Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(1):40-51

Research Article ISSN: 2394 - 658X

Analyzing the Transportation Worker Identification Credential (TWIC) Program

Borget Alfred Anoye

Department of Mechanical and Energetical Engineering, Institute National Polytechnique Félix Houphouët Boigny (INP-HB), Yamoussoukro, Ivory Coast
borgetanoye@yahoo.com

ABSTRACT

The Transportation Worker Identification Credential (TWIC) Card is a form of identification that is required for all maritime or offshore workers who need unescorted access to secure areas of MTSA regulated facilities. These measures are all to protect U.S. owned ports from terrorist activity. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners, must obtain a TWIC. Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and United States Coast Guard (USCG) jointly administer the TWIC program. By relying on multiple authentication methods (credential, personal identification number or password and biometric information) as well as strong application authentication, the TWIC provides a higher level of security than verification methods currently in use. The biometrics used reduces significantly the risk of fraudulent or altered credentials and the risk of unauthorized access. With the TWIC heavy security system, companies implementing the TWIC card will build the necessary trust required in business-to-consumer and business to-business activities. Also, the TWIC allows securing the supply chain from the beginning to the end and ensuring that no information and components are compromised. Although the TWIC is a powerful security tool, the widespread detailed information collected by TSA poses the direct risk that this information, in the wrong hands, could enable precisely the safety threat that these programs seek to prevent. In this era of widespread identity theft, it is imperative that TSA consider carefully the potential danger of disseminating the highly sensitive personal information gathered.

Key words: Enrollment, Enrollment, IDMS, Credential Issuance, Background Check, Privilege Granting, Access Control

---

INTRODUCTION

On the aftermath of September 11, 2001, U.S government and the Congress developed several federal legislative mandates in response to threats and vulnerabilities identified in the transportation system nationwide. These mandates consist of the U.S. Patriot Act of 2001, the Aviation and Transportation Security Act of 2001, and the Maritime Transportation Security Act of 2002. The USA PATRIOT Act requires a security threat assessment on commercial drivers who transport hazardous materials and provide appropriate tools required to intercept and obstruct Terrorism. The Aviation and Transportation Security Act (ATSA) requires a security threat assessment on the transportation system and the development of policies and programs to counter those threats, including background checks for transportation workers with unescorted access to secure areas. The Maritime Transportation Security Act of 2002 (MTSA) requires the completion of background checks and issuance of biometric transportation security cards for all maritime personnel requiring access to secured areas of vessels and facilities. Terrorists, as a threat, may gain access to secure areas of the transportation system by compromising current identity management and access control systems. As ports, waterways, and vessels handle billions of dollars in cargo annually, securing the transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy. Ports are susceptible to terrorist attacks because of their size, general proximity to metropolitan areas, volume of cargo being processed, and link to the global supply chain. Controlling access to secure areas is critical to improve port security [1]. Through the MTSA, Congress directed the Department of Homeland Security (DHS) to prescribe regulations that would prohibit an individual from gaining unescorted access to a secure

area of a regulated facility. Unless that individual holds a duly-issued transportation security card and is otherwise authorized by the owner or operator to be in such a secure area [2]. In accordance with these legislative requirement, the DHS initiated the Transportation Worker Identification Credential (TWIC) program to protect critical portions of the Nation's maritime transportation infrastructure from acts of terrorism. The Transportation Worker Identification Credential (TWIC) program was established in December 2001 with the intent to issue a biometric security credential to individuals who require unescorted access to secure areas of facilities and vessels. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners, must obtain a TWIC [3]. Port employees, longshoremen, mariners, truckers, and others who require unescorted access to secure areas of ports and vessels would be required to be vetted under the TWIC program. TSA began national deployment of the TWIC program on October 16, 2007, with the enrollment of maritime workers at the Port of Wilmington, DE. Enrollment began in Corpus Christi, Texas; Baton Rouge, La.; Beaumont, Texas; Honolulu; Oakland, Calif.; Tacoma, Wash.; Chicago/Calumet, Ill.; Houston; Port Arthur, Texas; Providence, R.I.; and Savannah, Ga. shortly thereafter. As of May 2018, TSA issued TWIC credentials to over 3 million workers enrolled in the program while identifying and preventing approximately 50,000 TWIC applicants who did not meet the required security threats assessment from receiving a TWIC [4]. The purpose of this paper is to analyze the TWIC program and present the challenges faced by the program.

THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROGRAM

The Transportation Worker Identification Credential (TWIC) program is a Department of Homeland Security (DHS) initiative. Within DHS, the Transportation Security Administration (TSA) and United States Coast Guard (USCG) jointly administer the TWIC program:

- TSA conducts background checks and recurrent vetting, issues credentials, and takes civil enforcement action against individuals engaged in credential alteration and fraudulent use. TSA is responsible for TWIC enrollment, security threat assessment and adjudication, card production, TWIC issuance, appeal/waiver for TWIC denials, and technology/TSA system management
- In the maritime environment, the Coast Guard develops and enforces TWIC regulations, takes civil action against facility owners, and refers criminal matters against facility owners and cardholders to the appropriate Federal, state, or local prosecuting agency. USCG enforces the use of TWIC at MTSA regulated vessels, facilities and OCS facilities, and conduct biometric check as part of vessels and facility compliance inspections.

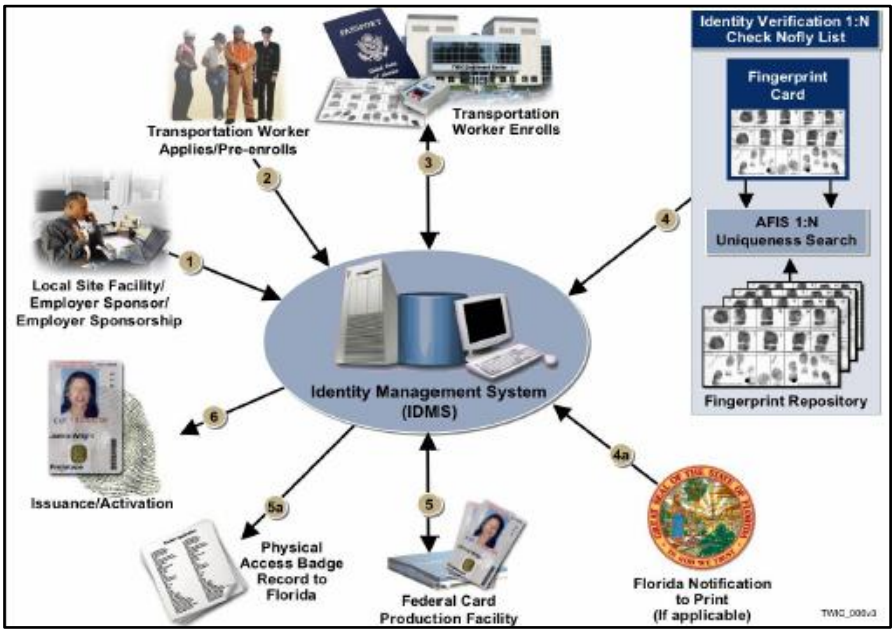

Fig. 1 TWIC Program Components [6]

The TWIC program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, and vessels regulated under the MTSA and all U.S. Coast Guard credentialed merchant mariners [2]. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners, must obtain a TWIC.

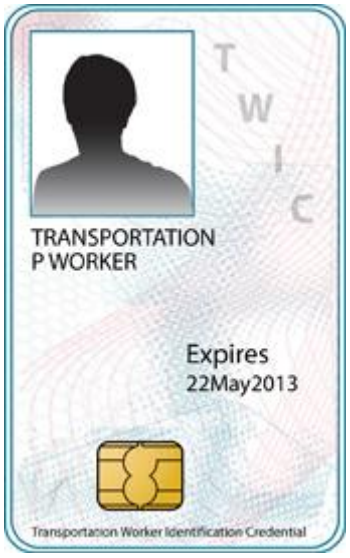

Fig. 2 The TWIC Card

To obtain a TWIC, an individual must visit a TWIC application center to provide required documentation, biographic and biometric information, be fingerprinted, take a digital photograph, pay a non-refundable fee and successfully pass the security threat assessment of TSA. The TWIC is valid for five years, unless renewed before the five-year term ends. Applicants undergo a comprehensive background check that examines criminal history records, terrorist watch lists, immigration status, and outstanding wants and warrants. Individuals lacking lawful presence and certain immigration status in the United States, connected to terrorist activity, or convicted of certain crimes are ineligible to obtain a TWIC [2]. Only individuals who are not deemed a terrorism security risk after a criminal history records review and national security database check will be issued a TWIC.

The provided card contains a computer chip, known as an Integrated Circuit Chip (ICC), which stores the holder's information and biometric data. The chip can be read by inserting it into a reader or holding it near a "contactless" reader. There are also a magnetic strip (similar to a credit card) and a linear barcode on the back as alternative reading methods [5]. By relying on multiple authentication methods (credential, personal identification number or password and biometric information) as well as strong application authentication, the TWIC provides a higher level of security than verification methods currently in use. The system wide encryption and the use of a minimal amount of data ensure maximum protection of personal information. The usage of the biometry reduces significantly the risk of unauthorized access.

