ibia INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

Comments to the House Homeland Security Committee

H.R. 3202 - *Essential TWIC Assessment Act*

November 7, 2013

The International Biometrics & Identification Association (IBIA) welcomes the opportunity to provide comments on H.R. 3202, the Essential Transportation Worker Identification Credential Assessment Act, as offered by Ms. Jackson Lee of Texas before the U.S. House of Representatives Committee on Homeland Security in an Amendment in the Nature of a Substitute. IBIA is a non-profit trade association that promotes the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

IBIA appreciates the Committee's desire to address questions raised by the Government Accountability Office (GAO) in its report dated May, 2013 about the security benefits of the Transportation Worker Identification Credential (TWIC) program.

We understand that this bill is primarily intended to provide an independent and objective assessment of the extent to which the TWIC program, as implemented, improves maritime security. As characterized in the GAO report, the Department of Homeland Security (DHS) takes the position that the "lack of a common credential could leave facilities open to a security breach with falsified credentials". On the other hand, GAO states that "this assumption has not been validated and DHS has not demonstrated how, if at all, TWIC will improve maritime security."

Like the Committee, IBIA is frustrated that the TWIC program has been so long to be fully implemented. IBIA also supports the Committee's efforts to undertake an independent and objective assessment. However, as discussed in detail below, IBIA is greatly concerned that, any assessment undertaken pursuant to H.R. 3202 as drafted, would be inherently biased against TWIC.

The following are specific comments related to items included in sub-sections of the bill under Section 2(b) that describe the contents of a comprehensive assessment:

Current Language:
Section 2(b)(1) - an evaluation of the extent to which the program, as implemented, addresses known or likely security risks in the maritime environment

Comments: IBIA does not believe that it is possible to evaluate the security effectiveness of the TWIC program as it is currently implemented. The key security element of the TWIC program – the use of biometric readers to validate the card and verify the card holder's identity – is not currently required by regulation. Therefore, the program's security benefits cannot be uniformly assessed.

To illustrate, at the highest risk maritime facilities and vessels, there is currently no adequate method of protecting against a security breach resulting from the unauthorized use of stolen, lost, borrowed or forged TWIC cards. While the TWIC card contains certain physical security features that can be visually verified to provide some protection against forgeries, it is possible for a determined individual with criminal or terrorist intent to obtain a high-quality forgery of a TWIC card that would pass visual inspection. Also, there is no way for security personnel to visually detect if the TWIC card has been revoked by TSA as a result of the card being reported lost or stolen or if the card holder has been designated by TSA as ineligible to continue holding a TWIC card.

Further, visually comparing the photo on the card to the person presenting the card, as a means of confirming identity, is subject to human error and/or human fatigue. For these reasons, the U.S. government has determined that visual inspection of government-issued credentials offer little or confidence in the identity of the holder[1].

As currently implemented, the TWIC program – with no mandatory use of electronic readers at high-risk facilities and vessels – is vulnerable to security threats resulting from the unauthorized use of stolen, lost, borrowed or forged TWIC cards.

Recommendations: Change the language to read as follows: *An evaluation of the extent to which the program addresses known or likely security risks in the maritime environment based on the deployment of electronic readers.*

Current Language:
Section 2(b)(2) - an evaluation of the extent to which internal control deficiencies identified by the Comptroller General have been addressed

Comments: IBIA has no objection or suggested changes to the above provision.

Current Language:
Section 2(b)(3) - a cost-benefit analysis of the program, as implemented, and consideration of the use of alternate biometric technologies that provide the same or greater security effectiveness, including –

[1] See Section 6.3.1 Table 6-2 – Physical Access – Federal Information Processing Standard 201-2 (FIPS 201-2) - Personal Identity Verification of Federal Employees and Contractors which states that the visual (VIS) authentication mechanism provides an assurance level of "little or no confidence". See http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

(A) technologies and programs, including the biometric entry and exit system required by section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458; 8 U.S.C. 1365b);
(B) technologies and programs in use at United States port facilities and vessels, particularly for purposes of access control to critical infrastructure;
(C) international technologies and programs that are in use, including for purposes of access control to critical infrastructure; and
(D) new and emerging technologies.

Comments: There are two unrelated topics in Section 2(b)(3) which are addressed separately. This comment relates to the cost-benefit analysis. IBIA believes that it is not possible to conduct a meaningful cost-benefit analysis for the TWIC program as implemented. Since TWIC is currently implemented without readers, the security benefits cannot be assessed.

