

IAB Agenda

- **Opening Remarks** (*Tim Baldrige, NASA*)
- **Credentialing Interoperability in DHS Programs** (*Tom Lockwood, DHS*)
- **Backend Attribute Exchange** (*Chris Loudon*)
- **Results of Winter Blast Exercise** (*Craig Wilson, DHS/FEMA*)
- **Status of NASA HSPD-12 Implementation** (*Tim Baldrige, NASA*)
- **TWIC Update** (*Maurine Fanguy, TWIC PM*)
- **SP 800-116 Strategy for use of PIV Credentials in PACS** (*Bill Macgregor, NIST*)
- **Closing Remarks** (*Tim Baldrige, NASA*)



Access-Based / Privilege-Based Credentialing Programs

Creating an Interoperable Credentialing Framework



Daily DHS Screening Opportunities

- **Process 1.2 million inbound travelers at POEs - 630,000 aliens**
- **Screen over 1.9 million domestic air travelers**
- **Conduct 135,000 biometric checks for visa applicants and border crossing**
- **Process nearly 30,000 immigration benefit applications**
- **Verify the employment status of 3.2 million new employees in the U.S. for approximately 121,000 employers**
- **Based on statutory authority, execute background checks for critical infrastructure workers (Hazmat, TWIC, chemical sector)**
- **Continuously vet nearly 400,000 participants in Trusted Traveler Programs and process over 600 enrollment applications**



Core Problem Areas Identified in 2006 & Strategic Objectives

Core Problem Areas

- Inefficient information and data collection. DHS often requires individuals to provide the same information, including biometrics, it has already collected;
- Multiple credentials issued. DHS issues new credentials to the same individuals rather than associating multiple licenses, privileges, or status with a single credential. Credentials are not all securely issued nor do they all include tamper-resistant features;
- Inconsistent vetting processes for like programs and re-vetting of the same individuals; and
- Reliance on visual inspection. DHS often relies on “visual verification” of a credential to establish identity and the associated license, privilege, or status, rather than electronic verification.

Resulting Strategic Objectives

- Design credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used;
- Design enrollment platforms and data collection investments so that they can be reused by other DHS programs where appropriate – establishing a preference for “enroll once, use many” environment;
- Vetting, associated with like uses and like risks, should be the same;
- Entitlement to a license, privilege, or status should be verified using technology;
- Immigration status determinations by DHS components should be verified electronically; and
- Ensure opportunities for redress – individuals should be able correct information held about them.

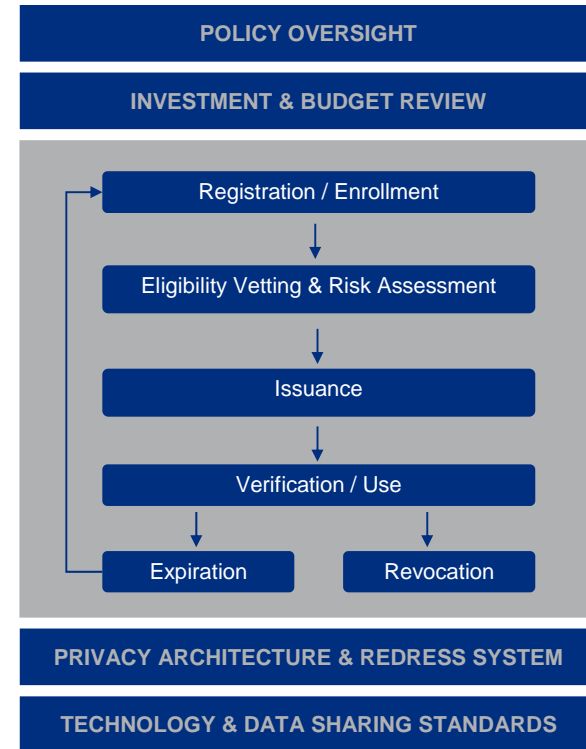
Consistent with mission, business need, legal authorities and privacy considerations



Credentialing Principles

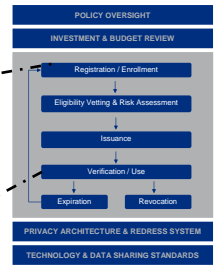
The following principles are designed to guide future development.

