# Using the Prototype TWIC for Access

## *A System Integrator Perspective*

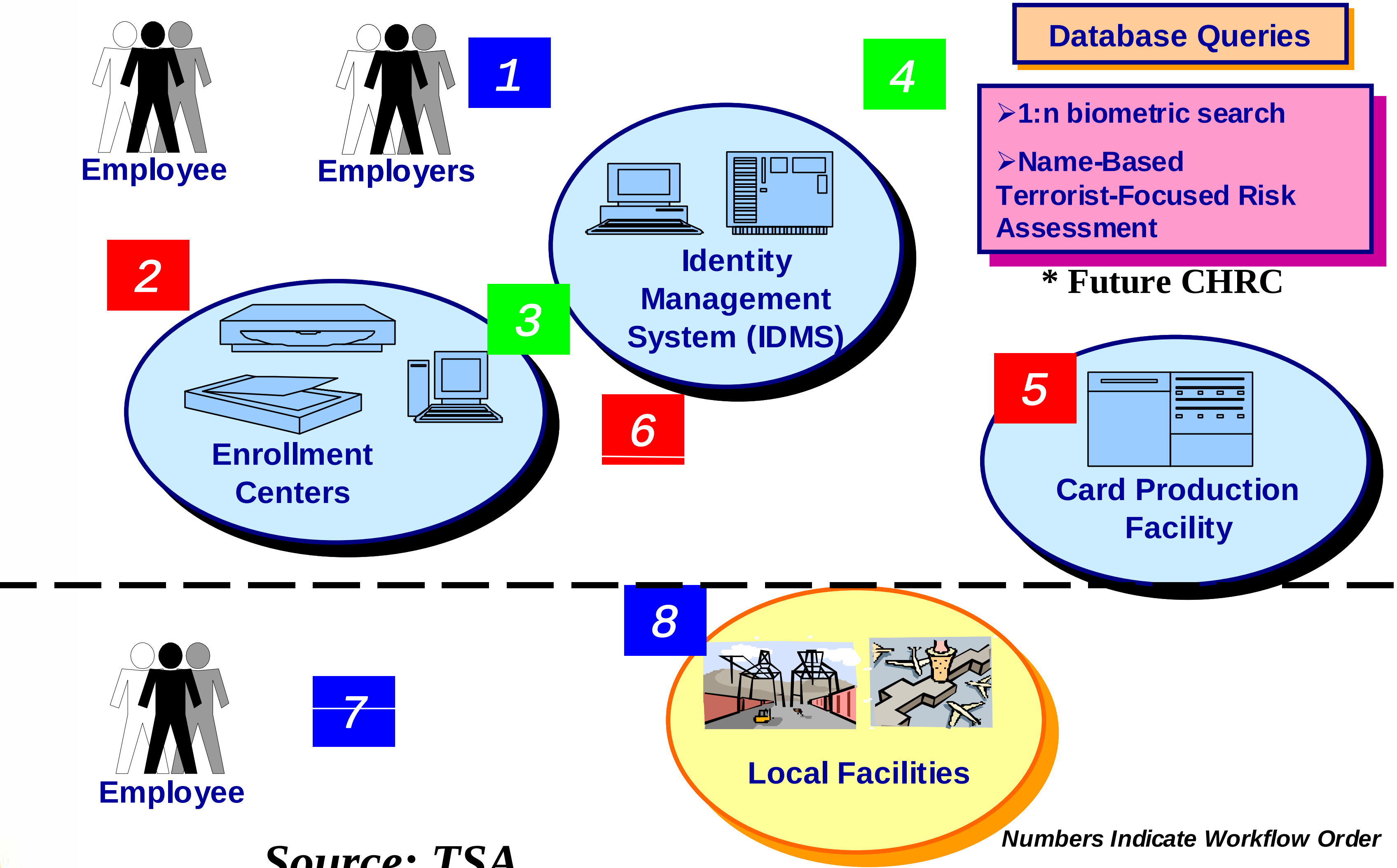
AAPA Port Security Seminar and Exhibition, Seattle, WA

