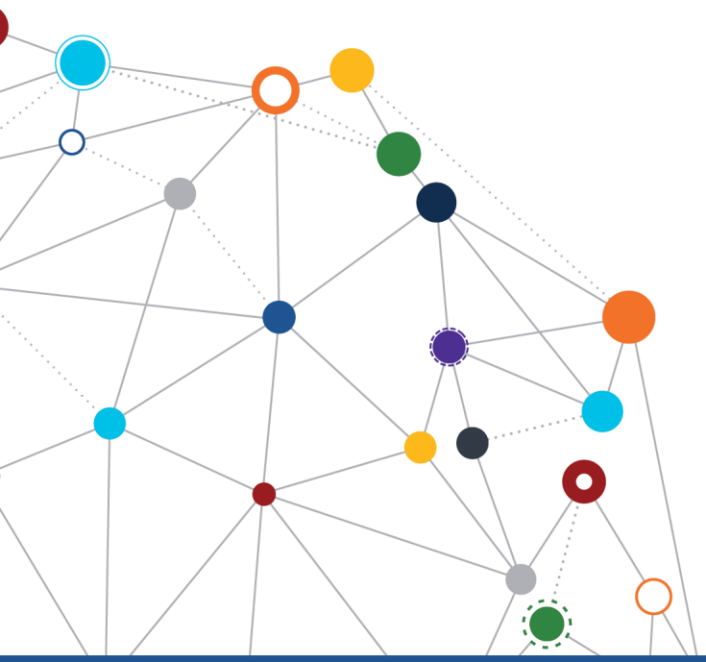
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Identity Proofing

November 2018 | Enterprise Program Management Office



VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

1 Context 3
2 Challenge 3
3 Guidance 4
3.1 VA User Identity Proofing 5
3.2 External User Identity Proofing 6
4 Application of Practices 12
4.1 Approval of a New External CSP 12
4.1.1 Purpose 12
4.1.2 Assumptions 12
4.1.3 Use Case Description 12
4.2 Key Practices 13
5 Impacts 13
Appendix: References 14

Figure 1: Overview of IAM Progression 4
Figure 2: Identity Proofing Steps 5

Table 1: Change Matrix 2
Table 2: IAL Overview and Acceptable Uses 7
Table 3: General External CSP Practices 9
Table 4: External CSP Practices by IAL 10
Table 5: Key Practices IAM Identity Proofing EDP 13

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	11/5/2018	IAM EDP Identity Proofing Segment document approved

1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11,[1] the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

Identity proofing, also known as identity verification, is the first step to providing user access to VA services. NIST 800-63-3, released in June 2017, makes impactful changes to identity proofing requirements.[2] Historically, only four (4) external identity providers (IdPs) have met the security requirements (Level of Assurance 3) to provide credentials required for access to VA sensitive information, such as electronic health records (EHRs). Currently, no external IdPs are listed by the General Services Administration (GSA) under the new NIST guidelines.

While VA can provide compliant identity proofing through local badging offices for internal staff, VA is already faced with challenges handling the current volume of requests and the occasional interruptions of the infrastructure. Identity proofing is required to provide timely access to VA services and prevent impersonation, leading to unauthorized access and fraud. The progression of how IAM services are engaged by users and system owners can be seen in Figure 1. This document focuses on the area highlighted in red.

[1] Note that M 11-11 is a pending rescission. A draft OMB policy aligned with NIST 800-63 can be found at https://policy.cio.gov/identity-draft/.

[2] The National Institute of Standards and Technology (NIST) Special Publication 800-63, Revision 3, *Digital Identity Guidelines*, can be referenced at https://pages.nist.gov/800-63-3/sp800-63-3.html.