- Design credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used
- Vetting, associated with like uses and like risks, should be the same
- Immigration status determinations by DHS components should be verified electronically
- Entitlement to a license, privilege, or status should be verified using technology
- Design enrollment platforms and data collection investments so that they can be reused by other DHS programs – establishing a preference for “enroll once, use many” environment
- Ensure opportunities for redress – individuals should be able to correct information held about them





Credential Framework



		REGISTRATION AND ENROLLMENT	ELIGIBILITY VETTING AND RISK ASSESSMENT	ISSUANCE	VERIFICATION AND USE	EXPIRATION AND REVOCATION	REDRESS / WAIVER
CAPABILITIES	Government		Terrorism and broad scope criminality, immigration, identity, etc.	Physical credential, detailed security / verification features, developed to widely used specification (e.g. FIPS 201 or ICAO)	High level assurance of identify, authenticity and status validity	Match against central records	Intake
			Terrorism and limited scope criminality, immigration, identity, etc.				Determination of misidentification
	Regulated			Physical credential, detailed security / verification features, developed to limited use specifications	Authenticity and status validity emphasis, lower level or no identity verification	Match against distributed records	Determination of Waivability
			Terrorism nexus only	Physical credential with minimal security / verification features or process without physical credential			Availability of misidentification / waiver decision for reuse by other screeners
	Guidelines					One time use credential	
				Sponsor approved			
TREND ANALYTICS							



Current Over-Arching Efforts

- Credentialing Framework Initiative (CFI)
 - Business Process and Functionality Vision
 - Cohesive capability framework across the credentialing lifecycle
 - Information Technology / Enterprise Architecture Assessment
 - Identifies the relationships between the credentialing processes, the business capabilities, and the IT services that support them
 - Transition Plan
 - Identifies a prioritized set of recommended suites that will be implemented to meet the capabilities identified in the Credentialing Capabilities Framework
- HLS Enterprise Architecture Strategic Efforts
 - Analysis of enterprise services
 - Inclusive of Enterprise Perspectives & Efforts (leveraging CIO strategic framework)
 - Enterprise Architecture (EA Committee – Lee Smith)
 - Enterprise Data Model (EDMO Committee -- Donna Roy)
 - Mature Core Centers of Capabilities & Department Investments
 - IDENT (Biometric), TECS (Biographic), E-Verify (Employment Eligibility, SSN), SSOLV (SSN), SAVE (Immigration Status)
- Policy to support Physical and Logical Security Applications – Routine & Incident
 - Create an authoritative source for baseline-standard of DHS credential physical features and core data elements
 - Develop Private Sector Screening Guidelines to support CI/KR/HSPD-11