July 19, 2006

# The Challenge

***How do I manage "below the line?"***

## TWIC Process



Database Queries

- 1:n biometric search
- Name-Based Terrorist-Focused Risk Assessment

* Future CHRC

*Numbers Indicate Workflow Order*

***Source: TSA***

# Key Takeaways

**TWIC prototype system provides extensive capabilities to:**

- Verify TWIC as genuine
- Ensure TWIC belongs to individual presenting
- Check the status of the card (e.g. active/in use or suspended/revoked)

**Many tools are available for port security / facility administrators to manage access control**

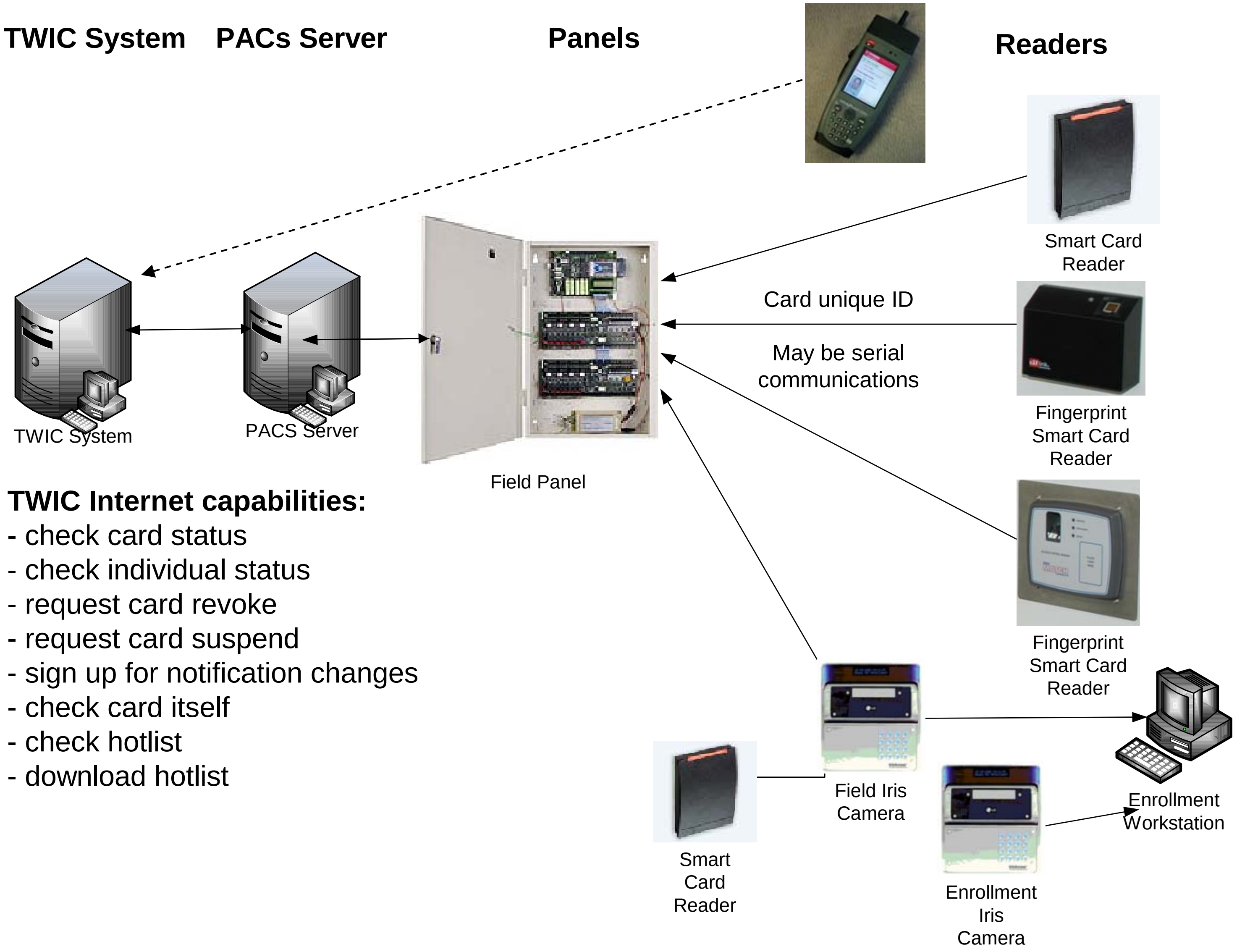
- Online tools
- Offline tools

**As with all credentials, there are risks in using TWICs for access control that must be understood and mitigated**

- Front-end
- Back-end

# A Crash Course

## *How do Physical Access Control Systems Work?*



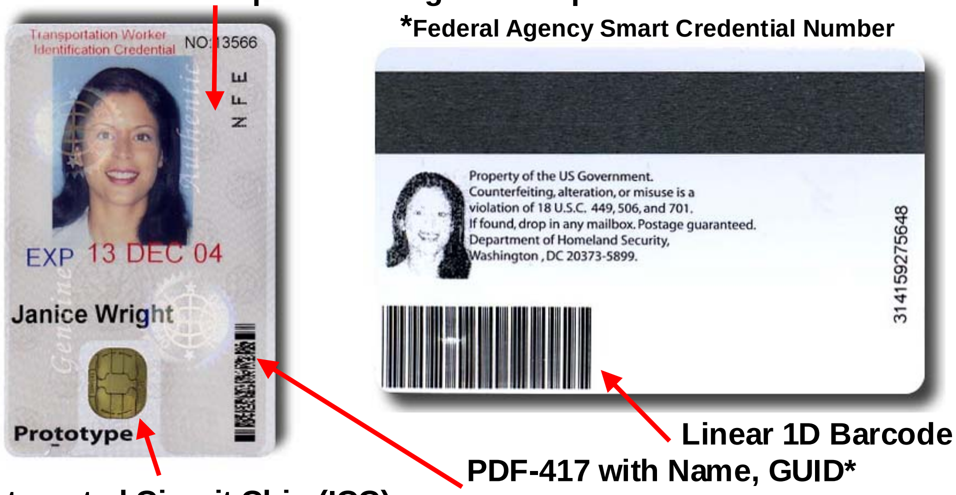
**TWIC Internet capabilities:**

- check card status
- check individual status
- request card revoke
- request card suspend
- sign up for notification changes
- check card itself
- check hotlist
- download hotlist