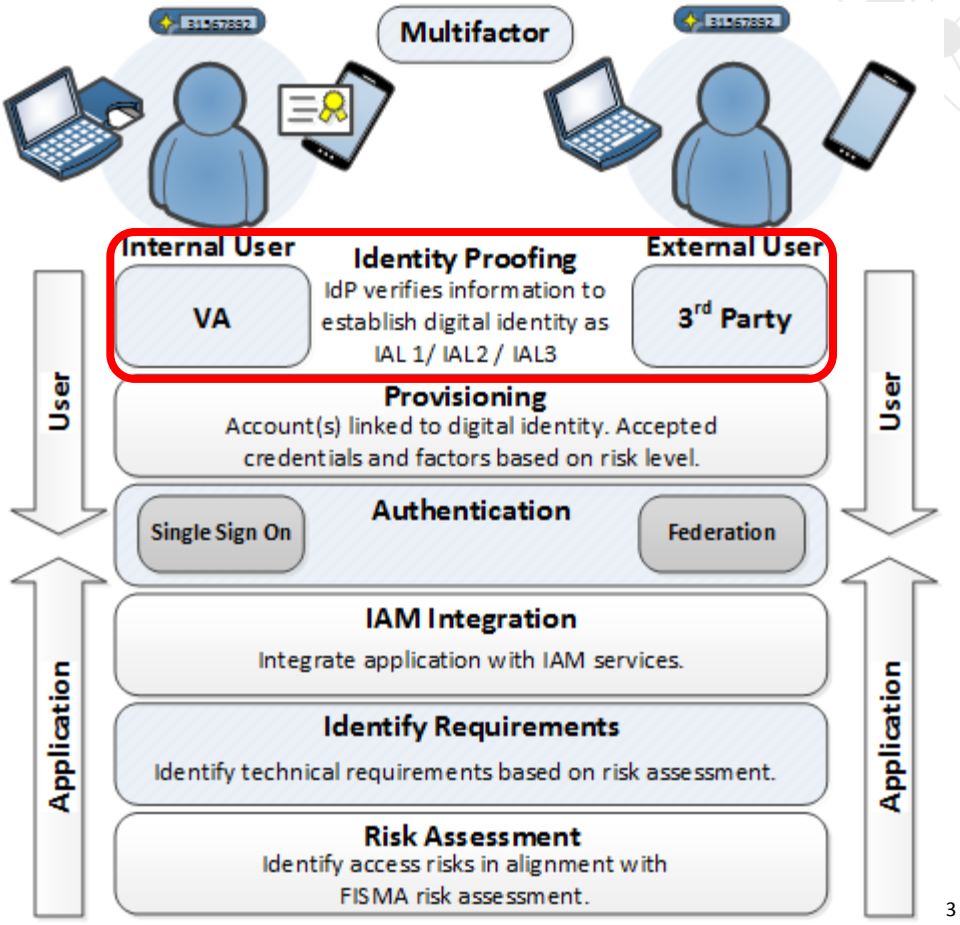


Figure 1: Overview of IAM Progression

3 Guidance

Projects that are required to use the Veteran-Focused Integration Process (VIP)[4] are subject to the VA Assessment and Authorization (A&A) Process,[5] which is based on the Risk Management

[3] Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[4] The VIP 3.1 Guide, April 2018, can be referenced at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27.

[5] The VIP Security Guide, (referenced at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27), provides details about the A&A process and how it reflects an implementation of NIST guidance and VA security policies. For additional information on VA Assessment and Authorization, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

Framework (RMF).[6] The associated risk assessment will result in a projected identity proofing and provisioning assurance level (IAL), which will drive identity proofing requirements. Please see the *IAM Risk Assessment* Enterprise Design Pattern (EDP) for more information on risk assessments and assurance levels.[7]

3.1 VA User Identity Proofing

All VA internal users undergo identity proofing before initiating any type of support for VA. The identity proofing process is part of the overall process for the issuance of a Personal Identity Verification (PIV) card, non-PIV card, or Flash Badge. The VA Office of Identity, Credential, and Access Management (OICAM) is responsible for compliance of the identity proofing service.

The VA IAM service provides a list of available attributes. To ensure accuracy, user identity attributes are captured during the identity proofing service. If additional attributes are required to support a business service, a Privacy Impact Assessment (PIA) may be required. If a PIA is required, the project team must contact the Office of Privacy and Records Management (OPRM) and coordinate with VA OICAM.[8]

For user account access to any VA system, VA applicants must be proofed at IAL 3, ensuring appropriate identity proofing for all VA positions and permission levels. Applicants should complete the steps shown in Figure 2.

Figure 2: Identity Proofing Steps

- **Resolution:** The Credential Service Provider (CSP) collects personally identifiable information (PII) from the applicant.
    a. An application is submitted. A PIV request form captures attributes that will be verified.

[6] Refer to the NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* at https://pages.nist.gov/800-63-3/sp800-63-3.html. In addition, the VA Handbook 6500, *Risk Management Framework for VA Information Systems*, can be referenced at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.
[7] Reference the *IAM Risk Assessment* Enterprise Design Pattern (EDP) at https://www.oit.va.gov/library/recurring/edp/.
[8] For additional information, refer to https://www.oprm.va.gov/privacy/privacy_compliance.aspx.

b. The applicant submits fingerprints at a VA facility for a Special Agreement Check (SAC).
c. The applicant is sponsored by an authorized VA user.
d. The applicant schedules an appointment and appears in person for identity proofing by an approved official within the PIV office.
e. The applicant presents at least two forms of superior[9] identity evidence, such as a passport and driver's license.[10] The PIV Office should not use a Social Security Card unless it is necessary for performing identity resolution; identity resolution cannot be accomplished by collecting another attribute or combination of attributes.

