COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1.A
Identity Proofing and Verification

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding identity proofing and verification. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, *Code of Virginia*
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).

- The document was reviewed by IMSAC during a council workshop, May 2, 2016.

- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C. IMSAC allowed at least 30 days for the submission of written comments following the posting and publication and held a meeting dedicated to the receipt of oral comment on June 30, more than 15 days after the posting and publication. The following comments were received on July 13, 2016, via the Virginia Regulatory Town Hall, with the response shown in brackets []:

    - For purposes of setting minimum standards for identity proofing and issuance of credentials/tokens/authenticators, continue to use levels of assurance as defined in the latest approved NIST 800-63 document series. This will be especially important to both identity providers and relying parties in the commercial sector. [Noted]

  - On pages 21 and 22 under discussions of Level of Assurance 2, 3, and 4, add references to "virtual in-person proofing" as an approved method consistent with draft 800-63A. [The assurance model applied in the IMSAC guidance document series has been amended to be consistent with NIST SP 800-63-3. A definition for “virtual in-person proofing” based on NIST SP 800-63A has been added to this document.]
  - On page 15, add a definition of "virtual in-person proofing" perhaps based on section 5.4.3 of draft 800-63A. [A definition for “virtual in-person proofing” has been added to this document, consistent with NIST SP 800-63A.]
  - On page 12, add a definition of "remote network identity proofing." This could be modeled after language contained in NIST 800-63 series documents. [The term “remote network identity proofing” has not been defined in the NIST SP 800-63 document series. However, the term “remote” has been defined in the NIST SP 800-63 document series and in this document, and the definition covers remote transactions across a network in an identity proofing context.]

- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for identity proofing and verification within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology
§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council
§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act
Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the IMSAC Reference Document: Terminology and Definitions, which may be accessed at http://vita.virginia.gov/default.aspx?id=6442475952

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3
- Electronic Identity Management Act (§ 59.1-550), available at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550
- International Telecommunication Union, Recommendation X. 1255, available at http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for identity proofing and verification to enable registration and authentication events within a digital identity system. The minimum specifications conform with NIST SP 800-63-3.

The document defines minimum requirements, components, process flows, assurance levels, and privacy and security provisions for identity proofing and verification. The document assumes that specific business, legal, and technical requirements for identity proofing and verification will be established in the identity trust framework for each distinct digital identity system, and that these requirements will be designed based on the Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL) requirements for the system.

This guidance document focuses on identity proofing and verification. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines digital authentication as the process of establishing confidence in user identities digitally presented to a system.[1] Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

Digital authentication begins with enrollment. The enrollment process involves an applicant applying to a CSP. If approved, the CSP creates a credential and binds it to one or more authenticators. The credential includes at least one identifier, which can be pseudonymous, and may include one or more attributes that the CSP has verified. The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or provided by a third party. The authenticator and credential may be used in subsequent authentication events.

The process used to verify an applicant's association with their real world identity is called identity proofing. The strength of identity proofing is described by a categorization called the Identity Assurance Level (IAL, see *IMSAC Reference Document: NIST Assurance Model*).

This document establishes minimum specifications for the identity proofing and verification components of enrollment events in a digital identity system. Identity trust frameworks for digital identity systems should document the business, legal, and technical requirements for these components, as well as requirements for the remaining components of the system. Minimum specifications for identity trust frameworks have been defined in *IMSAC Guidance Document 2: Identity Trust Frameworks*.

Identity Proofing Requirements

Identity proofing and verification for enrollment should be designed to meet the specific requirements for the assurance model defined by the governing identity trust framework for the digital identity system. A trusted enrollment process ensures that (i) the RA and CSP have established the true identity of the applicant, (ii) the enrollment protocols satisfy the requirements for each assurance level, (iii) the RA and CSP maintain a record of the identity evidence and transaction flows to meet audit and compliance requirements, and (iv) the RA and CSP implement enforcement mechanisms to ensure compliance with all applicable provisions established in the identity trust framework.

[1] The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

At a minimum, identity proofing and verification requirements should establish that:

- A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The applicant whose authenticator is issued is in fact the person who is entitled to the identity;
- It is difficult for the claimant to later repudiate the enrollment and dispute an authentication using the subscriber's authenticator;
- Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated).

Enrollment, and the associated identity proofing and verification processes, may be completed through remote or in-person (physical or virtual) protocols. Provisions for remote versus in-person identity proofing and verification should be established in the identity trust framework for the digital identity system and satisfy requirements of the applicable assurance model.