# Key Questions for when an individual presents their TWIC

Local sites could be presented with TWICS by people they may not know…key questions to answer:

- Is it a real TWIC?
- Is it their TWIC?
- Is it a TWIC in good standing?
- Does that person have a need to access my facility or facilities?
  - If so, which areas and when?
- How often do I want to have these questions answered for this individual, group of individuals or all of my workers?
  - First time they show up
  - Every time they show up
  - Daily, Monthly, Annually
  - Etc.



Transportation Worker Identification Credential
NO: 3566
N F E
EXP 13 DEC 04
Janice Wright
Prototype
Property of the US Government.
Counterfeiting, alteration, or misuse is a violation of 18 U.S.C. 449, 506, and 701.
If found, drop in any mailbox. Postage guaranteed.
Department of Homeland Security, Washington , DC 20373-5899.
314159275648

Contactless Chip

Magnetic stripe with FASC-N*

*Federal Agency Smart Credential Number

Linear 1D Barcode

PDF-417 with Name, GUID*

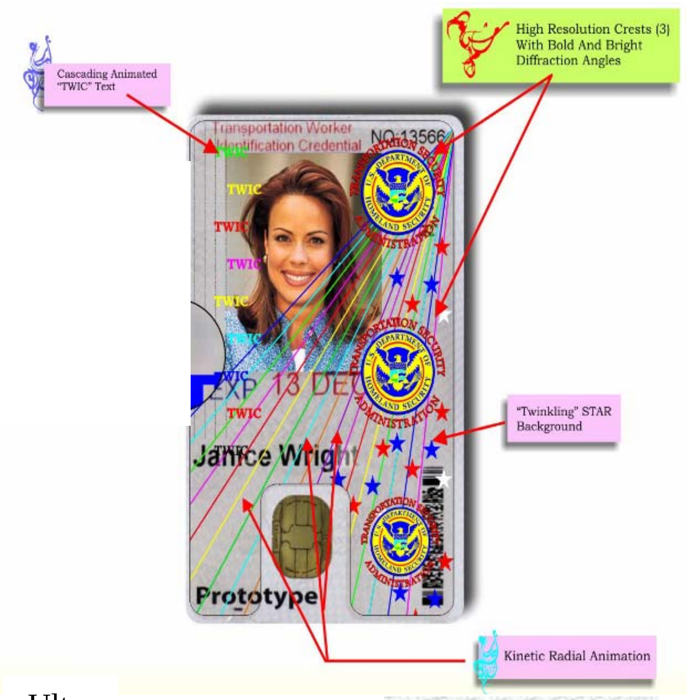
*Global Unique ID

Integrated Circuit Chip (ICC)

