

## **IBIA Suggested Discussion Points for NMSAC TWIC Working Group**

### 1. Review of TSA Guiding Principles

The NMSAC TWIC Working Group (hereafter NMSAC) should review and either accept or propose modifications or additions to the TSA guiding principles included in the proposed task statement as shown below:

- a) Non-proprietary;
- b) Incorporating appropriate security and privacy controls;
- c) Interoperable with FIPS 201-1;
- d) Capable of being a platform for future capabilities;
- e) Capable of supporting maritime operations;
- f) Suitable for manufacturing.

### 2. Concept of Operations

NMSAC should provide high-level operational use case scenarios that define the one-time process of registering and authorizing local facility or vessel access for a specific user. The use case scenarios should also describe typical user experience and interaction with the readers during the authentication process when accessing facilities and vessels. The use case scenarios should describe both fixed base and handheld mobile readers. For example, the requirement for contactless card use may not be as important for hand held readers since there is an interactive process with the user that does not suggest a high throughput requirement and these readers are not continuously exposed to weather. Use case scenarios should describe the data flow and communications from the reader to an access control system (ACS) and/or host server.

Use case scenarios could describe unique user populations that may have different operational interactions with the ACS readers. This could include such populations as regular workers associated with a facility, workers that may visit multiple facilities frequently, workers that may visit facilities only occasionally and when scheduled in advance through another system (e.g., long haul truckers), and merchant mariners. Verification of identity could also be linked to verification of purpose (e.g., manifest) for occasional visitors.

Requirements for facilities and vessels may vary significantly and could be influenced by physical constraints (e.g., multiple independent organizations operating inside a common protected area) as well as local regulations.

### 3. The Relationship Between TWIC and FIPS 201-1

NMSAC should define the areas of divergence between TWIC operational requirements and FIPS 201-1 and the rationale for each. One obvious example is the need for secure contactless access to the biometric data without requiring PIN entry. Another could be that TWIC may not wish to allow “free-read” of the card holder unique ID without first establishing a cryptographically secure session between the card and the reader.

### 4. TWIC Card Data Model

To the extent practical, TSA should describe its draft concept of a TWIC card data model. NMSAC should make recommendations for any changes or additions to this data model that are needed to support operational requirements.

### 5. Data Privacy

NMSAC should define the basic privacy principles that will govern the operational use of TWIC cards. For example, it could be required that a TWIC card never disclose information to an unknown reader and that any transmissions between a card and a reader must be protected through some cryptographic means.

### 6. Key Management

Assuming that some scheme of mutual authentication is to be defined for secure communication between the TWIC card and the reader over the contactless interface, consideration should be given to how cryptographic keys are distributed and loaded onto the TWIC card and the card readers. What will be the role and responsibility of the local facility/vessel operator in this process? What will be the role and responsibility of TSA and its card issuing contractor? Who is liable if a key is revealed, disclosed or leaked? What are the operational impact issues when a key is determined to have been exposed? How is reader maintenance managed in terms of potential key exposure? What happens if a working terminal (containing keys) is lost, stolen or misplaced?

### 7. Communication Between Facility/Vessel Operators and TSA

NMSAC should describe the suggested communication interfaces between the local facility/vessel operator and the TSA central issuance and TWIC database management that are necessary to maintain\access a list of revoked TWIC credentials and to manage, to the extent it may be required, the creation of site-specific cryptographic keys.

### 8. Environmental, Electrical and Safety Requirements and/or Standards

The environmental, electrical and safety requirements for readers should be defined or specific environmental standards should be called out. Note that these requirements may

be different between fixed mount and hand held mobile reader devices. The requirements should describe the following:

- Electrical safety
- Ergonomic safety
- Electrostatic discharge
- Electromagnetic compatibility
- Radiated RF immunity
- Temperature ranges
- Humidity and condensing moisture
- Dust and other airborne contaminants
- Shock and vibration

9. Input Power (fixed mount readers only)

Define the requirements for input power. Below is an example of a requirement developed by TSA for biometric readers to be used in airports:

*A biometric device should permit operation using 115 VAC / 60 Hz power line with up to ±15% voltage tolerance and up to ± 5% in frequency tolerance or 12V DC ± 10% voltage tolerance. A biometric device should be installed to securely route the power and data cables (if applicable) to protect from tampering.*

10. Power Loss Recovery

Should the reader include a capability of storing, retrieving and automatically recalibrating to the properly calibrated biometric sub-system configuration after disruption of power?

