

Transportation Worker Identification Credential (TWIC)

Stakeholder Brief



Transportation Security Administration Credentialing Program



TWIC Program



Vision

Improve security by establishing a system-wide common credential, used across all transportation modes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system.

Goals

- Improve security
- Enhance commerce
- Protect personal privacy



Related Legislation



USA PATRIOT Act of 2001

Requires states to conduct background checks through the Attorney General and TSA before issuing licenses to individuals to transport hazardous materials in commerce.

Aviation and Transportation Security Act of 2001 (ATSA)

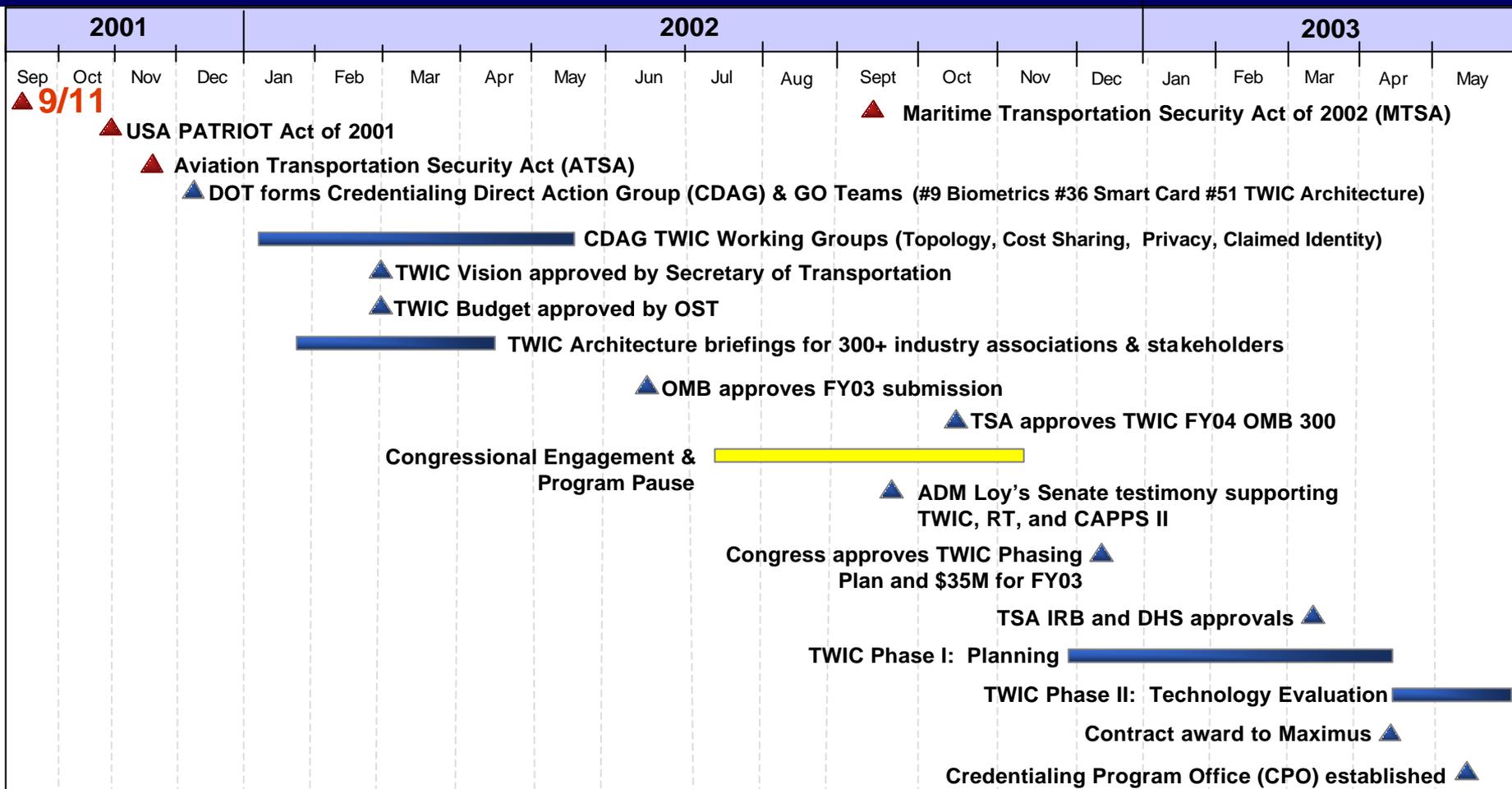
Grants the TSA Administrator broad authority for transportation security; requires TSA to ensure the adequacy of security measures at airports; directs strengthened access control points in airport secured areas; and, requires TSA to consider the use of biometric, or similar technologies, to identify individuals employed at airports.