# Is it a real TWIC?

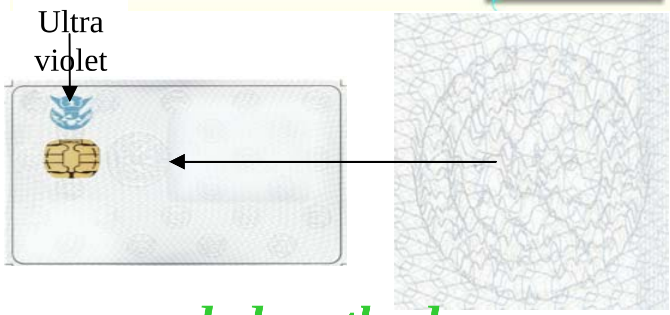
There are several methods of verifying the TWIC is real – these include:

- Magstripe
- Physical / topographical security features
- Barcode / 2D barcode
- Mutual or External Authentication (secret handshake)
- Issuer digital signature
- Digitally signed information on chip(s)


Cascading Animated "TWIC" Text
High Resolution Crests (3) With Bold And Bright Diffraction Angles
Transportation Worker Identification Credential
NO 13566
TWIC
EXP 13 DEC
Janice Wright
Prototype
"Twinkling" STAR Background
Kinetic Radial Animation

Good news is that all of these can be done offline

Bad news is that there are time trade-offs to some of these; I.e. you may not want to do them on every access event

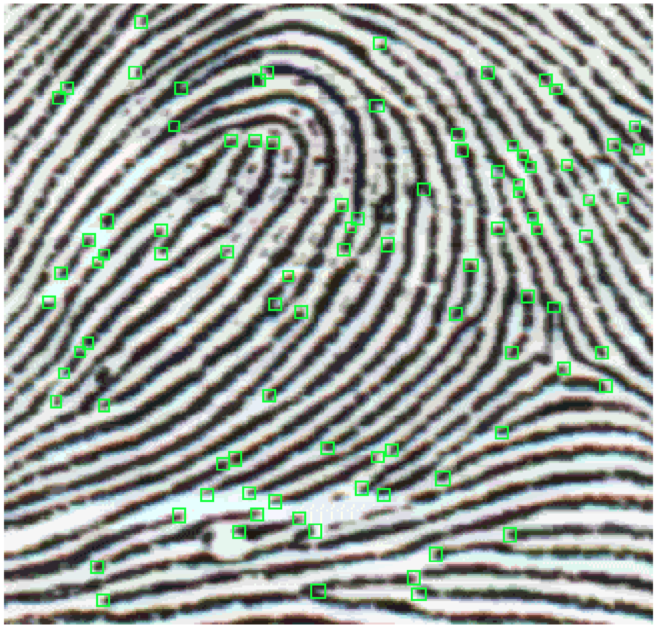


*Note: items in green are the preferred/recommended methods*

# Is it their TWIC?

There are several methods of verifying the TWIC belongs to the individual presenting it – these include:

- Visual verification of photo
  - Vs. printed on the card
  - Vs. stored and digitally signed on the chip
- PIN verification
- Facial biometric match
- Fingerprint biometric match
- Iris biometric match (local / operational)
- Hand geometry biometric match (local / operational)