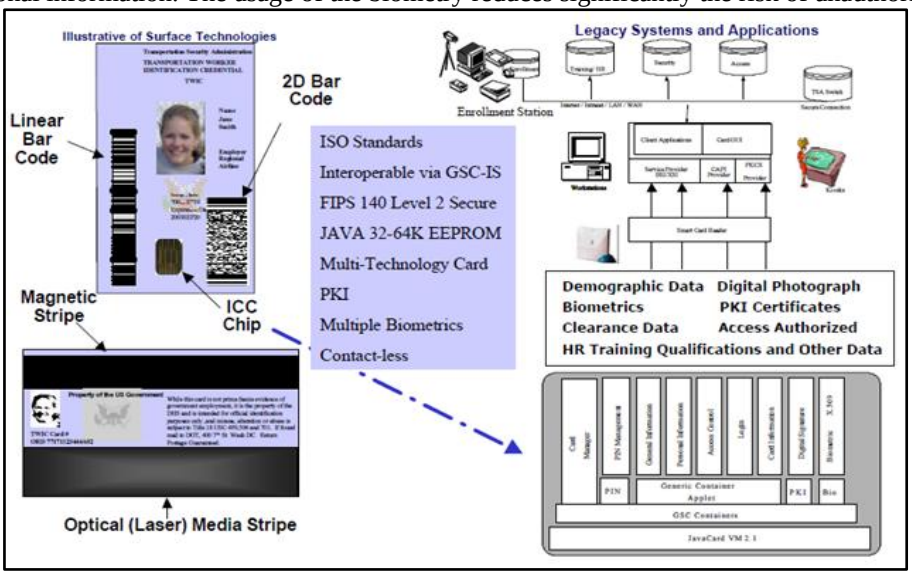

Fig. 3 Card architecture

TWIC electronic cards readers are devices that comply with the TWIC Reader Hardware and Card Application Specification published by TSA. The readers can be fixed or portable. TWIC card reader technology allows biometric matching using a contactless reader and determines whether a card has been revoked or reported lost or stolen. TWIC Readers confirm that the card is authentic and issued by TSA; that the card has not expired; that the card has not been revoked or reported lost or stolen; and through a biometric fingerprint match the person presenting the card is the rightful holder. Many readers can obtain and/or exchange information with a TWIC card. TSA maintains and publishes a list of TWIC readers that have been evaluated by independent laboratories for compliance [5].

Fig. 4 TWIC Reader

THE TWIC PROCESS

With the TWIC Program, at each transportation facility to which the worker requires access, privileges must be granted. The identification security of the TWIC Program is designed to establish a chain of trust that ties the individual to a security check, and then the card to the individual through the use of a biometric identifier. The TWIC biometric identification data can be accessed and verified when presented at any facility to gain access to secure areas. This ensures that the individual presenting the TWIC to the reader is in fact the individual who applied for and was approved by the Transportation Security Administration for such access; that a threat assessment has been completed on that identity; and that each credential issued is linked to the rightful holder.

TWIC card issuance:

1. A registered employer (or local facility) initiates a request for TWIC to be generated.
2. TWIC applicant completes pre-enrollment and enrollment in-person.
3. Enrollment record request sent to IDMS.
4. 1:N check of Reference Biometric performed.
5. Name-based threat assessment initiated and go, no-go results are returned to IDMS.
6. Authorization to produce TWIC and requisite data sent to Card Production Facility.
7. The user's card is personalized and encoded.
8. Card is securely shipped to the designated Enrollment Center.
9. TWIC Applicant returns to Enrollment Center, validates his identity using the reference biometric, and the card is electronically unlocked and issued.
10. IDMS is notified of TWIC issuance and activation.

TWIC card usage at local facility:

11. TWIC holder requests access privileges at transportation facility.
12. Local facility notifies IDMS that access privileges have been granted.
13. Threat/intelligence information is received, and the generated watch list is compared to IDMS.
14. TWIC Hotlist is broadcast to all facilities, as well as a specific notification to any site where privileges have been granted.
15. Revocation and Disposition.

