pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Federal ID Assurance Standards

ITP Number	***Effective Date***
BPD-SEC013I	January 18, 2008
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

1. Introduction

Defense against fraudulent and malicious intrusion on government-owned assets is at the forefront of commonwealth security policy. The threats of identity fraud and cyber-terrorism are at all-time highs and identity protection is a national priority. At the same time, information sharing and greater collaboration among government agencies have become increasingly vital for the country's security. In an attempt to resolve the lack of trust between federal agencies, and improve agency interoperability, the federal government has established policy that sets minimum proofing standards for various levels of identity trust, and a common credentialing system that can be uniformly accepted by all federal agencies. These proofing and credentialing standards have been published for voluntary incorporation by the states and other partners of the federal government, and a Federal Bridge Certification Authority (FBCA) has been established to cross-certify credentialing programs for federal interoperability.

The Commonwealth of Pennsylvania Identity Management and Access Protection (IPAM) policy published in the SEC013 series of Information Technology Policies (ITPs) and supporting documentations incorporates a set of assurance levels that are compliant with the Federal Standard; however, the commonwealth naming convention for these levels is different. This is because the assurance level nomenclature of the federal Office of Management and Budget (OMB) and the nomenclature used by the FBCA also differ. The purpose of this document is to:

- explain the rationale behind the Commonwealth Assurance Level nomenclature;
- establish its correspondence to the OMB and FBCA;
- detail the federal proofing requirements necessary to attain each Assurance Level; and;
- detail the federal guidance provided for how these Assurance Levels are to be utilized for authentication to secured assets.

2. Assurance Level Proofing Requirements

Table I: *Identity Proofing Requirements* identifies the minimum proofing requirements appropriate for each assurance level. The requirements for these levels were derived from a combination of National Institute of Standards and Technology (NIST) SP 800-63 and the X.509 Certificate Policy for the FBCA. In addition to the commonwealth nomenclature for each assurance level, Table I also lists the corresponding assurance levels from NIST/OMB E-Authentication guidance and the FBCA.

References to "Address of Record" in the following tables refer to the applicant's current address as recorded in the agency's account records for that individual. If the applicant claims to have a different address than the "Address of Record," the individual is to be directed to complete the agency's address-update process prior to completing the credentialing process.

References to in-person proofing are applicable when the applicant appears directly in front of the Registrar. Remote proofing is applicable when identity proofing documentation has been forwarded to the registrar and the applicant is not physically present.

Table I. Identity Proofing Requirements	
Assurance Level	**Minimum Requirements**
100 (None) Corresponds to: • NIST/OMB Level 1 • FBCA Rudimentary Level	No specific requirements at this level. This level indicates there is no assurance of identity other than the recipient's word.

Table I. Identity Proofing Requirements	
Assurance Level	**Minimum Requirements**
200 (Low) Corresponds to: • NIST/OMB Level 2 • FBCA Basic Level Note: This level was accepted by the Department of Homeland Security for First Responders during the 2006 Winter Fox exercise.	In-Person: Requires possession of a valid current primary government photo ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport). Registrar or Enrolling Official: • Inspect Photo-ID, compare picture to applicant, record ID number, address and date of birth. If ID appears valid and photo matches applicant then: a) if ID confirms the address of record, then authorize issuance of the credentials and send notification of same to that address; b) if ID does not confirm address of record, issue credentials in a manner that will confirm the applicant's address. For instance, the agency may choose to mail the credential to the address of record in an envelope stamped "if not at this address, return to sender." Remote Delivery Channel: Requires possession of a valid government ID number (e.g., a driver's license or passport) and a financial account number (e.g., checking account, savings account, loan or credit card) with method of confirmation (e.g., bank contact, credit check). Registrar or Enrolling Official: • Inspects both ID number and account number supplied by applicant. Verify information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to uniquely identify the individual. • Initiate address confirmation and notification: a) Send notice to the address of record confirmed by the records check; or b) Issue credentials in a manner that confirms the address of record supplied by the applicant; or c) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at the number or e-mail address indicated by the applicant's records.

Table I. Identity Proofing Requirements	
Assurance Level	**Minimum Requirements**
300 (Moderate) Corresponds to: • NIST/OMB Level 3 • FBCA Medium Level	In-Person: Requires possession of a verified current primary government photo ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport). Registrar or Enrolling Official: • Inspect Photo-ID and verify via the issuing organization or through credit bureaus or similar databases. Confirm that name, date of birth, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address, and date of birth. If ID is valid and photo matches applicant then: a) if ID confirms address of record, authorize or issue credentials and send notice to address of record; b) if ID does not confirm address of record, issue credentials in a manner that confirms address of record. Remote: Requires possession of a valid government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Registrar or Enrolling Official is to: • Verify information provided by applicant including ID number and account number through record checks, either with the applicable agency or institution or through credit bureaus or similar databases. Confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records while recording the applicant's voice.