Rather than a ranking of cost–benefits against other credentialing programs and approaches, a more useful approach could be a comparison of the benefits of TWIC, as it was intended to be implemented, with other existing credentialing programs. IBIA believes that the TWIC program, when properly implemented with electronic readers, can provide the security benefits the program is designed to provide and would welcome a constructive evaluation of alternative credentialing approaches.

Recommendation: As drafted, IBIA cannot support the provision in Section 2(b)(3) because electronic readers – the key security element of TWIC – have not been implemented and the results would inherently be biased against the TWIC program. However, if the language is modified to require a cost/benefit assessment of the TWIC program as it was intended to be implemented with electronic readers, IBIA could support the Committee's assessment.

Comments: Regarding the second part of Section 2(b)(3), as written, it can be interpreted to mean that there would be an evaluation of the security effectiveness of one biometric technology vs. another (e.g., fingerprint compared with iris recognition). If this interpretation is correct, IBIA does not believe that it is necessary to evaluate alternate biometric technologies. This is because the TWIC program already provides the flexibility for maritime operators to implement alternative biometric technologies in conjunction with the TWIC card as long as a chain of trust is maintained through appropriate one-time registration into the maritime operator's access control system using the federal standard fingerprint biometrics.

For example, The Georgia Ports Authority uses hand-vein recognition biometric readers for access to their facilities and this use of alternate biometric technology is consistent with the

Coast Guard's proposed regulations for TWIC readers. Based on the above, IBIA does not believe that an evaluation of alternative biometric technologies is needed.

Recommendations: IBIA recommends in Section 2(b)(3), delete the following: "…*and consideration of the use of alternate biometric technologies that provide the same or greater security effectiveness, including –*

(A) technologies and programs, including the biometric entry and exit system required by section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458; 8 U.S.C. 1365b);

(B) technologies and programs in use at United States port facilities and vessels, particularly for purposes of access control to critical infrastructure;

(C) international technologies and programs that are in use, including for purposes of access control to critical infrastructure; and

(D) new and emerging technologies."

The following are specific comments related to items included in Section 2(e) of the bill related to the Reader Rule:

Current Language:
Section 2(e) - "TRANSPORTATION SECURITY CARD READER RULE. – *The Secretary of Homeland Security may not issue a final rule requiring the use of transportation security card readers until –*
(1) the Comptroller General informs the Committees on Homeland Security of the House of Representatives and Commerce, Science and Transportation that the submission under sub-section (a) is responsive to the recommendations of the Comptroller General; and
(2) *the Secretary issues an updated list of transportation security card readers that are compatible with active transportation security cards.*

Comments: At the highest-risk maritime facilities and vessels, the implementation of electronic card readers is essential to addressing an existing vulnerability related to a security breach resulting from the unauthorized use of stolen, lost, borrowed or forged TWIC cards. The security industry has long recognized that, for high-risk facilities, it is best security practice to control access with electronic readers that can quickly, consistently and efficiently validate card authenticity, check expiration dates, check for card revocation and confirm card holder identity. Delaying implementation of the TWIC reader rule would only perpetuate this security vulnerability. For this reason, IBIA believes that the proposed assessment should not further delay the deployment of electronic TWIC card readers at the highest risk maritime facilities and vessels.

Recommendations: Delete Section 2(e) in its entirety.

Further, IBIA hopes that the Committee supports our efforts to encourage the Coast Guard to expand the requirement for mandatory use of TWIC readers to include a larger number of general cargo container terminals and petroleum facilities than currently identified in its TWIC Reader Requirements Notice of Proposed Rulemaking (NPRM). In our formal comments on the NPRM, IBIA noted that the Coast Guard's economic analysis has several issues that overstate the cost of TWIC reader deployment or understate its economic benefits. For example, we believe that the Maritime Security Risk Assessment Model (MSRAM) used by the Coast Guard is severely flawed since it did not consider the secondary economic cost impact that would result from the extended disruption of a large container terminal or petroleum facility as a result of a terrorist security incident. The result is the NPRM limits the mandatory use of readers to only 5% of TWIC holders. IBIA hopes that Congress will also address this issue.

IBIA looks forward to working with Congress to ensure an effective and fully implemented TWIC program that enhances security and reduces security risks for maritime facilities and vessels regulated pursuant to section 102 of Public Law 107-295, as originally envisioned by Congress.