- **Validation:** An authorized and trained PIV Office Representative validates the applicant information by checking an authoritative source.
    a. Successful completion of a SAC is no issues within 120 days of issuance; and for PIV cards, an initiated National Agency Check with Written Inquiries (NACI), or higher background investigation, is validated.
    b. The identity evidence is validated to include attributes.
    c. Issuing sources for identity evidence are queried to validate that the information matches.
- **Verification:** The PIV Office verifies that the applicant matches the identity evidence presented.
    a. The applicant is compared to the photo that is part of the identity evidence. For remote proofing of internal VA users, liveliness checks must be performed. If remote proofing cannot be successfully completed, the applicant must appear in person.
    b. A biometric is captured (fingerprint) to verify the biometric submitted for the SAC.
    c. The applicant is successfully proofed.

3.2 External User Identity Proofing

External CSPs must not be used without approval in advance by VA OICAM. While VA strives to use externally-issued credentials for Veteran convenience, and in alignment with OMB guidance, all VA IAM services must comply with federal policy. NIST Publication 800-63-3

[9] The National Institute of Standards and Technology (NIST) Publication 800-63 defines strengths of identity proofing evidence as *unacceptable, fair, strong*, and *superior*. For the requirements to achieve each given strength, refer to Table 5-1, *Strengths of Identity Evidence*, at https://pages.nist.gov/800-63-3/sp800-63a/sec5_proofing.html.

[10] Section 5.2.1 of the National Institute of Standards and Technology (NIST) Publication 800-63A, *Digital Identity Guidelines*, provides quality requirements for identity evidence collected during identity proofing, ranging from *unacceptable* to *superior* to establish a valid identity; at https://pages.nist.gov/800-63-3/sp800-63a.html.

established updated requirements for identity proofing.[11] The requirements for external identity proofing are based on the IAL. A description of each IAL and its projected use is shown in Table 2.

Table 2: IAL Overview and Acceptable Uses

IAL	Description
IAL1	Pseudonymous: There is no requirement to link the applicant to a specific real-life identity. Appropriate for polling or other uses where the user identity does not need to be known or additional identity proofing will be performed later.
IAL2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this identity. This is the minimum that is recommended by the Office of the National Coordinator for Health Information Technology (ONC) as part of their draft Trusted Exchange Framework and Common Agreement (TEFCA) for access to electronic health records (EHR).
IAL3	A physical presence is required to connect the applicant with the claimed identity. It is appropriate for transactions where impersonation creates a high risk of fraud or other negative outcomes.

Once the IAL is specified as a result of the risk assessment,[12] it will guide the project team in identifying an external CSP, when required. There are three possible options for selecting an external CSP:

- The project team must select a CSP that was previously approved by OICAM. If VA OICAM does not have an approved CSP that can meet business requirements, the project team may submit a request to approve another external CSP.
- VA OICAM must first evaluate an external CSP for approval that is based on the Trust Framework Solutions (TFS) initiative.[13]
- If a suitable CSP is not available through TFS, VA OICAM must perform an external CSP risk assessment of a CSP that is not approved by TFS.

[11] For additional information, refer to The National Institute of Standards and Technology (NIST) Special Publication 800-63, Revision 3, *Digital Identity Guidelines*, at https://pages.nist.gov/800-63-3/sp800-63-3.html.
[12] For more information, refer to the *IAM Risk Assessment* Enterprise Design Pattern at https://www.oit.va.gov/library/recurring/edp/.
[13] Refer to the Trust Framework Initiative at https://www.idmanagement.gov/trust-services/#identity-services.

Trust Framework Solutions (TFS) initiative

The GSA ID Management Web Site enables project teams to review external CSPs for approval as part of TFS.[14] The GSA created this site to identify CSPs approved by the Federal Identity, Credential, and Access Management (FICAM) TFS initiative. The TFS program reviews the trust frameworks of commercial and non-profit organizations to determine whether the policies, processes, legal agreements, privacy protections, security controls, and audit requirements are comparable with the U.S. Government requirements. If comparable, the commercial and non-profit organizations that manage the trust frameworks of their communities will become adopted Trust Framework Providers. If the non-government service is acceptable for the mission purpose and has the same risk rating, it may be used. Currently, no external CSPs have been assessed to be compliant with any of the updated assurance levels identified in NIST 800-63-3.[15] Compliance with the previous NIST Level of Assurance (LOA) requirements is not an indicator of compliance with the current requirements.