Maritime Transportation Security Act of 2002 (MTSA)

Requires the issuance of biometric transportation security cards and the completion of background checks for entry to any secure area of a vessel or facility.



TWIC Program History



- TWIC Legislative Authority
 - USA PATRIOT, ATSA 2001, MTSA 2002
- Cabinet Level (DOT) Approval Feb 2002
- TWIC Public Meetings Jan-Apr 2002

- Congress Approved TWIC Regional Plan and \$35M for FY03
- President's FY04 Budget Includes \$55M for TWIC
- ADM Loy Strongly Supports TWIC in Testimony: "TWIC is Flagship Program"

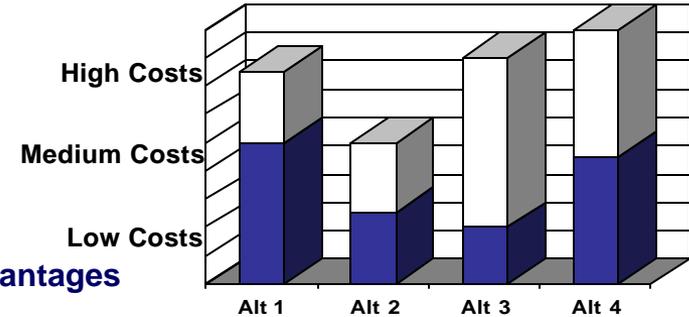


Alternatives Analysis



Conducting evaluation of Alternative 2 based on Alternatives Analysis and Balanced Scorecard results.

Total Program Cost to Nation
 Federal Share of Total Cost



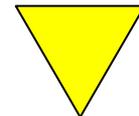
Advantages

Disadvantages

Alternative 1:
Federal Implementation and Funding

- Common infrastructure
- Matches individual with credential technology
- Centralized control of implementation

- High system replacement costs
- Public perception / privacy concerns
- Potential impact on commerce



Alternative 2:
Federally led Public / Private Partnership

- Common infrastructure
- Matches individual with credential technology
- Leverage existing systems
- Options for shared cost

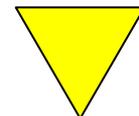
- Requires local commitment to Public / Private Partnership



Alternative 3:
Federal Requirements / Local Implementation and Funding

- Stakeholder independence
- Matches individual with credential technology
- Local acceptance

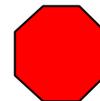
- Divergent to interoperability goal
- Requires 100% local implementation, design, and execution
- Lack of economy of scale



Alternative 4:
Federally led Public / Private Partnership with Low Tech Credential

- Lower initial costs
- Common infrastructure

- Security vulnerabilities due to low technology credential
- Higher labor costs for human sensors at checkpoints



