INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

June 13, 2013

To: U.S. Coast Guard Notice of Proposed Rulemaking
Docket No. USCG-2007-28915
Transportation Worker Identification Credential Reader Requirements
Notice of Proposed Rulemaking

The International Biometrics & Identification Association (IBIA) is pleased to provide comments on the Transportation Worker Identification Credential (TWIC) Reader Requirements Notice of Proposed Rulemaking (NPRM). These comments include and expand on verbal comments made by IBIA at the public hearing held by the Coast Guard in Arlington, VA on April 17, 2013.

IBIA is a non-profit trade association based in Washington, DC representing providers and implementers of high-assurance personal identification solutions. IBIA's members provide essential security technology and integrated solutions in both government and commercial sectors for such applications as secure credentialing, access control, cyber security, law enforcement, defense intelligence, border security, mobile device security, and secure electronic transactions.

IBIA is proud to have actively supported the TWIC program since its inception. Our members played a major role in the development of the technology behind the TWIC program. For example, in 2007, IBIA was asked by the Coast Guard and TSA to organize and lead a voluntary team of security industry professionals to assist the National Maritime Security Advisory Committee (NMSAC) in defining a technical specification for TWIC readers that would reflect the unique operational and functional requirements of the maritime industry. As a result of these efforts, NMSAC was able to deliver a draft TWIC reader technical specification to TSA and the Coast Guard and this specification was published by TSA on September 11, 2007.

We urge the Coast Guard to consider the comments that follow. IBIA believes that the recommendations and suggestions provided will enhance the effectiveness of the TWIC program in meeting its security objectives and will provide measurable benefit to the maritime industry if incorporated in the final rule. If you have any questions, please contact me at tovah@cl-law.us or by phone at (202) 587-4855.

Sincerely,

Tovah LaDier

Tovah LaDier
Managing Director

INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION
919 18TH STREET, NW • SUITE 901 • WASHINGTON, DC 20006 • USA
TEL 202.587.4855 • FAX 202.587.4888 • WWW.IBIA.ORG

INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

U.S. Coast Guard Notice of Proposed Rulemaking
Docket No. USCG-2007-28915
Transportation Worker Identification Credential Reader Requirements
Notice of Proposed Rulemaking

The requirement for reader use should be expanded to include more general cargo container terminals and petroleum facilities.

The Maritime Transportation Security Act (MTSA) of 2002 transportation security card requirement, as well as the Security and Accountability For Every (SAFE) Port Act of 2006 electronic TWIC reader requirements call for the installation and use of electronic readers to verify and validate the information presented on a TWIC upon requesting unescorted access to a secure area of a vessel or facility. The NPRM proposes that the use of TWIC readers be required only at facilities and vessels in Risk Group A. According to the NPRM, this represents only 5% of the TWIC holder population and we do not believe that this is consistent with the intent of Congress in the previously referenced legislation. Facility and vessel operators in Risk Groups B & C (which represent approximately 95% of TWIC holders) would be permitted to rely solely on visual inspection of TWIC cards for persons seeking unescorted access to secure areas.

We believe that the mandatory use of TWIC readers should be expanded to include additional facilities in Risk Group B in order to achieve a more appropriate and uniform level of access security for this critical component of our maritime infrastructure. For example, many large general cargo container terminals and petroleum facilities are included in Risk Group B. This classification seems to be counter intuitive since disruption to any one of these facilities could have significant negative consequences for our nation's economy. Further, the economic analysis supporting this NPRM does not appear to consider the secondary economic cost impact that would result from the disruption of such facilities because of a terrorist security incident.

Also, it does not appear that the NPRM considered in its risk analysis that maritime facilities and vessels are often co-located in close proximity on the waterfront such that a lower risk group facility or vessel will often be immediately adjacent to or will have direct line of sight to a higher risk group facility or vessel. This creates the potential for a terrorist to use fake TWIC credentials to gain access to a less secure facility or vessel that relies on visual inspection protocol and then use that location to mount an attack on an adjacent facility or vessel.

At a minimum, we recommend that the Coast Guard expand the mandatory requirement for TWIC readers to include general cargo container terminals and petroleum facilities now assigned to Risk Group B. This will enhance the security of these facilities, encourage the participation of labor unions, and allow these facilities to effectively compete for grant funding to support their implementation of TWIC readers and supporting systems.

INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

U.S. Coast Guard Notice of Proposed Rulemaking
Docket No. USCG-2007-28915
Transportation Worker Identification Credential Reader Requirements
Notice of Proposed Rulemaking

Visual inspection of TWIC cards is not an effective security protocol when compared to the use of electronic readers.

The primary reason that we support expanding the mandatory use of TWIC readers is because we strongly believe that visual (or "flash pass") inspection of TWIC cards is not an adequate security protocol. This is particularly true for those facilities in Risk Group B (such as general cargo container terminals and petroleum facilities) that represent important economic infrastructure assets. We base this conclusion on the following facts:

1. Visual inspection of TWIC cards is subject to human error. After all, security personnel are human and we believe that they will be unable to consistently adhere to the Coast Guard's recommended visual inspection protocol – particularly if they are tired, distracted or have other duties to perform.