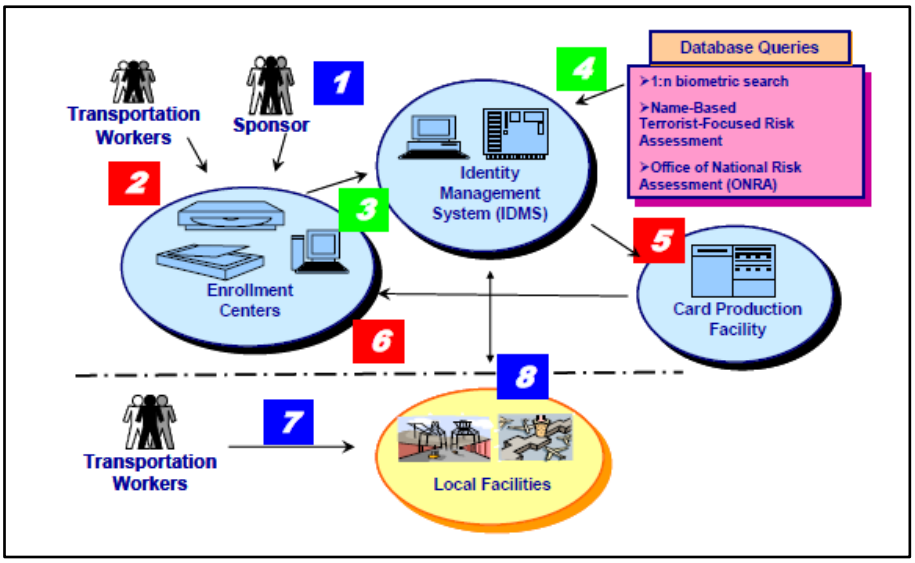

Fig. 5 TWIC Process [6]

THE TWIC SYSTEM WORKFLOW

Employer/ Sponsor Registration

The sponsor is either the employer, or, in the case of self-employed workers (i.e. self-employed truck drivers), a participating facility operator. In any case, sponsors must register the applicants before the applicant can apply (i.e., pre-enroll) for a TWIC. Employers must register and establish a link between them and the applicants they wish to sponsor. The TSA trusted agents at facility provides employers and other sponsors with instructions on how to register and sponsor applications. Employer registration occurs electronically via a secure web portal established by TSA. Employer registration required the employer or facility operator to provide the following information, company name, address, type of business, and the company Employer Identification Number (EIN).Once the registration form has been completed and submitted, TSA began the process for approving the entity as a sponsor. This process end up with a TSA confirmation that the employer or facility operator is a recognized business entity authorized to participate to the TWIC program. Employers are then authorized to provide a list of employees they are sponsoring.

Pre-Enrollment

Applicants are encouraged, but not required, to pre-enroll, as it can save time by pre-enrolling online. Applicants with access to the internet can pre-enroll to save time during enrollment. The pre-enrollment process allows applicants to provide much of the biographic information required for enrollment; to select an enrollment center where they wish to complete the enrollment; and to make an appointment. During pre-enrollment, applicants will enter biographic information required for the security threat assessment and make an appointment at the enrollment center. Although appointments are not required for enrolling, appointments are encouraged to save applicants time.

Enrollment

Enrollment is the process of completing the application process and collecting biometric information. Biographical information may be provided during pre-enrollment. Any biographical information that is not collected during pre-enrollment is collected during the enrollment process. Additionally, biometric information collection and identity verification that need to occur in person is conducted during this process. At TSA Enrollment Center, applicant completes the TWIC Disclosure and Certification Form, provide required documents, provide a set of fingerprints, sit for a digital photograph, and pay a fee. Applicants are encouraged to complete the TWIC Disclosure and Certification Form and bring it with them to the enrollment center. Participants are able to enroll or obtain a TWIC if he or she does have the required forms of identification and signed the TWIC Disclosure and Certification Form. If participating in the process, the helper/translator will also sign the form and provide contact information. The enrollment process for a pre-enrolled applicant takes approximately 10 minutes. The enrollment process for those who did not pre-enroll takes approximately 15 minutes. There may be a wait time at the enrollment center depending on the amount of workers choosing to enroll at any particular time [6]. Applicants also will be required to pay the fee in cashier's check, money order or credit card. Employers with a large number of workers are encouraged to volunteer to host a mobile enrollment site. The TSA will notify the applicant when the credential is ready for pickup and what processes are necessary to activate the TWIC. Trusted Agents, who work for the center, assist applicants and confirm that the documents provided match the identity of the individual, are certified, and valid. They verify applicant’s information and collect the applicant biometric samples, electronic signature, and digital photograph. Once collection is complete, all applicant enrollment information are

encrypted and securely transmitted to IDMS. By design, and for security and privacy reasons, no enrollment data is stored at the local facility level [7].