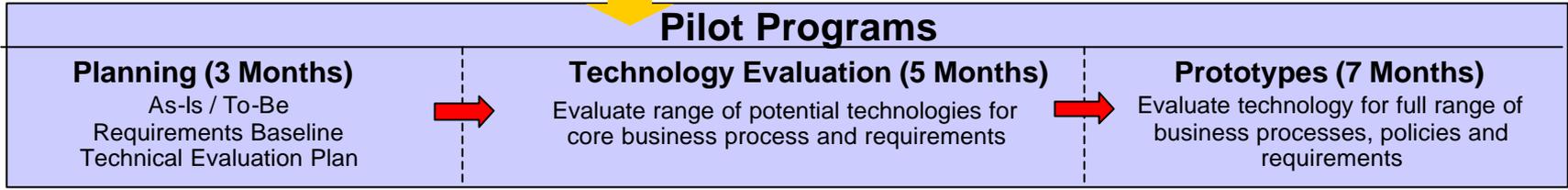


Work Streams



Today

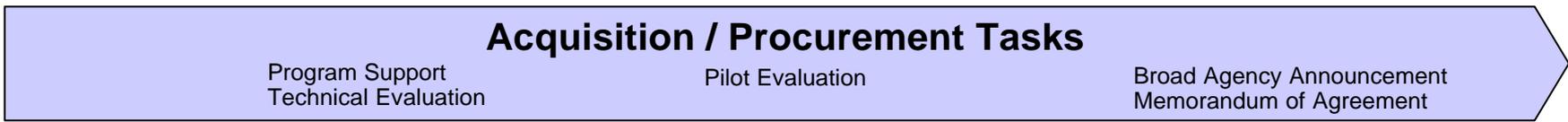
Pilot Programs



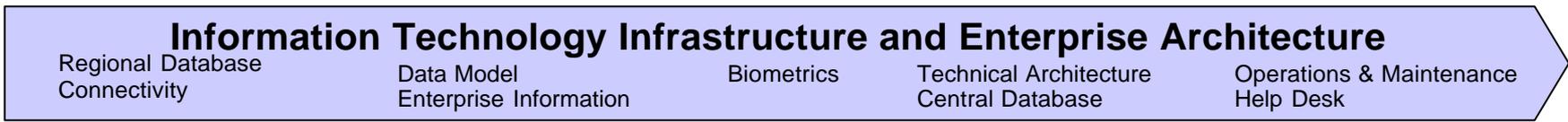
Business Case Development



Acquisition / Procurement Tasks



Information Technology Infrastructure and Enterprise Architecture



Business Policy Issues

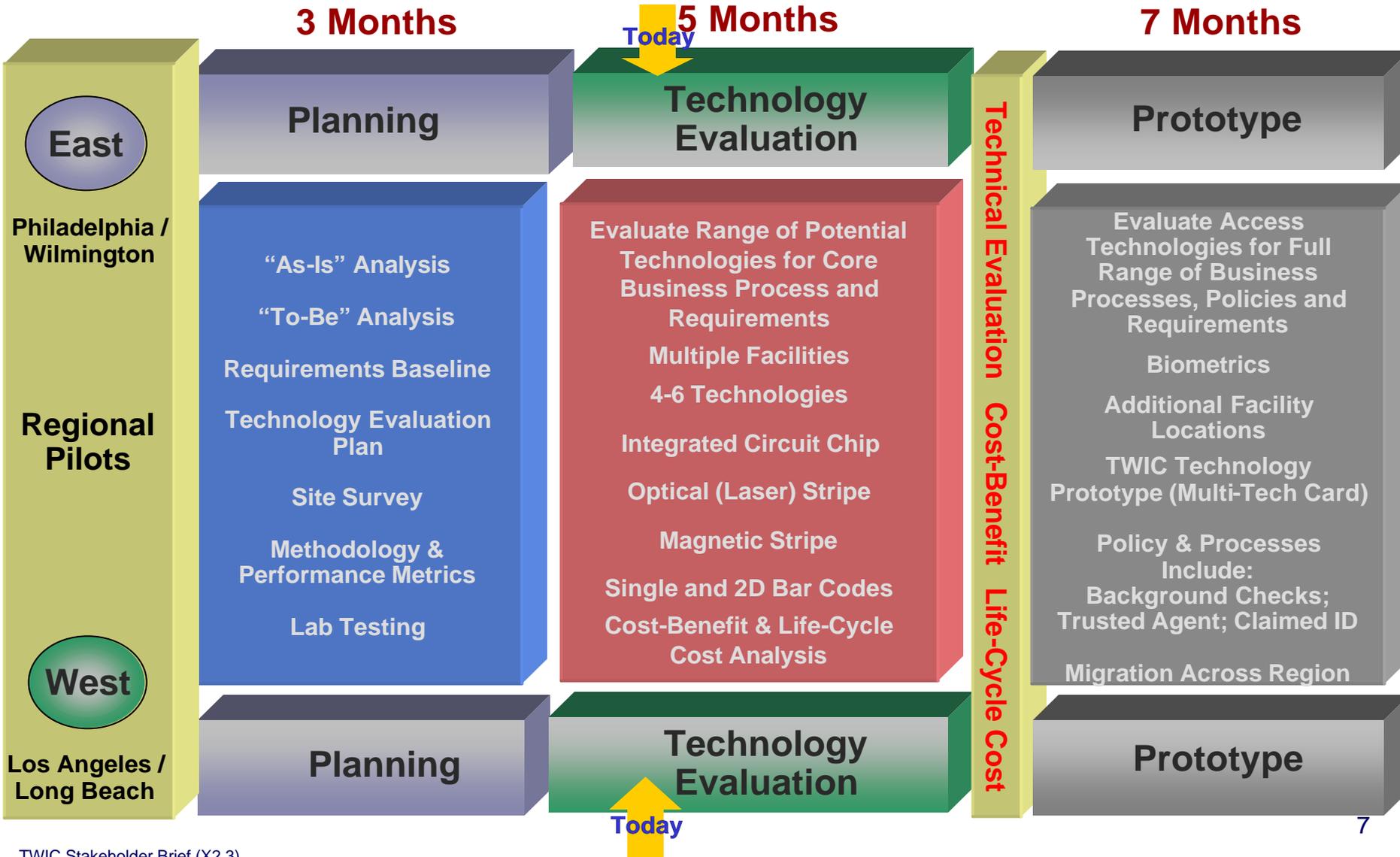


Stakeholder Engagement





Regional Pilots





Technology Evaluation Phase



Illustrative

Purpose: Evaluate multiple access control technologies for core business processes and requirements.		Maritime							HQ			Pipeline	Air			Rail		Other		
		Port of Wilmington DE	Packer Avenue Terminal PA	Penns Terminal PA	Beckett Street Terminal NJ	APL Terminal CA	LBCT Terminal CA	Crowley Marine CA	Delaware River & Bay Maritime Exch PA	Port HQ Long Beach CA	Port HQ Los Angeles CA	Conoco Phillips Oil Refinery PA	PHL Airport PA	PNE Airport PA	LAX Airport CA	CSX Facility PA	Union Pacific Rail ITCF CA	Customs House PA	ILWU Union Hall CA	Salem Nuclear Plant NJ
<input type="checkbox"/> East Coast Sites <input type="checkbox"/> West Coast Sites	Enrollment	X	X		X	X	X	X	X	X	X	X	X	X	X	X				
	Optical (Laser) Memory Stripe				X		X	X		X			X							
	ICC	X				X		X			X			X		X				
	Bar Code (2D)	X					X	X												
	Bar Code (3x9)		X					X							X					
	Magnetic Stripe							X	X			X		X						