Good news is that all of these can be done offline

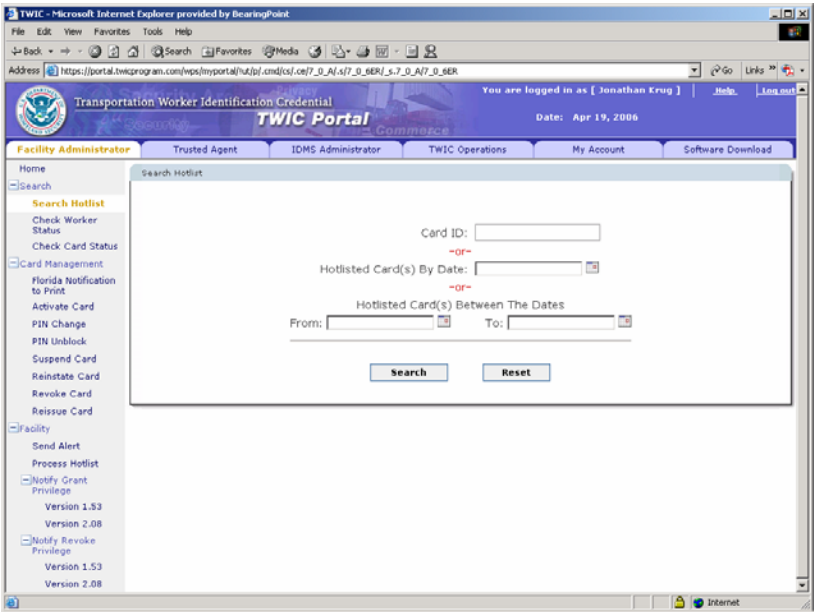
Bad news is that there are time trade-offs to some of these

*Note: items in green are the preferred/recommended methods*

# Is it a TWIC in good standing?

There are several methods of verifying the TWIC is in good standing – these include:

- Visual verification of expiration date
- Web-based check of the card status
- Notification registration
- Certificate Revocation List download
- Hot List download
- Physical Access Control System verification



TWIC - Microsoft Internet Explorer provided by BearingPoint

Address: https://portal.twicprogram.com/wps/myportal/!ut/p/.cmd/cs/.ce/7_0_A/.s/7_0_6ER/_s.7_0_A/7_0_6ER

Transportation Worker Identification Credential
TWIC Portal

You are logged in as [ Jonathan Krug ]

Date: Apr 19, 2006

Search Hotlist

Card ID:

-or-

Hotlisted Card(s) By Date:

-or-

Hotlisted Card(s) Between The Dates

From: To:

Good news is that many of these can be done offline

Bad news is that there need to be periodic updates of these bad-card lists

*Note: items in green are the preferred/recommended methods*

# Does that person have a need to access my facility?

This is a key decision that is expected to be made on a local (i.e. port/facility) basis:

- This typically involves enrollment or treatment of the TWIC as a badge in the site's local Physical Access Control System
- This may involve assignment to specific groups that govern specific location / reader access privileges as well as time / day restrictions (PACS)
- Automated tools can be made available such that this information doesn't have to be entered by hand (i.e, can be read from the TWIC and input into local PACS system)
- There are some groups that sites may want to not enroll in their local PACS (e.g., long haul truckers); different tools can be used for these groups

BearingPoint

# How often do I want to have these questions answered for this individual or group?

This is one area of risk that must be addressed:

- Full updates of hotlists / certificate revocation lists will likely be updated within TWIC on a daily / 24-hour basis; online checks will be available in real time
- The approach taken should be consistent with the site security plan along with the current threat/marsec level
- One approach is to strongly address all questions initially (I.e., one time), then enroll the individual locally; some checks (e.g. biometric) will then be conducted at each card read; others (e.g. revocation lists) may be less frequent
- Applications / readers are available to conduct all types of checks, including:
  - Card Authenticity
  - Card belongs to person
  - Card is in good standing

# What other areas of risk should I think about?

## Other areas of risk:

### Uniqueness of TWICs presented in PACS

- All TWICs will have a unique number; it will be a long unique number
- Some legacy PACs may have a limitation on the length of this unique number that they can process, creating a uniqueness issue
- Notional (Simplified) Example: John Doe’s TWIC number is 10000001; John has been given access to the local PACs at Port Always Sail; Jane Doe’s number is 20000001; if the local PACs only reads the last 4 digits, both cards appear as “0001”; this could give Jane access under John’s number/TWIC presented
- Mitigation: check local PACs for maximum length of unique IDs accepted

