

Comments on Transportation Worker Identification Credential (TWIC) Biometric Reader Specification and TWIC Contactless Smart Card Application

March 30, 2007

Notice of Proposed Rulemaking Docket: Coast Guard 2007-27415

The American Association of Port Authorities (AAPA) has been a leader in this country's efforts to bolster port security, and has worked closely with Congress on the passage of the Maritime Transportation Security Act (MTSA) that originally mandated the Transportation Worker Identification Credential (TWIC). AAPA is an alliance of public ports in the Western Hemisphere, and our comments on the Department of Homeland Security's (DHS) proposed rule to implement the Transportation Worker Identification Credential (TWIC) reflect the views of our U.S. members, who own most of the public port facilities in the United States. This includes most facilities that handle containers, auto and ro/ro cargo, cruise passengers, as well as many bulk and breakbulk cargos.

AAPA and many of the association's member ports were represented on the National Maritime Security Advisory Committee's (NMSAC) TWIC Working Group. AAPA and its members provided input into the biometric reader specifications and contactless smart card application discussions and recommendations. AAPA endorses the recommendations provided to DHS by the NMSAC in their entirety. The responses to the questions below reflect this endorsement.

- 1. Should additional security measures be included in the specifications, such as the use of a PIN, to further minimize the chance that a fingerprint template from a lost or stolen credential could be obtained by an unauthorized individual? AAPA does not agree with the addition of a PIN requirement during the TWIC verification process under any circumstances. See question #2 below for fingerprint template security rationale. If so, would the addition of a PIN or other security measure adversely impact operations? Any additional security requirement, particularly the addition of a PIN would increase transaction time, user error, and cost to the system for a minimal gain in security. PINs are forgotten, mis-entered and in many cases are written down in the same location that cards are stored. Does the length of the PIN affect adverse impacts in any measurable way? Longer PINs would likely result in longer transaction times, increased digit input errors, and more frequent forgotten PIN scenarios.**
- 2. What, if any, privacy concerns exist if the fingerprint template is obtained by an unauthorized individual? Because a template is NOT a fingerprint image, but an algorithm generated by reference points, it is of very little use to an identity thief. These algorithms are currently unable to be reverse engineered into usable complete fingerprint images. In point of fact, it would be a lot more accurate and much less challenging to extract a useable fingerprint image from a car door, window, soda can or drinking glass. For this reason, encryption of the fingerprint template is not cost effective or security enhancing. It would simply add unnecessary costs, program administration and time to the transaction.**
- 3. How would the recommended specifications impact facility and vessel security and operations? In terms of security, AAPA strongly supports the implementation of TWIC for maritime workers and believes it is an important enhancement to our current security system.**

Providing a federal card that includes a terrorist and criminal background check of workers will provide facilities added security for their access control process and establish a national standard. From the port perspective, the main impact to operations is lost work time (labor) and increased truck turn times and congestion (transportation) due to transaction time, user error, equipment failure, and queuing at gates and turnstiles. Adding unnecessary additional security measures (such as PIN and template encryption) that increase the likelihood and/or impact of these factors for a minimal perceived security gain is detrimental to operations.

4. **How would the recommended specifications impact existing physical access control systems?** AAPA recommends that the specifications, data requirements, and hardware integration be compatible with legacy systems that ports have invested in during the first seven rounds of port security grant funding in anticipation of TWIC. If data requirements are such that these existing systems are rendered unusable, the technology rollout process will be greatly impacted. The resources and infrastructure requirements for installing new systems would likely cause delays and add cost. At a minimum, most ports will have to install new readers that interface with the TWIC. Our hope is that the existing backend controller/server and related infrastructure is compatible with the technology chosen for TWIC.
5. **Are there alternative designs we should consider, and if so, what are the advantages and disadvantages of the alternative designs?** The NMSAC TWG did consider some alternative designs as suggested by the biometric technology industry group. AAPA stands by the NMSAC recommendation. **How would the recommended specifications impact product, system, and operational costs?** See answer to Question #4.
6. **How quickly could the recommended specifications be incorporated into the design and manufacture of access control equipment?** This is a question for the biometric technology industry.
7. **Should there be a process for identifying a Qualified Products List (QPL) or other equivalent regime? If so, what is the most efficient and effective way of creating a QPL?** AAPA agrees there should be a Qualified Products List. The products on the list should have been properly test by the appropriate laboratories (such as UL) and standards setting organizations. An appropriate government agency (such as GSA) should vet all vendors and products through an application process and provide a QPL list to facilities and vessels implementing TWIC.

The American Association of Port Authorities stands ready to work closely with DHS to ensure the systems required for port facilities work well in the maritime environment so we can achieve the dual goals of enhancing security while continuing the efficient movement of cargo.

Sincerely yours,



Kurt J. Nagle
President