Multiple Types of Access Control Points

- Vehicle gates
- Truck multi-lanes
- Unmanned personnel turnstiles
- Building and door access
- High volume pedestrian entrances
- SIDA

Multiple Transportation Modes

- Port, Airport, Trucking, Rail, Pipeline, and HQs

Multiple Access Control Technologies

- Smart Chip, Magnetic Stripe, Optical Media, Single and 2D Barcodes



Prototype Phase



Illustrative

Purpose: Broaden evaluation using multiple technologies over the full range of business processes and requirements.		Maritime							HQ			Pipeline		Air			Rail		Other			
		Port of Wilmington DE	Packer Avenue Terminal PA	Penns Terminal PA	Beckett Street Terminal NJ	APL Terminal CA	Maersk Terminal CA	LBCT Terminal CA	Crowley Marine CA	Delaware River & Bay Maritime Exch PA	Port HQ Long Beach CA	Port HQ Los Angeles CA	BP Refinery CA	Conoco Phillips Oil Refinery PA	PHL Airport PA	PNE Airport PA	LAX Airport CA	CSX Facility PA	Union Pacific Rail ITCF CA	Customs House PA	ILWU Union Hall CA	Salem Nuclear Plant NJ
<input type="checkbox"/>	East Coast Sites																					
<input type="checkbox"/>	West Coast Sites																					
Business Processes	TWIC Multi-Application / Multi-Technology Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Contactless	X							X	X	X			X								X
	Biometrics	X			X				X	X	X					X	X	X				X