### TWIC presented has been suspended or revoked and local PACS is not aware

- Mitigation: perform more frequent hotlist / CRL checks
- Register site TWIC access in TWIC system; directed messages will be received when status of card changes
- Consider fielding applications/capabilities that perform real-time credential status checks

# What other areas of risk should I think about (cont'd)?

**Other areas of risk:**

- **Individual forgets TWIC or TWIC doesn't read properly; mitigation:**
  - Perform web-based biometric match
  - Issue temporary / visitor credential; may want to have reduced access privileges
  - Have capability to troubleshoot cards and readers
- **Biometric match not working; mitigation:**
  - Employ alternate verification
  - E.g., photo, PIN, alternate biometric
  - Note: many measures taken to ensure fingerprint biometric match will function properly

# What kind of specs & standards apply?

## TWIC Prototype Reader Specifications

### Fixed Reader Specifications

- IP65 (environmental sealing; may be achieved with enclosure for biometric sensor)
- ISO 14443A/B (contactless smart card interface)
- 8-25 VDC, specific mounting guidelines
- Credential data output in SIA Wiegand format as required by the PACs (note, optional requirements of RS-232, RS422, RS-485 or TCP/IP based on PACS
- MTBF of 10,000 hours
- FIPS 140-2 Hardware Security Module for protection of keying material
- Field Upgradeable
- TIG-PACS v2.2 / TWIC data model
- ANSI-INCITS 377(pattern) 378 (minutia) for fingerprint biometric matching; Equal Error Rate of 1%
- Read and match biometric in less than 2 seconds

### Mobile (Hand-held) Reader Specifications

- Add ISO 7816 for contact smart cards, if desired

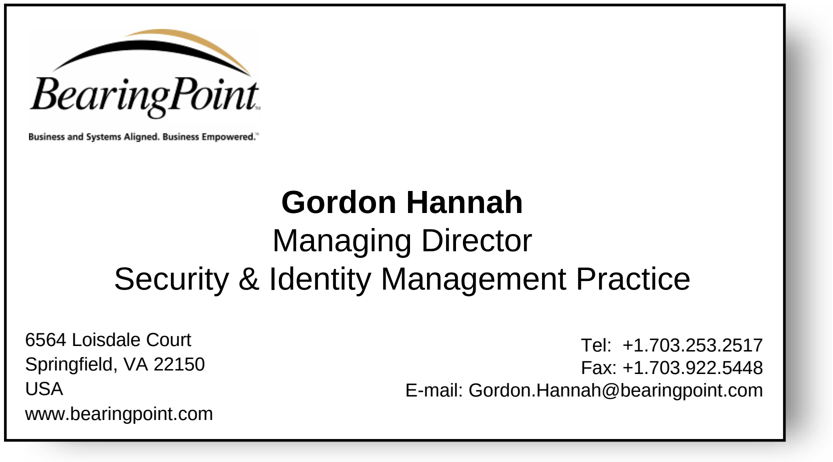
# What will my local infrastructure cost?

## Notional costs

- **Non-biometric, fixed TWIC physical access readers**
  - $50-$100, expected to drop with volume orders
  - Higher if PIN pads are included
- **Biometric, fixed TWIC physical access readers**
  - Fingerprint: $500-$1,200, expected to drop w/volume
  - Iris: $3,000-$7,000
  - Hand Geometry: $1,500-$3,000
- **Handheld / mobile readers**
  - PIN / CRL based: $1,000 - $2,000, expected to drop with volume orders
  - Biometric based: $800 - $1,500

- **Installation of fixed readers is typically 6 labor hours for biometric (keying material may be needed); 1 labor hour for non-biometric**
- **Additional funding may be needed for PACs system installation, cabling, power, communication infrastructure, gates, turnstiles, etc. if not currently in place**

# Contact Information



Business and Systems Aligned. Business Empowered.

**Gordon Hannah**
Managing Director
Security & Identity Management Practice

6564 Loisdale Court
Springfield, VA 22150
USA
www.bearingpoint.com

Tel: +1.703.253.2517
Fax: +1.703.922.5448
E-mail: Gordon.Hannah@bearingpoint.com

# BearingPoint®

Global Management & Technology Consulting