Components and Process Flow

The enrollment process, during which identity proofing and verification protocols are invoked, generally involve the following components:

- The applicant's attestation of a claimed identity
- The applicant's presentation of evidence to prove the existence of the claimed identity
- The RA's review and validation of the applicant's claimed identity and supporting evidence
- The CSP's verification of the applicant's claimed identity
- The CSP's issuance or enrollment of a credential bound to the applicant's authenticator

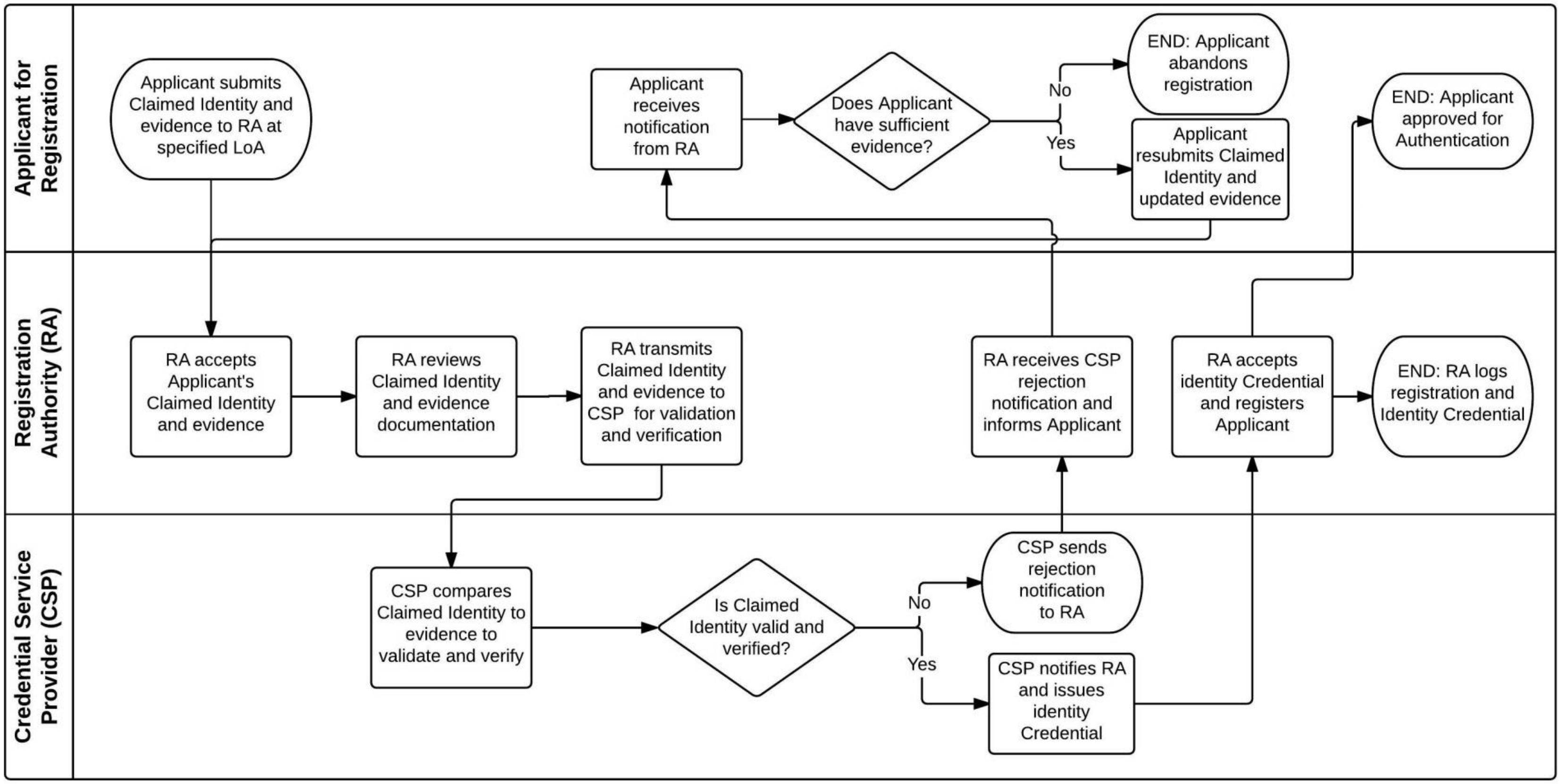
The process flow for implementing the components of the identity proofing and verification for enrollment generally consists of the following (**Figure 1**):

1. The applicant attests to the trusted RA a claimed identity at a specified assurance level
2. The applicant provides the RA either remotely or in person, depending on the assurance model requirements of the identity trust framework, evidence to prove the existence of the claimed identity (identity proofing) Note: Source of original identity document(s) must meet the assurance model and related compliance requirements set by the RA and defined in the identity trust framework
3. The RA transmits the identity proofing evidence to the CSP to verify whether the evidence may be considered valid (identity Validation)
4. The CSP compares the applicant's claimed identity to information associated with the claimed identity to determine whether it relates to the applicant (attribute verification)[2]