Business Processes

- Biometrics
- Background Checks
- Claimed Identity
- Central Database
- Watch List
- Threat Data
- Liability
- Privacy
- Trusted Agent
- Topology
- Enrollment Centers

Analysis

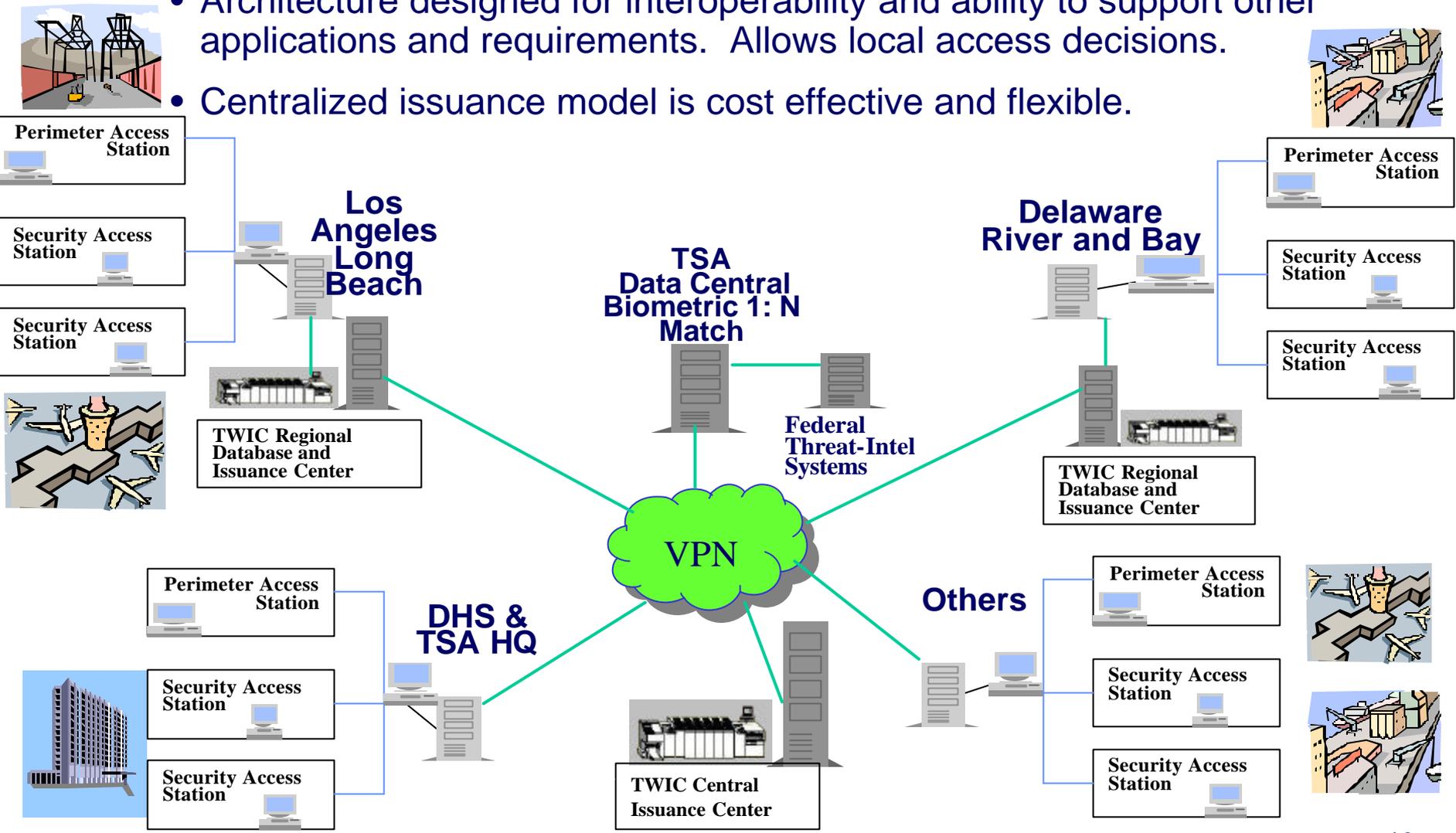
- Cost-Benefit Analysis
- Life Cycle Cost Analysis
- Technical Evaluation
- Implementation Options



Pilot System Architecture



- Architecture designed for interoperability and ability to support other applications and requirements. Allows local access decisions.
- Centralized issuance model is cost effective and flexible.