2. Visual inspection is not an effective method of detecting counterfeit TWIC cards. There are numerous Web sites that sell high-quality fake IDs complete with holograms, color shifting ink, etc. that would defy visual detection. Failure to mandate the use of TWIC readers in Risk Group B facilities and vessels will further encourage a black market in fake TWIC cards.

3. Visual comparison of the printed photo on the TWIC card with the face of the card holder is subject to human error and is not an effective method of detecting stolen or borrowed TWIC cards. A person's appearance is likely to change slightly over the five-year life of a TWIC card. For example, they may start wearing glasses or grow facial hair. These variations in facial appearance will naturally result in security personnel having difficulty detecting the fraudulent use of TWIC cards - whether such use is for mounting a terrorist attack or for some other prohibited activity such as "job renting".

4. It is important to emphasize that it is impossible for security personnel conducting visual inspection of TWIC cards to detect that the card has been revoked by the government. If TSA receives a report that a TWIC card has been lost or stolen, or that a card holder is now identified as a security threat, they will immediately add the TWIC card identifier number to the TWIC Cancelled Card List. This CCL is readily accessible to maritime operators by downloading the list from the TWIC Web site. However, only a TWIC reader can read the unique card identifier number from the card and compare it with TSA's CCL. The identifier number is not printed on the card.

5. As a result of Homeland Security Presidential Directive 12, all agencies in the Executive Branch of the government were required to issue an interoperable, tamper-resistant,

biometrically-enabled Personal Identity Verification smart card credential. PIV cards have now been issued to over 7 million government workers. This includes civilian employees, members of the military and all government contractors. The security technology in the PIV card is the same as the technology included in the TWIC card and is based on a Federal standard developed by the National Institute of Standards and Technology (NIST).

The Office of Management and Budget has now directed executive branch agencies to expedite the "full use of the PIV credentials for access to federal facilities and information systems". However, in its most recent update to the Federal PIV standard that was issued last year, NIST reduced its ranking of the value of visual inspection of PIV cards and has determined that visual inspection of the PIV card for physical access provides an identity assurance level consisting of "LITTLE or NO confidence". In an earlier version of the standard, NIST had ranked visual inspection as providing "SOME confidence". Based on this guidance, we believe that Federal agencies will likely deploy PIV readers (that are similar to TWIC readers) rather than rely on visual inspection of PIV cards. It seems contradictory that employees of the National Endowment for the Arts will be required to use PIV readers to access their facilities, but unescorted access to secure areas of large container terminals, on which our country depends for its economic vitality, will be based on visual inspection of TWIC cards.

TWIC readers can quickly and consistently check that (i) the card holder is the same person to whom the card was issued by matching the presented biometric with the biometric identifier stored on the card, (ii) check that a TWIC card has not expired, (iii) check that a TWIC card is not a copy or clone and that it is a legitimate card issued by TSA, and (iv) check that the card has not been revoked by the government by comparing the card unique identifier against the CCL.

Reader transaction recordkeeping should be protected as SSI only to the extent that records contain personally identifiable information

The NPRM proposes a requirement for owners and operators using TWIC readers to maintain transaction records for each person accessing secure areas and to treat such records as Sensitive Security Information (SSI) in accordance with 49 CFR Part 1520. We agree that reader transaction log records should be secured against unauthorized access to protect the privacy of the cardholder, but only if such records include name, commercial driver's license number, photo or other personally identifiable information (PII). If such records do not include PII and only include such information as the Federal Agency Smart Credential Number, date, time, location, etc., then we see no reason to apply SSI protection measures.

INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

U.S. Coast Guard Notice of Proposed Rulemaking
Docket No. USCG-2007-28915
Transportation Worker Identification Credential Reader Requirements
Notice of Proposed Rulemaking

Minimum recordkeeping data elements should be expanded.

The NPRM proposes that TWIC reader transaction records include the following data elements: (1) FASC–N; (2) date that access was granted; (3) time that access was granted; and (4) if captured, the name of the individual to whom access was granted. We recommend that minimum TWIC reader transaction records also include an identifier of the specific reader device. Further, if the reader is a portable device, the transaction record should also include an identifier of the operator. These additional data elements will provide essential information on location and/or operator to enhance the accuracy and usefulness of the audit trail.

The economic analysis should be reviewed and updated with more current and accurate data.

IBIA reviewed the TWIC Reader NPRM Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis document (USCG-2007-28915 dated February, 2013) which was included in the Docket. We understand that this document is intended to provide an assessment of the potential cost and benefits of the TWIC reader proposed rule.