[2] The attribute verification process may consist of multiple steps and factors, including attribute information, knowledge-based tests, biometrics, activity history, counter-fraud checks, etc., depending on the assurance model requirements established in the identity trust framework. Specific attribute verification requirements should be defined in the governing identity trust framework for the digital identity system. Minimum specifications for attribute verification will be addressed in a forthcoming guidance document in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

5. Upon successful completion of the attribute verification process, the CSP issues to the RA a credential bound to an authenticator for the applicant, confirming the applicant's claimed identity at the appropriate assurance level defined in the identity trust framework for the digital identity system
6. RA maintains a record of the evidence and transaction for the enrollment process.

Figure 1. Identity Proofing and Verification Process Flow


Applicant for Registration
Registration Authority (RA)
Credential Service Provider (CSP)
Applicant submits Claimed Identity and evidence to RA at specified LoA
Applicant receives notification from RA
Does Applicant have sufficient evidence?
No
Yes
END: Applicant abandons registration
Applicant resubmits Claimed Identity and updated evidence
END: Applicant approved for Authentication
RA accepts Applicant's Claimed Identity and evidence
RA reviews Claimed Identity and evidence documentation
RA transmits Claimed Identity and evidence to CSP for validation and verification
RA receives CSP rejection notification and informs Applicant
RA accepts identity Credential and registers Applicant
END: RA logs registration and Identity Credential
CSP compares Claimed Identity to evidence to validate and verify
Is Claimed Identity valid and verified?
No
Yes
CSP sends rejection notification to RA
CSP notifies RA and issues identity Credential

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for identity proofing and verification apply the Fair Information Practice Principles (FIPPs).[3] The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.[4]

The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem Steering Group (IDESG) in October 2015 (**Appendix 2)**.

The minimum specifications for identity proofing and verification apply the following FIPPs:

- Transparency: RAs and CSPs should be transparent and provide notice to applicants regarding collection, use, dissemination, and maintenance of person information required during the enrollment, identity proofing and verification processes.
- Individual Participation: RAs and CSPs should involve the applicant in the process of using person information and, to the extent practicable, seek consent for the collection, use, dissemination, and maintenance of that information. RAs and CSPs also should provide mechanisms for appropriate access, correction, and redress of person information.
- Purpose Specification: RAs and CSPs should specifically articulate the authority that permits the collection of person information and specifically articulate the purpose or purposes for which the information is intended to be used.
- Data Minimization: RAs and CSPs should collect only the person information directly relevant and necessary to accomplish the enrollment and related processes, and only retain that information for as long as necessary to fulfill the specified purpose.
- Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for the purpose specified in the notice. Disclosure or sharing that information should be limited to the specific purpose for which the information was collected.
- Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that person information is accurate, relevant, timely, and complete.
- Security: RAs and CSPs should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: RAs and CSPs should be accountable for complying with these principles, providing training to all employees and contractors who use person information, and auditing the actual use of person information to demonstrate compliance with these principles and all applicable privacy protection requirements.

[3] The term “person information” refers to protected data for person entities. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Protected Education Records, and related categories. Specific requirements for the privacy and security of person information should be defined by the identity trust framework for the digital identity system.

[4] The FIPPs endorsed by NSTIC may be accessed at http://www.nist.gov/nstic/NSTIC-FIPPs.pdf . The FIPPs published in SICAM may be accessed at http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf.

8 Alignment Comparison

The minimum specifications for identity proofing and verification established in this document have been developed to align with existing national and international standards for e-authentication and identity management. Specifically, the minimum specifications reflect basic requirements set forth in national standards at the federal and state level, ensuring compliance while accommodating other identity management standards and protocols. This document assumes that each digital identity system and supporting identity trust framework will comply with those governing standards and protocols required by Applicable Law.

The following section outlines the alignment and disparities between the minimum specifications in this document and core national standards. A crosswalk documenting the alignment and areas of misalignment has been provided in **Appendix 3**.

NIST SP 800-63-3

The minimum specifications in this document conform with the basic requirements for digital authentication set forth in NIST SP 800-63-3 (Public Review version). However, as the NIST guidance defines specific requirements for federal agencies, the minimum specifications in this document provide flexibility for digital identity systems across industries in the private sector and levels of governance. This flexibility enables digital identity systems to adhere to the specifications but do so in a manner appropriate and compliant with their governing identity trust frameworks.

State Identity and Access Management Credential (SICAM) Guidance and Roadmap

The minimum specifications in this document conform with the basic requirements for identity proofing and verification set forth by NASCIO in the SICAM Guidance and Roadmap. The NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with the NIST guidance for federal agencies, the minimum specifications in this document provide flexibility for digital identity systems across industries in the private sector and levels of governance.