Enrollment Processing

Once all of the biographic and biometric data has been collected and sent to the IDMS, enrollment processing is initiated. This consists of:

- 1: N duplicate check against TWIC fingerprint database. Identify Subject and Add Subject to Gallery.
- Watch list (and/or other threat screening) check. Identify Subject (if performed locally).
- Criminal History Records Check (external interface to FBI IAFIS)
- Name-based checks (external)

The Identity Management System (IDMS)

The Identity Management System (IDMS), the process of validating, capturing, storing, securing, maintaining, and matching an individual's identity, securely managed all aspects of individual enrollment record information in the TWIC system. IDMS was designed and operated by TSA to store applicant enrollment, but was physically located in a federal facility with a secure logical and physical security. Although IDMS was not designed to process classified information, it benefices from the heavy sensitive security controls required to process classified data within this secure facility and stores volunteer applicant enrollment records. All enrollment record information, stored in an encrypted format, is composed of three components of information: biometric images, biometric templates and personally identifiable information. For additional protection, IDMS will store each of these three information components separately to prevent the entire enrollment record from being violated by intruders. As a result, access to any of the three information components or the entire enrollment record will be limited to those with a need to access the information and would yield to worthless information since it is encrypted for any intruders [3].

Security Threat Assessment

Security Threat Assessment (STA), conducted by TSA, includes checks against criminal history records, terrorist watch lists and immigration databases. The biographical information collected from volunteer applicants during pre-enrollment and enrollment are formatted and sent via secure password protected e-mail to TSA employees in order to run the terrorist databases that TSA maintains. TSA uses the applicants' biographic and biometric information, housed in TSA's Technology Infrastructure Modernization system, to correlate against four databases to check for criminal, immigration, and terrorism-related offenses that could preclude the applicant from obtaining a TWIC. Under TWIC regulations at 49 Code of Federal Regulations (CFR) 1572.5(a), TSA determines that an applicant poses a security threat and may deny a TWIC if [1]:

- The applicant has a disqualifying criminal offense described in 49 CFR 1572.103. Per the regulations, there are 12 permanently disqualifying and 15 interim disqualifying offenses. Appendix C provides the list of disqualifying offenses TSA uses.
- The applicant does not meet the immigration status requirements described in 49 CFR 1572.105.
- TSA conducts the analyses described in 49 CFR 1572.107 and determines that the applicant poses a security threat.
- The applicant has been adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109.

Any individual who meets the minimum criteria established by TSA as a possible match undergoes an extensive review by agency personnel. TSA uses this deep analysis and screening process to determine the level of security threat posed by the individual. A determination that someone poses or is suspected of posing a security threat is only made after a review by the Director of the Credentialing Program Office (CPO) who conducts the final review. The purpose of this process is to protect applicants from being incorrectly identified as a threat and to minimize the number of false positives errors. After this review, the name of any TWIC applicant posing or suspected of posing a security threat is then forwarded to the appropriate law enforcement or intelligence agency. TSA continues this process by conducting security threat assessments on individual issued TWIC cards on an as needed basis for security purposes. If no adverse information is disclosed, TSA typically completes a security threat assessment in less than 10 days. However, processing time increases for an applicant with a criminal history or other disqualifying information, and is further lengthened if the applicant initiates an appeal or waiver. This security threat assessment is the same for those applying for, transferring, or renewing a HAZMAT endorsement (HME) on their state-issued commercial drivers licenses (CDLs). If TSA determines that an applicant poses an imminent threat to transportation or national security, TSA may notify the applicant's employer. Generally, TSA will not provide the reasons for a disqualification to an employer [2]. However, if TSA has reliable information concerning an imminent threat posed by an applicant and providing limited threat information to an employer, facility, vessel owner, or Coast Guard Captain of the Port would minimize the risk, then TSA would provide such information.

Background Check Process

To perform the background check and complete its analyses, TSA compares the applicant's information, saved on IDMS, against four main systems. These systems include [8]:

1. Federal Bureau of Investigation's (FBI). Next Generation Identification System that provides criminal history information. The FBI deployed the FBI Next Generation Identification Rap Back. The Rap Back Service provides authorized agencies with notification of criminal and, in limited cases, civil activity of individuals that occurs after the initial processing and retention of criminal or civil transactions. The Rap Back Service implements new response services to notify agencies of subsequent activity for individuals enrolled in the service. This feature provides a more timely process of confirming suitability of those individuals placed in positions of trust and notifying users of criminal activity for those individuals placed on probation or parole.
2. U.S. Citizenship and Immigration Services (USCIS). Systematic Alien Verification for Entitlements to verify lawful immigration status.
3. TSA's Transportation Vetting System, which matches an applicant's information against select terrorist watch lists, U.S. Marshals Wants and Warrants, and Office of Foreign Asset Control persons of interest.
4. The Automated Biometric Identification System (IDENT) for a biometric and fingerprint-based check against information provided by DHS, the Department of State, the Department of Justice, and the Department of Defense.