System Attributes



- Positive match of credential – person - background check - access level through the use of a secure reference biometric
- Business and Standards based approach and flexible solution architecture enables TWIC System to support multiple users, requirements and applications
 - Government Smart Card Interoperability Specification (GSC-IS) provides broad interoperability
 - Open architecture and multiple technologies support leveraged investments
 - TWIC is a tool that enables business process improvements and E-Gov
 - Capable of meeting needs across DHS
- Centralized ability to interface with other federal agencies and databases for “watch list”, threat and intelligence information
- Secure record control and network of databases, provides capability to disseminate “threat alerts,” revoke security access system-wide for specific individuals, hot-list, or deal with lost-stolen cards
- Reduces risk of fraudulent / altered credentials through use of state-of-the-art anti-tamper and anti-counterfeit technologies



Beyond the Scope of TWIC



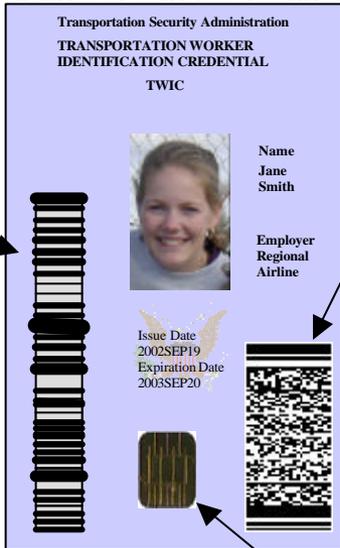
- **Possession of a TWIC does not automatically grant the holder access to secure areas.**
 - Only facilities grant access. Facilities have complete control over who is granted access to secure areas, and what level of access is granted.
- **The TWIC program will not develop site-specific secure area definitions.**
 - The TWIC regulations will point to the definitions of “secure areas” as determined in national security plans, regulations or by statute.
- **The TWIC program does not prevent facilities from specifying additional access requirements.**
 - Facilities may require background investigations, access procedures, or credentials beyond those provided by TWIC.