External CSP Risk Assessment

If a suitable CSP cannot be identified using TFS, VA OICAM must review and approve any candidate CSP before any agreement is formed, or the CSP must agree to complete the TFS approval process. The risk assessment is used to meet compliance and identify high risk practices that could lead to impersonation, such as considering access to an email account as verification when the applicant is the registered owner. VA OICAM must perform the following actions to assess and approve any candidate CSPs:

- VA OICAM must consult with their Senior Agency Official for Privacy (SAOP) to determine the need to conduct a Privacy Impact Assessment (PIA) that is based on the collection of PII.
- VA must publish a System of Records Notice (SORN), if needed.
- VA OICAM must perform a documentation review to verify that compliant practices are met by any external CSP that is submitted for approval. Compliant CSP practices must be defined by VA policy based on NIST 800-63-3. Documentation may include those submitted for an Authorization to Operate (ATO) with another Federal agency.

A requirement for a user to submit PII to an external CSP to access VA services may create liability for VA. The service should be considered part of the Service Level Agreement (SLA). For more information on requirements to procure external CSP services, seek guidance from VA OICAM[16] and the Technology Acquisition Center (TAC).[17]

---

[14] Refer to the GSA ID Management site at https://www.idmanagement.gov/trust-services/#identity-services.
[15] Refer to assurance levels identified in NIST 800-63-3 at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec6.
[16] Reference the Office of Identity, Credential, and Access Management at https://www.osp.va.gov/Office_of_Personnel_Security_and_Identity_Management.asp.
[17] Reference the Technology Acquisition Center (TAC) at https://www.va.gov/opal/about/tac.asp.

Table 3 and Table 4 provide an overview of the external CSP requirements defined by NIST Publication 800-63A (see the NIST publication for the full text).[18]

Table 3: General External CSP Practices

Area	Requirement
General	• Identity proofing must not be performed to determine suitability or entitlement to gain access to services or benefits. • Collection of PII must be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. • CSP must provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes. • If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, CSPs must implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. • CSP must provide mechanisms for redress of applicant complaints or problems. The CSP must assess the mechanisms for their efficacy in achieving resolution of complaints or problems. • Identity proofing and enrollment processes must be performed according to an applicable written policy. • CSP must maintain a record, including audit logs, of all steps taken to verify the identity of the applicant and must record the types of identity evidence considered. Record retention should be defined in years according to VA policy. • All PII collected as part of the enrollment process must be protected to ensure confidentiality, integrity, and attribution of the information source. • All proofing transactions must occur over an authenticated protected channel. • The CSP should obtain additional confidence in identity proofing using fraud mitigation measures

[18] For additional information, reference the National Institute of Standards and Technology (NIST) at https://pages.nist.gov/800-63-3/sp800-63a.html.

	• In the event a CSP ceases to conduct identity proofing and enrollment processes, the CSP must be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. • Regardless of whether the CSP is an agency or private sector provider, the following requirements apply to the agency offering or using the proofing service regarding privacy. The agency must consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements. The agency must consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements. The agency must publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable. • The CSP should not collect the Social Security Number (SSN) unless it is necessary for performing identity resolution, and identity resolution cannot be accomplished by collection of another attribute or combination of attributes. • Due to significant and repeated data breaches of PII, knowledge-based verification (KBV) should not be used for identity proofing in any manner except for IAL 1.

Table 4: External CSP Practices by IAL[19]

Area	IAL1	IAL2	IAL3
Presence	No requirements	In-person and unsupervised remote; VA shall plan a method to support both based on applicant preference	In-person and supervised remote
Resolution	No requirements	The minimum attributes necessary to accomplish identity resolution	Same as IAL2

[19] The National Institute of Standards and Technology (NIST) Publication 800-63 defines strengths of identity proofing evidence as unacceptable, fair, strong, and superior. For the requirements to achieve each given strength, refer to Table 5-1, *Strengths of Identity Evidence*, at https://pages.nist.gov/800-63-3/sp800-63a/sec5_proofing.html.