11. Operational Availability

Following is an example of an operational availability requirement developed by TSA for biometric devices used in airport access control systems. NMSAC should define a similar requirement for TWIC readers.

*Biometric device reliability (Mean-Time-Between-Failure), maintainability (Mean-Time-To-Repair), and maintenance concept as designed should yield at least a **99.86%** operational availability rate ( $A_o$ ), whereas the cumulative down-time per unit during operational duty hours for all maintenance should not exceed 10 duty hours annually assuming a 20-hour duty day for 365 days each year.  $A_o$  is defined as:*

$$A_o = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \text{ for any single device, any duty day}$$

*Where downtime is the total amount of time the unit is not available for use during the duty day.*

*Downtime can be caused by three events:*

- (a) A critical failure (Any failure where the device cannot perform its mission for greater than 10 minutes and maintenance is contacted);*
- (b) A non-critical failure (Problem occurs and the fault condition is cleared within 10 minutes or is cleared without contacting maintenance); and*
- (c) Recalibration (Following either critical or non-critical failure, time spent restoring the biometric device to operational status, including running through calibration or checkout sequence/procedure.)*

## 12. User Interaction Indicators

Define the requirements for displaying status of any or all of the following:

- Power on
- Ready for use
- Battery level (handheld devices)
- Access granted
- Access denied
- Text messages (e.g., try again, see security officer, etc.)

## 13. Performance – Biometric Error Rates

The basic purpose of utilizing a biometric sub-system as part of an access control system is to verify the identity of the person attempting to gain access to a secure area. There are several fundamental metrics that quantify the performance of a biometric sub-system:

- a) Identity matching error rates (expressed as “false accept” and “false reject” error rates)
- b) Enrollment failures (expressed as “failure to enroll” errors)
- c) Inability of the technology to adequately acquire a biometric sample (expressed as “failure to acquire” errors)

NMSAC should define the minimum performance standards in categories a) and c). Enrollment (category c) is the responsibility of TSA. However, enrollment failures will create an exception condition that may require an operational policy change. Below is an example of standards as defined in a) for verification error rates for biometric readers developed by TSA for airports:

*To qualify as an acceptable biometric device, the device should operate at error rates at or below a transaction False Reject Rate (FRR) of 1% when the security threshold is set at a False Accept Rate (FAR) of 1%. Expressed another way, an acceptable biometric*

*device should have an Equal Error Rate (EER) of 1% or less. TSA's guidance assumes that up to three attempts should be allowed for each verification transaction.*

#### 14. Performance – Transaction Time

There should be a minimum requirement for throughput using fixed base readers for both pedestrians and vehicles. For example, this can be defined as the number of vehicles per hour and/or the elapsed time for a specific authentication transaction from the moment that a user places the TWIC card in proximity of the reader until the time that the gate, portal, or door is opened. Below is an example of a standard set by TSA for the use of biometric readers for access control at airports:

*To qualify as an acceptable biometric device, testing should indicate that the device can process biometric device transactions with an average duration of less than 6 seconds. The start time for the transaction should be the presentation of the claim of identity (such as card swipe, presenting smart card or bar code). The end time for the transaction should be when a verification decision is reached.*

#### 15. Access for Disabled

NMSAC should consider the policy and/or legal implications of requiring biometric authentication for those individuals that may be disabled and unable to comply with this requirement for legitimate reasons. Specifically in regards to biometrics – daily access should consist of elements that do not limit the employee's ability to access the workplace as well as perform his/her work duties. For example, you may require that card readers and biometric sensors be placed so that an employee in a wheelchair, or with another disability, can access the workplace without unnecessary difficulty.

In the event an employee's biometric is significantly altered, alternative authentication mechanisms should be in place to ensure that the employee is not disqualified due to procedures in the process, and the employee is still considered qualified to maintain his/her job under 29CFR1630<sup>1</sup>. However, security officers should always keep in mind that the desired level of security should not be compromised by considerations made in order to comply with the ADA. This includes special accommodations and/or relaxing the requirements for biometric enrollment.

#### 16. Security Levels Based on Threat

Should possession of a TWIC card in conjunction with biometric authentication (2-factor authentication) be a minimum requirement at all threat levels (MARSEC 1, 2 or 3) or will

---

<sup>1</sup> Sec. 1630.7 Standards, criteria, or methods of administration.