Approximately 40 percent of all applications trigger no matches against any of the data systems screened. For those applications, the TSA automated information system electronically adjudicates and approves the file. Electronic adjudications take approximately 1 to 39 days to reach a decision. The remaining 60 percent of the applications may match one or more databases and require a manual review. Adjudicators in the Security Threat Assessment Operations Adjudication Center conduct the manual adjudication. They are Federal employees trained to review each piece of information available and determine whether to grant or deny a TWIC. They also process waivers and appeals. Manual adjudications typically apply to cases that are more complex. Based on our review of 235 manually adjudicated cases, adjudicators may take up to 140 days to reach a decision [1]. Upon successful completion of the STA and applicant eligibility is approved, TSA's automated information system sends a signal to the Government Publishing Office to issue the TWIC. The TWIC is personalized by the centralized card production facility and shipped to the applicant's enrollment center. Applicant will be notified when the credential is ready to be picked up. Applicant returns to enrollment center to claim credential for use at MTSA regulated vessels, facilities, and OCS facilities. However, when adjudicators determine that the applicant is not eligible to receive a TWIC (or poses an imminent threat to the transportation system or national security), they issue a denial letter. Applicants may request a waiver or appeal of the TSA decision. TSA may notify the applicant's employer. Generally, TSA will not provide the reason for a disqualification to an employer. However, if TSA has reliable information concerning an imminent threat posed by an applicant and providing limited threat information to an employer, facility, vessel owner or Coast Guard Captain of the Port would minimize the risk, then TSA would provide such information [2].

Card Production and Personalization

Once successfully completed the applicant threat assessments, enrollment data is placed into a card format for card production. The information are then encrypted and transmitted to a secure DHS federal card production facility that operates in agreement with TSA. The card production facility conducts an electronic quality control check on enrollment record to ensure it arrived from an authorized enrollment center or an authorized user, and that the enrollment record was not modified or compromised in transmission. If the enrollment record is received intact, an electronic acknowledgement of receipt is sent to IDMS, and used to update the enrollment record to reflect current status. If the enrollment record does not pass the technical quality control check upon receipt at the card production facility, the applicant enrollment record is rejected and IDMS is notified [1]. Then the originating enrollment center is electronically notified of the anomaly for resolution. IDMS re-sends the completed enrollment record to the card production facility and the applicant enrollment record is updated. The resolution of this situation will not affect the applicant. Applicants information printed on the TWIC are the applicant name and photograph. Other information are securely stored on the card integrated circuit chip (ICC) for identity verification purposes. The information stored on the card includes biometric templates, name, biometric samples (i.e. fingerprint or iris scan), digital photograph, unique card serial number, and unique card number for the cardholder. The biographical information is electronically copied between the card surface during printing and the ICC to enhance the chain of trust between the chip, the card and the individual. Then the TWIC system compared the printed information to the electronic information to ensure that all elements matched before the credential is considered valid. Once the applicant TWIC is produced, it pursues a card quality assurance check at the card production facility to ensure that all technologies and card security features work properly. If the card does not pass the quality control check, it is physically destroyed in a secure process by the card production facility and the data was re-entered into the card production process until the final product passes quality control standards [3]. If the card passes the quality control check, the card ICC is electronically "locked" to prevent any information from being disclosed without it first being "unlocked" by the applicant in combination with the TWIC Trusted Agent at the enrollment facility. The card is ready for shipment once electronically locked, but not yet activated for access to secure areas. The electronically locked card is securely

shipped by the production facility to the originating enrollment center for issuance to the volunteer applicant. IDMS is notified electronically by the card production facility that the card has been completed and shipped, and the enrollment record is updated to reflect the most current status of the enrollment record. At this point, the applicant electronic enrollment record at the central card production facility is destroyed. The card production facility does not retain any personal records; therefore, the risks of physical security are mitigated by the fact that enrollment information was not retained at the facility. Once IDMS receives the "card complete" notice from the card production facility, the enrollment record is updated to reflect the most current status. Once the card is received at the local facility enrollment center, the applicant is scheduled and notified to report to the enrollment center through the means requested by the applicant during enrollment. The notification methods may include electronic mail or phone call [5].

Card Issuance

Issuance commences when the applicant arrives at the designated enrollment center. In the presence of a TWIC Trusted Agent, the individual performs a biometric verification with the index fingers to verify identity, unlock and activate the TWIC, and complete the issuance process. This personal protection mechanism for activation provides stronger security assurances than typical protections such as Personal Identification Numbers or passwords. Once the transportation worker has been issued a TWIC, IDMS is updated to reflect that the credential has been issued. As previously mentioned, the issued TWIC cannot be used for access to secure areas until activated at the participating location, by the local facility operator. Once the cardholder is in possession of his or her TWIC, the cardholder next step is to request access to a participating local facility [1].