Evidence	No identity evidence is collected	One piece of SUPERIOR or STRONG evidence, or two pieces of STRONG evidence, or one piece of STRONG evidence plus two (2) pieces of FAIR evidence	Two pieces of SUPERIOR evidence, or one piece of SUPERIOR evidence and one piece of STRONG evidence, or two pieces of STRONG evidence plus one piece of FAIR evidence
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG	Verified by a process that is able to achieve a strength of SUPERIOR
Address Confirmation	N/A	Required; enrollment code sent to any address of record; notification of proofing and enrollment code SHALL NOT be sent to the same address of record	Required. Notification of proofing to postal address
Enrollment Code Use	N/A	If issued via unsupervised remote identity proofing, enrollment code shall be sent to a confirmed address of record	
Enrollment Code Max Expiration	N/A	In-person or real-time delivery: 7 days; postal address delivery CONUS: 10 days postal address delivery OCONUS: 30 days; SMS or phone call delivery: 10 minutes Email: 30 minutes	In-person or real-time delivery: 7 days
Enrollment Code Design	N/A	A random six-character alphanumeric or higher entropy; QR code is also allowed with equivalent entropy	A random six-character alphanumeric or higher entropy; QR code is also allowed with equivalent entropy
Biometric Collection	N/A	Optional; VA only provides compatibility with fingerprints at this time	Mandatory; VA-only provides compatibility with fingerprints at this time

Security Controls	N/A	SP 800-53 Moderate Baseline	SP 800-53 High Baseline

4 Application of Practices

The following use case represents application of the identity proofing practices described in this document.

4.1 Approval of a New External CSP

4.1.1 Purpose

Updated Federal policy has been released with new requirements for identity proofing. VA has many IT services which require external users to have a compliant user account for access. An external CSP is required that is compliant with Federal policy and can scale to meet VA needs.

4.1.2 Assumptions

- A business justification exists for an external CSP for identity proofing.
- VA IAM and the GSA FICAM website do not have a suitable and compliant CSP to meet business needs.
- A risk assessment has been completed to determine the appropriate IAL.
- Once a CSP is determined to be technically viable, a review of the procurement process is outside the scope of this use case.
- Identity proofing is the focus of the use case; the use case does not discuss integration of new applications with VA IAM services.

4.1.3 Use Case Description

- The system owner has submitted the business case for a solution enhancement as a VIP Request (VIPR). The system requires integration with VA IAM for user access.
- The system owner contacts the VA IAM service to identify integration requirements. As part of the analysis, VA IAM determines that the volume of applicants for identity proofing would exceed processing capacity of the VA PIV offices, which are currently only used for internal VA users; an external CSP is required.
- VA IAM does not have an approved CSP that is compliant with the updated federal policy yet and one is not approved through FICAM. A risk assessment is required to approve a new external CSP.
- VA OICAM completes the risk assessment for a candidate CSP using vendor-supplied information, or available ATO documentation.
- Any gaps in compliance are identified. A risk based decision is made and the CSP is approved for integration with VA Single Sign On External (SSOe) and acquisition of services may proceed.

4.2 Key Practices

Table 5 highlights key practices identified in this Enterprise Design Pattern (EDP).

Table 5: Key Practices IAM Identity Proofing EDP

Category	Area	Description
Identity and Access Management	Identity Proofing	The VA IAM service provides a list of available attributes. If additional attributes are required to support a business service, the IAM service must be contacted, since a Privacy Impact Assessment (PIA) may be required.
Identity and Access Management	Identity Proofing	Internal VA applicants that will be issued a user account for access to any VA system must be proofed at IAL 3.
Identity and Access Management	Identity Proofing	For remote proofing of internal VA users, liveliness checks must be performed.
Identity and Access Management	Identity Proofing	Project teams must select a CSP previously approved by IAM. If VA IAM does not have an approved CSP that can meet business requirements, the project team may submit a request to approve another external CSP.
Identity and Access Management	Identity Proofing	VA IAM must give preference to an external CSP based on the Trust Framework Solutions (TFS) initiative before proceeding with other risk assessments.
Identity and Access Management	Identity Proofing	If a suitable CSP is not available through TFS, VA OICAM must perform an external CSP risk assessment of a CSP that is not approved by TFS or the CSP may opt to complete the TFS process.
Identity and Access Management	Identity Proofing	Compliant CSP practices must be defined by VA policy that is based on NIST 800-63A.

5 Impacts

If risk management is not used to define the technical requirements for IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access, data breach, or fraud

Appendix: References

- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- FISMA User Stories: https://vaww.portal2.va.gov/sites/asd/AERB/FISMASecurityCompliance/SitePages/Home.aspx
- TRM: http://trm.oit.va.gov/
- NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2
- TFS Providers: https://www.idmanagement.gov/trust-services/#identity-services

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.