Table I. Identity Proofing Requirements	
Assurance Level	**Minimum Requirements**
400 (High) Corresponds to: • NIST/OMB Level 4 • FBCA Medium (for Hardware) or High Level • FIPS 201 with Agency Discretion NACI	In-Person: Requires in-person appearance and verification of two independent ID documents or accounts, one of which is to be the current primary government picture ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant at the time of application. Registrar or Enrolling Official: • *Primary Photo ID:* Inspect photo-ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and date of birth. • *Secondary Government ID or financial account:* a) Inspect photo-ID and if apparently valid, compare picture to applicant, record ID number, address, and date of birth; or b) Verify financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that: name, date of birth, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. • *Record Current Biometric* Record a current biometric (e.g., photograph or fingerprints) to ensure that applicant cannot repudiate application. • *Confirm Address* Issue credentials in a manner that confirms address of record. • *Conduct appropriate background check if required.* Remote: Not Applicable

A credential is evidence attesting to one's right to credit or authority. In most cases for the commonwealth, this credential would take the form of that person's Personal Identity Verification (PIV) Card (a hard token); but it is also applicable to other data elements associated with an individual that authoritatively bind an identity to that individual (soft tokens). Applicants are to be vetted to the Table I minimum requirements before the appropriate Commonwealth of Pennsylvania Enterprise Directory (CoPED) assurance level is assigned and the corresponding credential issued.

Agencies may impose additional vetting requirements, such as a national background check (the FBI National Agency Check [NAC] and the National Agency Check and Inquiry [NACI]), or perform checks against criminal history records, terrorist watch lists, legal immigration status, or for outstanding wants and warrants. While these additional checks may be needed to meet specific agency requirements, they have no additional bearing on the assigned CoPED proofing level or designated assurance level.

Once an individual is vetted, his CoPED assurance level is stored as a user attribute in CoPED. Any additional checks required by an agency will also be maintained in CoPED to prevent duplication of effort in case another agency has the same special requirement. The personal

information used to vet the identity, however, will not be stored in this directory. Storage, management and security of the data collected in the vetting process is the responsibility of the enrolling agency and is to conform to all appropriate legislation governing the storage of personal data, including Pennsylvania Act 94 of 2006 (Senate Bill 712) the *Breach of Personal Information Notification Act ,* 73 P.S. §§ 2301, *et seq*.

Corresponding Federal Authentication Mechanisms

Table II, *Authentication Mechanisms for Physical and Logical Access,* demonstrates the Federal standard for determining appropriate Authentication Mechanisms for secured assets. This table presents separate columns for the FIPS 201-1 mechanisms for physical access, logical access from local workstations, and logical access for remote or network access. An additional column is also presented for the E-Authentication logical access mechanisms specified in SP 800-63, including the FBCA policies (SP 800-63, FBCA X.509 policy, and FIPS 140-2). Authentication at any level also allows access at all lower levels.

Table II. Authentication Mechanisms for Physical and Logical Access

Assurance Level	**FIPS 201-1 Mechanisms for use with PIV Card**			**E-Authentication**
	Physical Access	**Logical Access: Local Workstation Environment**	**Logical Access: Remote or Network System**	**Mechanism for Logical Access**
100 (None) Corresponds to: • NIST/OMB Level 1 • FBCA Rudimentary Level	No special access requirements	No special access requirements	No access to secure content, only access to public content	Password.
200 (Low) Corresponds to: • NIST/OMB Level 2 • FBCA Basic Level • PIV Some	• Visual • Card Holder Unique Identifier (CHUID)	CHUID	PIV Card PKI Certificate	Strong password (see SP 800-63 Section 8.2.2.4 for details).

Table II. Authentication Mechanisms for Physical and Logical Access				
Assurance Level	**FIPS 201-1 Mechanisms for use with PIV Card**			**E-Authentication**
	Physical Access	**Logical Access: Local Workstation Environment**	**Logical Access: Remote or Network System**	**Mechanism for Logical Access**
300 (Moderate) Corresponds to: • NIST/OMB Level 3 • FBCA Medium Level • PIV High Confidence	Unattended biometric	Unattended biometric		Two-factors: 1. Password or biometric required to activate token. 2. Soft token/hard token validated to FIPS 140-2 level 1 or higher, or one-time password device token validated to FIPS 140-2 level 1 or higher.
400 (High) Corresponds to: • NIST/OMB Level 4 • FBCA Medium (Hardware) or High Level • PIV Very High Confidence	• Attended biometric • PIV Card PKI Certificate	• Attended biometric • PIV Card PKI Certificate	PIV Card PKI Certificate	Hard token validated to FIPS 140-2 level 2 or higher which requires level 2 operator authentication (role-based) for two factors.

3. Related ITPs/Other References

- Federal Information Processing Standard (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems, February 2004
- Office of Management and Budget's (OMB) E-Authentication Guidance for Federal Agencies, M-04-04 [OMB 04-04], 12/16/2003.
- National Institute of Standards and Technology (NIST) Special Publication 800-63, Electronic Authentication Guideline, April 2006.
- FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.
- NIST Special Publication (SP) 800-30 Risk Management Guide for Information Technology Systems, July 2002.
- X.509 Certificate Policy for the Federal Bridge Certification Authority, September 2002.
- FIPS 140-2 Non-Proprietary Security Policy, June 23, 2004.

- Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers (NFI), Federal CIO Council, May 2009

4. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

5. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	1/18/2008	Base Policy
Revision	9/25/2009	Refreshed Document
	4/2/2014	ITP Reformat