Through our review, we determined that the economic analysis has several issues that overstate the cost of TWIC reader deployment or understate its economic benefits as follows:

1. There is no consideration given for the reduction in staffing cost through the use of electronic readers when compared to the alternative of performing visual inspection of TWIC cards at entry points.

2. The Accounting Statement (A-4) cites the benefit of readers through the reduction in human error when visually checking TWIC cards, but considers this as an "unquantifiable benefit". We believe that this benefit should be given more weight in the economic analysis – particular given the fact that visual inspection cannot detect the presence of a TWIC card on the CCL.

3. We believe that the cost avoidance of a terrorist security incident (TSI) through the use of TWIC readers is understated since the economic analysis does not appear to consider the secondary economic cost impact that would result from the extended disruption of large container terminals or petroleum facilities as a result of a TSI.

4. We believe that the TWIC Pilot grant fund expenditures used in the economic analysis to project the cost of TWIC reader national deployment overstate the physical access control system (PACS), infrastructure and installation cost of TWIC readers. We believe that discretionary costs not directly related to TWIC reader requirements (e.g., guard

stations, lift gates, fencing, etc.) were improperly included in the economic analysis as a cost of TWIC reader implementation.

5. TWIC reader transaction failure rates observed during the TWIC Pilot were extrapolated and used to project the cost of managing transaction failures in a national deployment. We believe that these error rates are not representative of the current state of TWIC reader technology and systems and should not be used as the basis for projecting future performance. User errors due to unfamiliarity with TWIC reader systems were to be expected in a pilot test and we believe that these types of errors account for a significant portion of the reader transaction failures. We also believe that the high error rates were negatively impacted by the fact that, during the pilot, TWIC cards were found to be prone to high rates of failure in the contactless mode (which unfortunately was the primary intended use case). We understand that TSA has since conducted a card failure analysis study and determined that TWIC cards issued since the fall of 2009 are much more durable and that contactless card failures should not be a problem in the future. We also note that the early vintage TWIC cards that exhibit this condition will all be replaced through the normal renewal process long before the enforcement date of this rule.

6. The economic analysis document provides the details that were used in estimating the average TWIC reader hardware and software acquisition cost at $12,499 for fixed readers and $14,036 for portable readers. We believe that these cost estimates are significantly overstated because the Coast Guard used software pricing from a single supplier that does not provide TWIC reader hardware. Most TWIC reader vendors include on-board reader software bundled with their hardware price. IBIA had provided the Coast Guard with its own estimate of reader acquisition costs in June 2011 which is available on our Web site at www.ibia.org/resources. This estimate suggested that the fixed and portable reader hardware and software acquisition cost should be in the range of $4,250 for a fixed or portable reader. It is recommended that the Coast Guard conduct a survey of TWIC reader manufacturers to develop a more current and accurate estimate of reader acquisition cost. We do believe that the NPRM estimate of 5% annual maintenance cost for TWIC readers is reasonable.

7. Updates to the cancelled card list (CCL) should be an automated function taking just a few seconds and should not be included as an on-going cost item with assigned labor expense.

INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

U.S. Coast Guard Notice of Proposed Rulemaking
Docket No. USCG-2007-28915
Transportation Worker Identification Credential Reader Requirements
Notice of Proposed Rulemaking

Since the pilot, TWIC readers have demonstrated effectiveness.

There have been concerns raised as to the effectiveness of the TWIC Pilot data as a result of questions raised in a Government Accountability Office (GAO) report. In spite of the voluntary nature of the pilot, high contactless failure rate of early TWIC cards, and the inexperience of implementers and users of TWIC reader systems at the time, IBIA believes that valuable data was obtained and useful lessons were learned that have helped lead to mature TWIC reader products and systems. Since the pilot test ended, voluntary deployment of next generation TWIC readers has shown that TWIC readers can achieve the security objectives of the TWIC program and, at the same time, enhance the efficiency of maritime operations.

As an example, SSA Marine is a large container terminal operator in California that has deployed 23 TWIC readers for facility access at three terminal locations. This operator has registered over 25,000 TWIC cards in their access control system. They have a very high volume of truck traffic with 4,500 daily gate moves and have recorded over one million TWIC reader access transactions since May 2012.

A key point included in this operator's experience with TWIC readers is that in less than one year, at one of their terminal facilities, TWIC readers have automatically detected and prevented the unauthorized use of over 2,400 revoked TWIC cards because they were included on the TSA Cancelled Card List. Most, if not all, of these revoked TWIC cards would have been accepted for access to facilities and vessels that rely only on visual inspection.

The SSA Marine experience also demonstrates high throughput at entry points. Specifically, this operator reported an average transaction time of 3.5 seconds which included card validation and fingerprint verification. This is significantly faster than the 8 second estimate used in the NPRM assumptions which were derived from the data collected during the TWIC Pilot Test that concluded in May, 2011. This case study is particularly instructive in that it illustrates the learning curve that will naturally occur following the implementation of any new system. We would expect similar throughput improvements as users become more familiar with the use of TWIC readers.

###