It is unlawful for a covered entity to use standards, criteria, or methods of administration, which are not job-related and consistent with business necessity, and:

- (a) That have the effect of discriminating on the basis of disability; or
- (b) That perpetuate the discrimination of others who are subject to common administrative control.

possession of a TWIC card alone (single factor authentication) be considered sufficient at reduced threat levels (e.g., MARSEC 1)? In times of elevated security levels (e.g., MARSEC 3), will there be an additional requirement for personnel to enter a Personal Identification Number (PIN) in addition to presentation of the card and the biometric match as an added authentication factor (3-factor authentication)? If so, consideration should be given to the operational impact in dealing with forgotten PINs under such a policy – particularly when you consider that users may not have used their PIN in a long time. Is there any tangible security benefit to requiring PINs at any threat level?

#### 17. Exception Procedures – Failure to Enroll Biometric

There will be a small number of users that are unable to successfully enroll their biometric characteristic due to a variety of factors. For example, some fingerprint patterns are difficult to measure due to age, injury or skin condition. Administrators should have procedures in place to handle such exception conditions. Alternatives to consider could include:

- Allow card and PIN-only access for those individuals that cannot use biometrics
- Consider including ability to provide biometric enrollment as a job-related requirement in the job description and deny assignment if not capable
- Restrict such individuals to access the secured areas at guard-attended access portal locations only.

#### 18. Exception Procedures - False Rejections

Administrators should expect false rejects in a biometric sub-system. These false rejects could be due to improper presentation of the biometric characteristic to the sensor (such as improper finger placement) or poor quality template capture during enrollment. The biometric sub-system should provide a capability to allow the user to make multiple attempts to authenticate with their biometric. To mitigate this issue, TSA has indicated that two fingerprints will be enrolled. If the primary biometric does not work, then the user can try their secondary biometric. The reader should accommodate this protocol. If multiple attempts with primary and secondary biometric enrollments are not successful, then the user will need to contact a security or administrative person for assistance in gaining access. NMSAC will need to review and comment on the false rejection rate standard set by TSA for biometric matching (after multiple attempts) and determine whether this meets operational needs and what exception procedures will need to be followed to minimize the impact to facility and vessel access control operations.

#### 19. Interface to Existing Access Control Systems

Existing access control systems may have limited data input capability for resolving the unique card holder number. Since TWIC cards are based on a very large theoretical population, there may be a conflict between the TWIC numbering scheme and the ability of the ACS to accommodate the scheme. NMSAC should review the TWIC card holder numbering scheme and give consideration to either (i) recommending a TWIC numbering scheme that fits existing ACS capabilities or (ii) providing guidance for upgrading or replacing existing access control systems.

The data output from the TWIC reader to the ACS may need to support multiple interfaces (e.g., Weigand, Ethernet, RS 485, etc.) to accommodate the widest number of legacy ACS installations. The minimum data output requirements should be defined. It may be necessary to perform a survey of a representative sample of facilities and vessels to determine the typical range of ACS in place, if any.

20. Maintaining Reader Software/Firmware

What should be the procedures and flexibility for reader firmware upgrades? It is more efficient to download firmware/software updates from a central location to each reader since the process of upgrading individual readers at the reader location can be labor intensive. However, downloading of cryptographic keys may have security implications that must be considered.

21. Operational and Reference Biometrics

In the TWIC Prototype Phase, TSA explored the possibility of allowing facilities and vessels to (i) use the required “reference” fingerprint biometric stored on the TWIC card for authentication or (ii) enrolling “operational” biometric data into a locally controlled database within the ACS and using the TWIC card as an “index pointer” to the biometric record stored off of the TWIC card. The advantage of the reference biometric concept was that no external database or secondary biometric enrollment was required. The advantage of the operational biometric concept was that other biometric modalities besides fingerprint could be used at the local facility or vessel (e.g., hand geometry, iris, face, etc.) for authentication of users. A third approach would be to give local facilities and vessel operators the capability to store the operational biometric in the TWIC card itself. However, this raises issues related to conflicts for those users that have to access multiple facilities and where several of these facilities may want to use incompatible operational biometrics stored on the TWIC card. Biometric data occupies significant storage space on the card and it is unlikely that space will be available for multiple operational biometric schemes. NMSAC should make a recommendation to TSA as to whether the government should endorse the local decision to use either reference or operational biometrics.

22. Migration

Consideration should be given to the process of phasing in new TWIC readers at a time when a portion of the user population may still be using legacy ID badges and/or readers. Will more than one type of reader need to be integrated into the ACS at the same time?