Privilege Granting

When a TWIC cardholder needs to gain local access privileges with an issued TWIC, the local facility used the local TWIC device reader (a computer owned and maintained by TSA) connected directly to IDMS through a secure web portal. Access privileges are granted upon: confirmation that the issued TWIC is still a valid card (by checking the card unique serial number in IDMS), and verification of the identity of the person holding the card (by using the biometric template stored on the card to match the cardholder index finger). As a result, IDMS is notified that the local facility has granted the TWIC card holder local access privileges [1]. The TWIC device does not store any biographical or biometric information and simply acts as a tool to exchange information between itself and IDMS. Local access control is granted or denied by comparing card numbers registered in the local access control system against the one presented by the cardholder at the time of attempting access. If the card presented to the electronic reader at the local facility is registered in the local access control system, then access is granted. If the card number is not matched, then the cardholder must contact the facility operator for resolution. Although the TWIC card verifies that the holder is not a security risk, local facilities, not TSA, have full control over who has authorized access to their secure areas. They retain authority to grant or deny access to employees and people who require access to the facility.

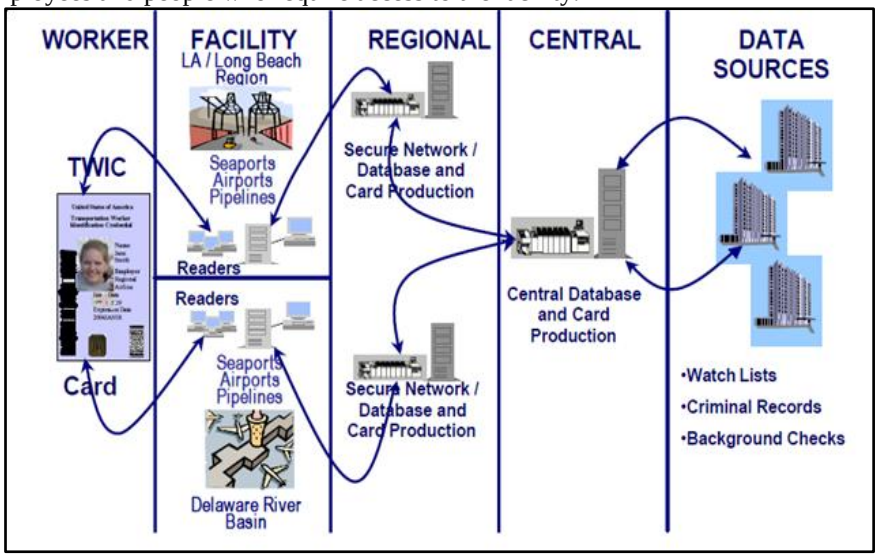

Fig. 6 TWIC System Components

Card Revocation

Revocation of the card may be necessary for a variety of reasons, such as a lost, stolen, deactivated, or otherwise unusable card. Revocation may occur by "hot-listing" the card using the card unique serial number. "Hot-listing" is a term of art used to describe cards that should not be used for unescorted access to secure areas. If the card is determined to be invalid, the cardholder must report to the enrollment center for resolution or re-issuance of a new card [3].

Appeals and Waivers Process

Applicants who are denied a TWIC will be notified of the reason for denial and instructed on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes, or if they are aliens in Temporary Protected Status. Applicants who seek a waiver and are denied may seek review by an Administrative Law Judge (ALJ). The applicant has 60 days from the time they receive a Final Determination of Threat Assessment to provide the required information to TSA for consideration [2].

INTERNAL CHALLENGES

TSA Challenges

An audit conducted by the OIG [9] shows that TSA's leadership, responsible for issuing Transportation Worker Identification Credentials (TWIC), does not provide sufficient oversight and guidance to ensure that the TWIC program operates effectively. Specifically, within the background check process, which TSA calls the security threat assessment:

- Fraud detection techniques are not monitored and used in completing the background check;
- Adjudicators may grant TWICs even if questionable circumstances exist;
- Key quality assurance and internal control procedures are missing from the background check and terrorism vetting processes; and
- New efforts tested for continuous vetting for disqualifying criminal or immigration offenses lack measures to determine the best solution.

The audit concludes that these issues exist, in part, because TSA leadership relies on the TWIC program office to implement necessary improvements while the TWIC program office focuses more on customer service than effectiveness of the program. Additionally, TSA organizational structure poses a problem. The TWIC program office lacks visibility into and authority over the other offices within TSA that support the TWIC program. As a result, there is a risk that someone with major criminal or immigration offenses maintains access to secured areas of maritime facilities.