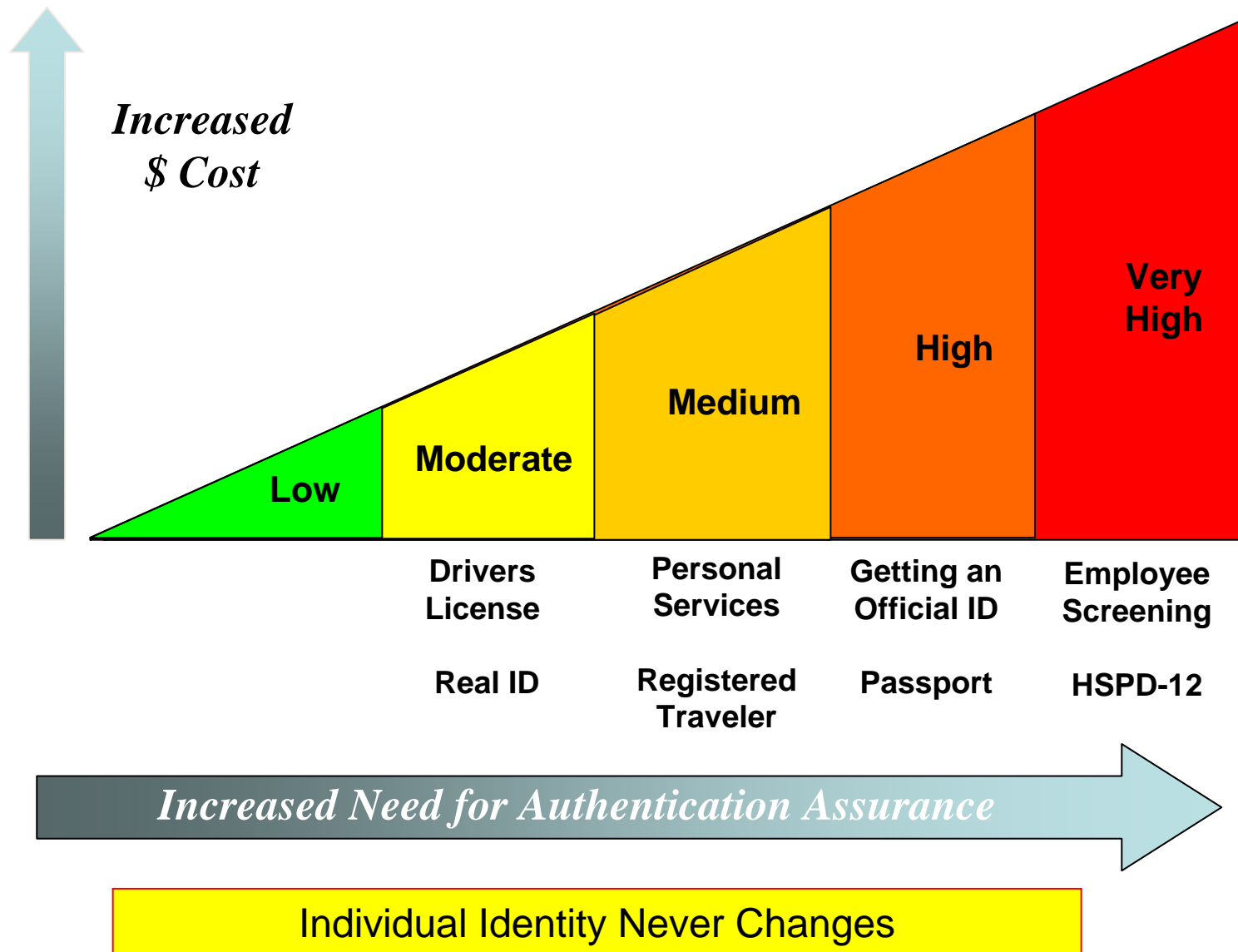
Trust Network & Interoperability

Vision of FIPS-201 - A scalable “Gold Standard” —

- Enhances common standards, guidelines, and capabilities that reduce fraud, prevent terrorism, improve the reliability, accuracy, and use of public and privately issued licenses and identification cards.
 - Makes it harder for someone to obtain these documents fraudulently and easier to detect documents that have been falsified.
 - Fosters verification of source document, including the inspection and/or authentication of the integrity of the source document and electronic verification of the identity information contained on the source document whenever possible.
 - Addresses privacy concerns and protections for personal identifying information through the accountability of public and private sectors to the federal, state, and local democratic processes.
- Technology and processes provide a strong-framework that is scaleable and applicable to diverse business process and applications – facilitating wider adoption of secure identity capabilities and diverse technologies
- Reduce costs for technology / capability adoption through open standards and shared-service models.

Technology & Process best practices for: Registration/Enrollment; Eligibility/Vetting & Risk Assessment; Issuance; Verification/Use; and Revocation