IDESG Identity Ecosystem Framework (IDEF) Functional Model

The minimum specifications in this document conform with the core operations and basic requirements for privacy and security set forth by IDESG in the IDEF Functional Model and Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend them to cover the NSTIC Guiding Principles. The minimum specifications in this document encourage adherence to the IDEF Functional Model, Baseline Functional Requirements, and the NSTIC Guiding Principles.

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council’s membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit: https://vita.virginia.gov/About/default.aspx?id=6442474173

Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for Privacy and Security

PRIVACY-1. DATA MINIMIZATION
Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION
Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION
Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION
Entities MUST NOT request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK
Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

PRIVACY-6. USAGE NOTICE
Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL
Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS
Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER NOTICE OF CHANGES
Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE
USERS MUST have the opportunity to decline enrollment; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION
Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY
Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK
Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL
Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION
Wherever feasible, identifier data MUST be segregated from attribute data.

SECURE-1. SECURITY PRACTICES
Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SECURE-2. DATA INTEGRITY
Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data—including authentication data and attribute values—during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SECURE-3. CREDENTIAL REPRODUCTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SECURE-4. CREDENTIAL PROTECTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SECURE-5. CREDENTIAL ISSUANCE
Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where enrollment and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of enrollment and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SECURE-6. CREDENTIAL UNIQUENESS
Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SECURE-7. TOKEN CONTROL
Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SECURE-8. MULTIFACTOR AUTHENTICATION
Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SECURE-9. AUTHENTICATION RISK ASSESSMENT
Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SECURE-10. UPTIME
Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SECURE-11. KEY MANAGEMENT
Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.

SECURE-12. RECOVERY AND REISSUANCE
Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original enrollment and credentialing operations.

SECURE-13. REVOCATION
Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SECURE-14. SECURITY LOGS
Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SECURE-15. SECURITY AUDITS
Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix

Component	NIST 800-63-3	SICAM	IDESG IDEF Functional Model
Applicant Claimed Identity	Alignment: Defines protocols and process flows for applicant assertion of claimed identity to federal agencies	Alignment: Defines protocols and process flows for applicant assertion of claimed identity to state agencies	Alignment: Identifies core operations within standard enrollment process flows for applicant claimed identity
	Misalignment: Federal protocols for applicant's claimed identity apply to federal agencies but may not be appropriate across sectors or private industry	Misalignment: Minor variations in terminology with Commonwealth's minimum specifications	Misalignment: Core operational definitions do not contain specific criteria for the process of applicant assertion of claimed identity
Applicant Identity Evidence	Alignment: Establishes rigorous requirements for what federal agencies may accept as identity evidence	Alignment: Establishes rigorous requirements for what state agencies may accept as identity evidence	Alignment: Defines core operations for attribute control and identity evidence, and for maintenance of records
	Misalignment: Federal requirements for acceptable identity evidence may not be appropriate across sectors or private industry	Misalignment: SICAM model provisions for acceptable identity evidence may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for acceptable identity evidence or maintenance of records
RA Validation of Applicant Claimed Identity	Alignment: Sets protocols and required flows for federal agencies to follow in RA Validation of claimed identity	Alignment: Sets protocols and required flows for state agencies to follow in RA Validation of claimed identity	Alignment: Documents core operations for Validation of claimed identity
	Misalignment: Federal protocols for RA Validation of claimed identity may not be appropriate across sectors or private industry	Misalignment: SICAM model for RA Validation of claimed identity may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for RA Validation of claimed identity
CSP Verification of Applicant Claimed Identity	Alignment: Provides clearly defined technical requirements for federal agencies to follow in CSP verification of claimed identity	Alignment: Provides clearly defined technical requirements for state agencies to follow in CSP verification of claimed identity	Alignment: Defines core operations for CSP verification of applicant claimed identity
	Misalignment: Federal verification protocols and requirements may not be appropriate across sectors or private industry	Misalignment: SICAM model for CSP verification of claimed identity may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria or technical requirements for CSP verification
CSP Issuance/Registration of Applicant Credential	Alignment: Establishes protocols and technical requirements for issuance/ enrollment of identity credentials	Alignment: Establishes protocols and technical requirements for issuance/ enrollment of identity credentials	Alignment: Identifies core operational roles and responsibilities for Issuance/ enrollment of identity credentials
	Misalignment: Federal credential issuance/ enrollment protocols may not be appropriate across sectors or private industry	Misalignment: State government credential issuance/enrollment protocols may not be appropriate across sectors or private industry	Misalignment: Core operational roles and responsibilities do not contain specific criteria for audit and compliance purposes