FAL/12-IP/16
10/3/04
English only

FACILITATION (FAL) DIVISION — TWELFTH SESSION

Cairo, Egypt, 22 March to 2 April 2004

Agenda Item 2: Facilitation and security of travel documents and border control formalities
2.3: Crew identity documentation

TRANSPORTATION SECURITY ADMINISTRATION (TSA) TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) SYSTEM

(Presented by the United States)

SUMMARY

This information paper presents to the Division activities taking place within the Transportation Security Administration with respect to the development of the Transportation Worker Identification Credential Program.

1. The Transportation Worker Identification Credential (TWIC) Program was developed in response to threats and vulnerabilities identified in the transportation system, and in accordance with the spirit and requirements of the USA PATRIOT Act of 2001, Aviation and Transportation Security Act of 2001, Maritime Transportation Security Act of 2002, and other U.S. statutory mandates for identifying individuals who pose a potential threat to the national transportation system. National Transportation System threat examples include the following:

a) inability to positively identify individuals entering secure facilities and areas;

b) inability to assess the threat posed by individuals due to inadequate background information; and

c) inability to protect current credentials against fraud.

The TWIC system will improve security by implementing an integrated, standardized, credential-based identity management capability for workers requiring unescorted access to secure facilities and areas of all modes of the national transportation system. The requirements for this credential will include:

a) verification of each TWIC applicant's claimed identity;

b) successful completion of a background check prior to issuance;

c) biometric technology to positively identify the TWIC holder at the point of entry;
d) fraud protection methods and technologies;

e) revocation process to deny access privileges to TWIC holders who are identified as posing a threat after issuance of their credentials;

f) process to immediately suspend access privileges for lost, stolen, or compromised credentials;

g) open and non-proprietary scalable architecture; compliant with the Federal Enterprise Architecture; and

h) compliance with the technical standards referenced in the Government Smart-Card Interoperability Specification (GSC-IS V.2.1) and the Biometric Profile – Interoperability and Data Interchange – Biometrics – Verification and Identification of Transportation Workers (INCITS-383) and related specifications.

2. The goal of the TWIC Program is to provide an integrated identity management solution as a tool for facilities operating within the National Transportation System to manage security risks in accordance with their security plans. This tool is also intended to enhance security related business practices by improving the efficiency of ingress and egress within secure areas and reducing the costs to companies, facilities, and individuals by introducing economies of scale and minimizing redundancy.

The TWIC solution is being developed in four phases. Phase I, Planning, was completed in 2002. During Phase I, a series of interactive meetings with over 400 associations and stakeholder organizations were conducted to educate, inform, and to gather and validate requirements. Phase II, Technology Evaluation, was completed in the fall of 2003. In Phase II, the following activities were accomplished:

a) evaluated variety of access control technologies;

b) issued test identity cards to transportation workers through pilot programs at 14 representative transportation facilities on the East and West Coasts; and

c) tested enrollment center, credential production, and card management concepts.

Planning for Phase III, Prototype, began in late 2003, and is scheduled to begin during the first quarter of 2004. Participation in Phase III is voluntary and the population and number of facilities involved in the project are designed to provide a robust test of the full TWIC solution across all modes of transportation.

3. The business processes that will be tested in Phase III are enrollment, application of biometrics, and card production. TSA currently plans to do a name-based terrorist threat assessment at sites participating on the East and West coasts, and in Florida. Florida has State statutory authority to conduct a finger print-based criminal history background check. To that end, TSA will monitor and evaluate the business processes for both of these checks.

Enrollment Centers will be located throughout the Prototype regions. Enrollment Center clerks (a.k.a. Trusted Agents) will collect and scan appropriate claimed identity documents from applicants and verify their authenticity via training and technological desktop tools. The enrollment center clerk will have visibility of status of the enrollment application and card throughout the process. Once the applicant's claimed identity is verified, the clerk will create a data record using biographic information and by capturing a biometric. The biometric images will be used to search the Identification Management System (IDMS) to prevent dual registrations and to provide positive verification of identity. The IDMS will have the ability to query terrorist hot lists, search for reference biometrics[1], send and receive data records for threat

[1] A *reference biometric* is captured at enrollment and used universally throughout the TWIC system to validate and 'lock' the claimed identity of an individual. The reference biometric will be determined during Prototype so that it may be introduced into the Prototype from its inception. The reference biometric does not preclude a facility's choice and use of an *operational*

screening, and send data to facilities. A terrorist threat assessment will then be conducted via a name-based check against a data source containing names of known or suspected terrorists. The enrollment record is then transmitted to a card production facility. The card is personalized and sent to the enrollment center. The cardholder will be required to return to the enrollment center to obtain his/her TWIC and to have the card "activated" and ready for local facility access to be granted. The local facility is responsible for defining and identifying the secure areas as part of its local security plan. Based on anticipated diversity of facilities (multiple locations, sizes and sophistication, multiple transportation modes) TWIC plans to evaluate performance in a wide range of secure areas.

To ensure that this evaluation is thorough and that it enables policy makers to determine whether the Program should be implemented nationwide, the TWIC Program is proceeding as follows:

> Within 45 days of contract award, the TWIC Program will submit the Prototype Evaluation Plan (PEP) to Border and Transportation Security (BTS) for its approval. The PEP will facilitate qualitative evaluations of key TWIC business processes, as well as quantitative evaluations of performance-based metrics.

4. A formal evaluation report will be produced at the completion of the Phase III and will be used to support the Department of Homeland Security (DHS) decision process to implement the TWIC solution. The report will detail objective evaluation criteria in technology, cost, operational performance and process, and metrics against those criteria.

5. As stated in the TWIC Business Case[2], the TWIC solution will conform to all applicable Federal, national, international and industry standards as they relate to the form, fit, and function of credentials. Conformance to standards will help reduce development costs and enhance opportunities for interoperability. Additionally, the TWIC will be made of durable materials and serve as a platform that may contain several technologies and/or media. It is the intention of the TWIC Program to ensure the card meets ICAO standards to accommodate trans-border crossing.

— END —

biometric.

[2] TWIC Program Business Case, Version 3.41, Section 2.7 Card Standards.