Authentication Cost / Risk / Benefit Analysis



FIPS-201 Interoperable Programs

Program	Description	Estimated Population	Regulation	Sponsor Organizations	Implementation Deadline
HSPD-12 <ul style="list-style-type: none"> • GSA-MSO-PIV • DHS-PIV • AG-PIV • IC Blue Card 	Executive branch "mandatory, standard for secure and reliable form of identification issued for its employees and contractors that: <ul style="list-style-type: none"> – issued based on sound criteria for verifying an individual employee's identity; – is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; - can be rapidly authenticated electronically; - is issued only by providers whose reliability is established by an official accreditation process 	2-4 Million	HSPD-12	Individual Federal Departments, Agencies, Offices, and Commissions	<ul style="list-style-type: none"> • Oct 27, 2007-- all current employees / contractors • Oct 27, -- all Federal department or agency employees employed over 15 years
Transportation Worker Identification Credential (TWIC)	Congress directed the federal government to issue a biometric transportation security credential to any individual with unescorted access to secure areas of facilities and vessels and all mariners holding Coast Guard issued credentials or qualification documents.	1-1.5 Million	Maritime Transportation Security Act of 2002	TSA & U.S. Coast Guard	<ul style="list-style-type: none"> • Sept 25, 2008
First Responder Authentication Credential (FRAC)	FRAC real-time capabilities to electronically validate the identity and attributes (qualification, certification, authorization, and/or privilege) of emergency response/critical government personnel responding to all-hazards events. Public and private sector emergency response support/critical personnel.	2-4 Million Law Enforcement 40-60 million all NIMS / NIPP sectors	9-11 After-action HR-1	FEMA Facilitates Issued by Public & Private Sector jurisdictions or organizations	<ul style="list-style-type: none"> • Final Standards to be completed by Sept 08 IAW 911 Act of 2007
Common Access Card (CAC)	All uniformed services personnel in the Department of Defense will be issued a Common Access Card (CAC) which replaces previous generation identification used by DoD. https://www.cac.mil/Home.do - DHS-USCG	4.3 Million Uniformed	HSPD-12	Department of Defense	<ul style="list-style-type: none"> • Oct 27, – all current employees / contractors • Oct 27, 2008– all Federal Dpt. or Agency employees employed over 15 yrs
Aviation Credential Interoperability Solution (ACIS)	ACIS was established to address physical access concerns at the nation's airports and establishes universal standards for aviation credentials; supports a single, interoperable identification for all airport personnel.	2-4 Million	49 CFR Subchapter C	TSA Regulates Issued by Private Sector organizations	TBD

Program	Criminal History	Terrorism	Legal Status	Required/Eligible Population
TWIC	10-fingerprint-based FBI Check (IAFIS). Disqualifiers are either permanent or interim (convictions within seven years or incarceration within 5 years of application) Criminal disqualifiers are based on: 49CFR§ 1572.103	Vetted through TSA Screening gateway and based on match of name, DOB, POB, and Gender weighted independently 49CFR§ 1572.107	Technology-based and visual authentication of Documents at enrollment, 10-Print IDENT, Name check against DACS via the Screening Gateway 49CFR§ 1572.105	Any individual with unescorted access to secure areas of facilities and vessels and all mariners holding Coast Guard issued credentials or qualification documents. Applicants sign TWIC Disclosure Form to certify above requirements.
HAZMAT	Same as TWIC 49CFR§ 1572.103	Same as TWIC 49CFR§ 1572.107	IDENT query and name check through SAVE program. 49CFR§ 1572.105	All drivers who seek to obtain, renew, or transfer an HME on their CDL. Must have a valid CDL to apply and include CDL, current HME, and employer information on application. 49CFR§ 1572.9
ACIS-SIDA II	Fingerprint-based FBI Check (IAFIS), Disqualifiers for convictions within 10 years are based on: 49 CFR § 1542.209:	Vetted through TSA Screening gateway and based on match of name, DOB, POB, and Gender weighted independently	Visual authentication of documents by trusted agent at enrollment, 10-Print IDENT, Name check through SAVE via the Screening Gateway,	All airport and airline employees requiring access to SIDA and Secure area of airports. Applicant information and fingerprints collected by accredited Airlines and Airports
DHSPIV	10 fingerprint-based FBI check, via IDENT Minimum suitability determinations include National Agency Check plus personal inquires to law enforcement, credit, employment and education, and reference. Reciprocal suitability/clearance determination throughout Executive branch. Criteria for suitability are based on: 5 CFR §731. 202	National Agency Check; Fingerprints transmitted to and enrolled in IDENT to perform a biometric watchlist check. Recurrent IDENT checks are performed.	Application for National Agency Check is processed through OPM, who checks SAVE. Fingerprints transmitted and enrolled in IDENT.	All DHS employees and contractors and new hires who have accepted a tentative offer of employment. Adjudications from other Executive Branches accepted for similar risk/sensitivity levels.
GSA MSOPIV	10 fingerprint-based FBI check, suitability determinations include National Agency Check plus personal inquires to law enforcement, credit, employment and education, and reference. Criteria for suitability are based on: 5 CFR §731. 202V	Same as DHS PIV	Same as DHS PIV	Federal employees, contractors, and volunteers who require routine, long-term access to Federal facilities, IT systems, and networks. Individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.). Discretion to include short-term (working in a Federal facility for less than six months) and employees and contractors in the PIV Program
DoD CAC	10 fingerprint-based FBI check, via DOD RAPIDS system, suitability determinations include National Agency Check plus personal inquires to law enforcement, credit, employment and education, and reference. Criteria for suitability are based on: 5 CFR §731. 202V	Same as DHS PIV	Same as DHS PIV	All Military and Civilian employees and DoD contractors with recurring access to DoD facilities and/or IT systems.
FRAC		Same as DHS PIV		

