OFFICE OF THE STATE CIO

IT POLICY LETTER

	NUMBER: **ITPL 10-17**
SUBJECT: **ESTABLISHMENT OF THE IDENTITY AND ACCESS MANAGEMENT (IdAM) POLICY** **Emphasis:** Enterprise Architecture Standard and Practice for Identity and Access Management	DATE ISSUED: DECEMBER 30, 2010
	EXPIRES: Until Rescinded
REFERENCES: State Administrative Manual Sections 4819.31.6, 4906, and 5100 Statewide Information Management Manual Sections 58A, 58D and 158A Federal Identity, Credential, and Access Management (FICAM) Roadmap	ISSUING AGENCY: OFFICE OF THE STATE CHIEF INFORMATION OFFICER

Note: Agency[1] Chief Information Officers (Agency CIO) and Department Chief Information Officers (CIO) are requested to forward a copy of this Information Technology Policy Letter (ITPL) to their respective Enterprise Architects.

DISTRIBUTION

Agency Secretaries
Agency Chief Information Officers
Agency Information Security Officers
Department Directors
Department Chief Information Officers
Department Information Security Officers

PURPOSE

California State Government faces significant challenges in carrying out its mission of delivering services to the public and meeting the needs of its business partners while leveraging current information technology. One of the key challenges is the ability to verify an individual's identity when conducting business.

Further, as state agencies increase their online service offerings, it becomes increasingly important to establish a framework for the development and use of an effective statewide cyber security solution that addresses identity and access management. Authentication and access to applications, especially those requiring connectivity across organizational boundaries (i.e. security domains), must be controlled by an Identity and Access Management (IdAM) policy and associated standard and framework.

Accordingly, to build on the statewide Enterprise Architecture (EA) established by the Office of the State Chief Information Officer (OCIO)[2] when ITPL 09-03 was released in April 2009, and further enhanced and clarified when ITPL ITPL 10-15 was released in December 2010, the purpose of this ITPL is to:

[1] When capitalized, the term "Agency" refers to one of the state's super Agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. When used in lower case, the term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this ITPL, "agency" and "department" are used interchangeably.

[2] Effective January 1, 2011, the Office of the State Chief Information Officer (OCIO) is renamed the California Technology Agency (Technology Agency).

	• Announce the addition of the IdAM EA Standard to Section 58D.1 of the Statewide Information Management Manual (SIMM) as Technical Reference Model (TRM) ID number 1.5.885.001. • Announce the addition of the State Identity and Credential Access Management (SICAM) EA Practice to Section 158A of the SIMM as TRM ID number 1.5.885.002.
BACKGROUND	As described in Government Code Section 11545, the OCIO has broad responsibility and authority to guide the application of IT in California State Government. This includes establishing and enforcing state IT strategic plans, policies, standards and EA. Agencies are required to implement their EA in accordance with the guidelines and instructions included in Section 58 of the SIMM, as described in Sections 4819.31.6 and 4906 of the SAM. In addition, as stated in the SAM Section 5100, agencies must use the American National Standards Institute (ANSI) standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. Consistent with the state's use of ANSI and FIPS standards, the Federal Identity, Credential and Access Management (FICAM) Roadmap was used as the basis for developing the IdAM EA Standard and the SICAM EA Practice.
POLICY	The IdAM EA Standard, TRM 1.5.885.001, included in the SIMM in Section 58A.1 shall be used for all exchange of authentication and authorization data between security domains within the California State Government. The implementation of the IdAM EA Standard and the framework for providing a federated domain trust service is identified in the SICAM Roadmap and Implementation Guidelines included as EA Practice TRM 1.5.885.002 in Section 158A of the SIMM.
ROLES AND RESPONSIBILITIES	Agency CIOs shall ensure departments are in compliance with this policy through their department CIOs. Agency-affiliated department CIOs shall ensure IT solutions are developed, modified or upgraded in accordance with SIMM Section 58. CIOs who are not affiliated with an Agency have the same responsibilities as Agency CIOs and Agency-affiliated department CIOs.
APPLICABILITY	All state agencies under the direct executive authority of the Governor's Office are required to comply with this policy.
EXCEPTIONS	Changes and variances may be proposed using the Compliance Component Tools in Section 3.2.2 of the Enterprise Architecture Developers Guide, and by following the EA Compliance Package submittal instructions in Section 5.2. Additional detail is also included in Section 4.1 within the "Compliance Components Modification" subsection. The Enterprise Architecture Developers Guide is available in Section 58 of the SIMM.
SIMM CHANGES	The SIMM, located at http://www.cio.ca.gov/Government/IT_Policy/SIMM.html, has been

updated to include the following changes:

- **SIMM Section 58D.1, Enterprise Architecture Standards, Technical Reference Model –** The addition of the IdAM EA Standard as TRM ID number 1.5.885.001.
- **SIMM Section 158A, Enterprise Architecture Practices, Technical Reference Model –** The addition of the SICAM EA Practice as TRM ID number 1.5.885.002.

CONTACT

Questions regarding this policy should be directed to Lee Mosbrucker, Deputy Director for Enterprise Architecture, at (916) 403-9624, or by e-mail at Lee.Mosbrucker@state.ca.gov.

SIGNATURE

/s/

Christy Quinlan,
Acting Chief Information Officer
State of California