Card Architecture



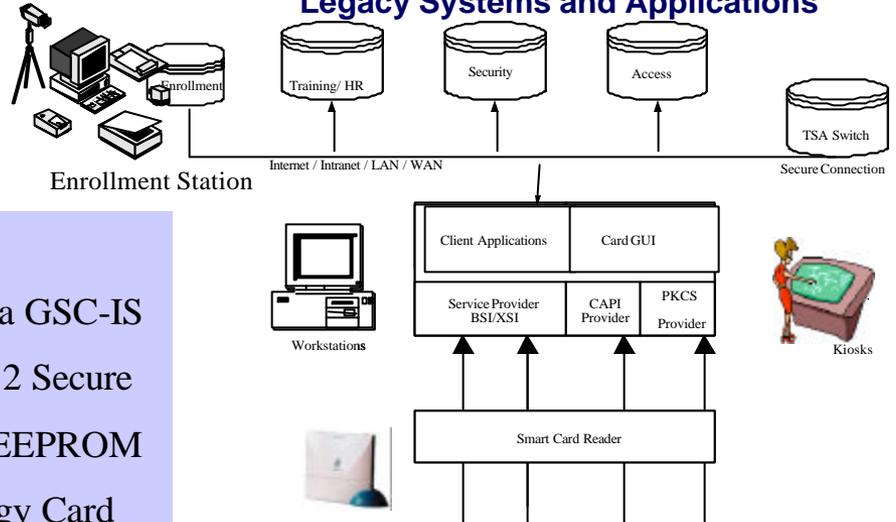
Illustrative of Surface Technologies



2D Bar Code

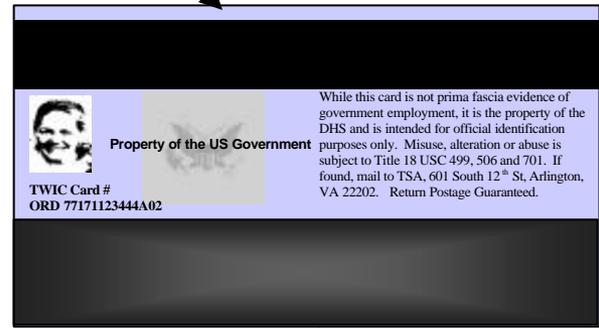
- ISO Standards
- Interoperable via GSC-IS
- FIPS 140 Level 2 Secure
- JAVA 32-64K EEPROM
- Multi-Technology Card
- PKI
- Multiple Biometrics
- Contactless

Legacy Systems and Applications

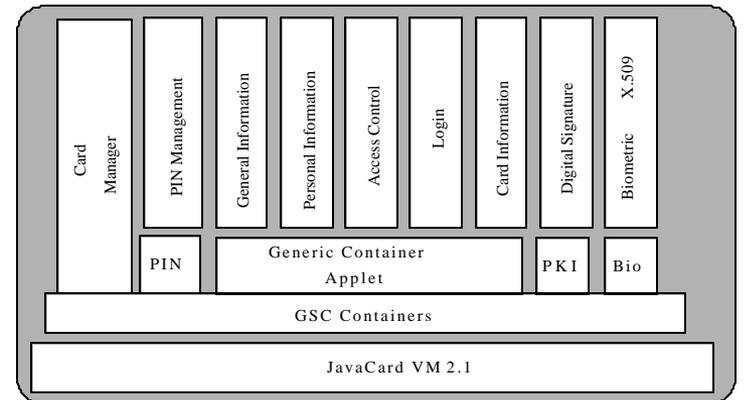


Magnetic Stripe

ICC Chip



Optical (Laser) Media Stripe





Business Policy Issues



- **Claimed Identification**

- “Breeder” documents
- Identity verification

- **Trusted Agent**

- TSA-certified enrollment sources
- Federal, state, private

- **Enrollment / Card Issuance**

- Enrollment process / sites
- Card production facilities

- **Background Checks / Investigations**

- Multiple levels
- Disqualifying offenses
- Confidentiality
- Adjudication / appeals / waivers

- **Biometrics**

- Selection of biometric

Card Topology

- Security features
- Card technologies
- Appearance

- **Regulations**

- Determine if regulations are required, if so
- Drafting and issuance of full-implementation regulations

- **Cost Sharing**

- Authorizing legislation
- Credential cost
- Collection process

- **Liability**

- Government liability for security breaches

- **Privacy**

- Protections



Privacy Considerations



Guiding Principles

- **Minimum Data:** Collect and retain only data that is absolutely necessary
- **Limit Use:** Use the data only for the purpose for which it was collected
- **Data Quality:** Data maintained is accurate, complete, current, and relevant
- **Data Security:** Secure and protect from unauthorized use (physical and cyber)
- **Accountability:** Internal controls to sustain the privacy of individual information

Actions to Date

- Created Privacy Workgroup
- Developed Privacy Impact Assessment as part of combined TWIC/Registered Traveler (RT) Program OMB Exhibit 300 submission
- Issued Government Paperwork Reduction Act 60-day notice to Federal Register on June 24, 2003
- Issued TWIC Privacy Act System of Record Notice—now pending DHS review/approval
- Briefed DHS Chief Privacy Officer on TWIC Program July 10, 2003



Conclusion



TWIC Program Benefits

Improves Security

- Reduced risk of fraudulent or altered credentials
- Biometrics used for secure, positive match of individual to authorized access level and clearances
- Ability to interface and communicate with other federal, local, and state agencies
- Ability to disseminate “threat alerts” throughout a nationally integrated system

Protects Individual Privacy

- Collection of minimum data elements
- Secure record control system and network
- Employs advanced information technology to protect personal information
- System-wide encryption implementation

Enhances Commerce

- Increases process speed and efficiency
- Enables improved management and utilization of resources
- Expanded e-government potential
- Public – private partnership
- Economies of scale purchasing
- Eliminates need for redundant credentials and background investigations
- Potential to reduce industry insurance costs
- Leverages current security investment and legacy systems