Technology Characteristics

	Common & Unique Reader Requirement	Use Case	Reader Interface Preference Reader Applications	Interoperability Test
GSA MOS HSPD-12	<ul style="list-style-type: none"> FIPS 201 	PIV Bio Metric VIS – Manual Electronic – CHUID PKI BIO A	Primarily Contact Fixed and Mobil Physical and Logical Access Reader	Commonality of core test Data Object
DHS HSPD-12 PIV Card	<ul style="list-style-type: none"> FIPS 201 Unique Identifiers <ul style="list-style-type: none"> - ??? Armed Leo & - ??? COOP/COG 	PIV Bio Metric VIS – Manual Electronic – CHUID PKI BIO A	Primarily Contact Fixed and Mobil Physical and Logical Access Reader	Commonality of core test PM Specific / Modular Interoperability Test
Transportation Worker Identification Credential TWIC	<ul style="list-style-type: none"> FIPS 201 TWIC Privacy Key 	TPK Bio Authentication VIS – Manual PKI	Contactless preferred Fixed and Mobil Physical and Logical Access Reader	Commonality of core test PM Specific / Modular Interoperability Test
First Responder Authentication Credential FRAC	<ul style="list-style-type: none"> FIPS 201 2D bar code on a machine readable zone of a drivers license <p>(note: majority of states using 2D bar code- a limited number of states still using mag-strip)</p>	PIV Bio Metric VIS – Manual PKI	Contact & Contactless Mobil Reader (Hand-Held)	Commonality of core test PM Specific / Modular Interoperability Test (attribute object)
Common Access Card CAC	<ul style="list-style-type: none"> FIPS 201 	PIV Bio Metric VIS – Manual Electronic – CHUID PKI BIO A	Contact & Contactless Fixed and Mobil Physical and Logical Access Reader	Commonality of core test
Aviation Credential Interoperability Solution ACIS	<ul style="list-style-type: none"> FIPS 201 	PIV Bio Metric Use Case Fixed and Mobil Physical and Logical Access Reader	Contact & Contactless	Commonality of core test



Being Interoperable with FIPS 201

1. **Non-Federal entities** can produce a physical credential that is **technically interoperable** with the Federal Personal Identity Verification Card (PIV) defined by FIPS 201 and related Special Publications. Interoperability and acceptance relies on several additional factors:
 - a. Implementation of an **identity authentication certificate (comparable to PIV Authentication)** that meets Federal requirements (additional certificates are optional)
 - b. Development of a **Smart Card Number (comparable to FASC-N)** that follows a set guideline to ensure uniqueness
 - c. **Compatibility of the data model** for the card with the Federal PIV data model
2. The PKI credential issuing organization must participate in the trust infrastructure known as the **Federal Bridge Certification Authority (FBCA)** at the **medium hardware level of assurance**.
3. Credential issued must satisfactorily pass the **electronic personalization requirements of the NIST test tool**.



Priority Deployments Strategy

Community Utility & Use

▶ Public Health & Medical

- ▶ Emergency Support for the Advanced Registration of Volunteer Health Professionals (ESAR-VHP)
- ▶ Patient tracking
- ▶ Family Reunification

▶ Fire Fighting

- ▶ Red card triage information
- ▶ Personnel qualifications
- ▶ Asset management and tracking

▶ Transportation Community

- ▶ Maritime & Port Operations
- ▶ Aviation Terminal Operations

▶ Federal Operations

- ▶ Physical & Logical Access
- ▶ Integration
- ▶ COOP / COG

▶ Public Safety & Security

- ▶ Physical & Logical Access
- ▶ Incident Management / Crime Scene Management
- ▶ Custody of evidence & chain of trust
- ▶ Streamline suspect identification & tracking throughout the process

▶ Communications

- ▶ Physical & Logical Access
- ▶ Disaster Access
- ▶ COOP operations



Back-up Slides

Specific Programs