Coast Guard Challenges

As of September 28, 2018, the Office of Inspector General (OIG) [4] conducted an audit to determine the extent to which the Department of Homeland Security completed an assessment of the security value of the Transportation Worker Identification Credential (TWIC) program as required by Public Law 114−278, Section 1(b). OIG also determined the extent to which the United States Coast Guard's (Coast Guard) oversight of the TWIC program ensures only eligible individuals are granted unescorted access to secure areas of regulated facilities. The result shows that:

- The Coast Guard does not have a full understanding of the extent to which the TWIC program addresses security risks in the maritime environment.
- Lack of oversight and poor coordination. The Coast Guard needs to improve its oversight and coordination of the TWIC program to reduce the risk of transportation security incidents.
- Delays regarding developing and implementing card reader technology have meant that for the initial period TWIC cards will not be used in card readers [10]. Therefore a person with an invalidated TWIC card may still be able to gain un-escorted access to facilities and vessels due to an inability to verify cards on site [11].
- Due to U.S.C.G. Policy, persons can still gain access to facilities and vessels without possessing a TWIC card, for up to 30 days, if their employer applies to the TSA (Online) for such a temporary exemption. The employee then carries a print out of their approval along with State issued ID such as a driver license. There is no provision for validation of this printed document but the employee is required to have escorted access which allows entry but prohibits them from certain areas without another employee escorting them [7].
- Due to technical problems and lack of awareness of procedures, the Coast Guard did not make full use of the TWIC card's biometric features as intended by Congress to ensure only eligible individuals have unescorted access to secure areas of regulated facilities.
- The Coast Guard only used electronic readers to verify, on average, about 1 in every 15 TWIC cards against the Transportation Security Administration's canceled card list. This occurred because the majority of the TWIC readers in the field have reached the end of their service life.

EXTERNAL CHALLENGES

Significant Delays

According to a report by the National Employment Law Project, some TWIC applicants have experienced significant delays. Specifically, many applicants that receive initial denials based on background check returns face waits of six to eight months to complete the process to obtain a TWIC. Over 10,000 applicants out of the 1.5 million port workers could not work for an average of 69 days because they had not obtained a TWIC by the implementation date [12].

Defective TWIC Cards

In November, 2011, the TSA announced that approximately 26,000 TWIC cards issued before April 5, 2011 would not work when inserted into a TWIC card reader. Each card contains a Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card in Federal databases, encoded on its ICC. On the faulty cards, the FASC-N has not

been fully encoded, causing the readers to view the card as an invalid card. The agency has posted a list online with the serial numbers of affected cards. They say that they will replace the faulty cards at no further cost to the affected individual [13].

Program Cost

Critics assert that the program has cost over $420 million and has little to show for it [7]. The General Accounting Office (GAO) report found the TWIC card reader pilot program results to be unreliable and questioned the program's premise and effectiveness in enhancing security.

Supply Chain

TWIC has a positive impact on supply chain. Ports, waterways, and vessels handle billions of dollars in cargo annually. Ports are susceptible to terrorist attacks because of their size, general proximity to metropolitan areas, volume of cargo being processed, and link to the global supply chain. Securing transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy. In addition to other security methods involved, business managers adopting the heavy TWIC security system are able to reduce and prevent the vulnerability observed in the supply chain nationwide. Therefore, tightened together to the TWIC, these securities measures help securing the supply chain from the beginning to the end and ensuring that no information and components are compromised.

Small Businesses Protection

Measures are in place to protect small businesses, such as small passenger vessels. TSA and the Coast Guard worked with the Small Business Administration to minimize adverse financial and operational impacts on small businesses wherever possible. The rule includes provisions that allow MTSA -regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. Employee access areas are typically include locations where waiters, entertainers and galley staff work and live. This provision reduces the impact on employees who rarely need to use spaces beyond those designated for support of passengers, while maintaining the integrity of a vessel's secure areas.

Privacy Concerns

How someone knows its personal information is safeguarded? Privacy and the security of personal information are critical to the TWIC program. Information collected at the enrollment center or during the pre-enrollment process is scanned into the TWIC system for the security threat assessment process. To ensure privacy is protected, applicant data is encrypted and stored at a secure government facility using methods that protect the information from unauthorized retrieval or use. Privacy groups like the Electronic Privacy Information Center (EPIC) understand that information collection may be necessary to ensure that those with ill intent do not gain access to the transportation infrastructure. However, they required TSA to take into consideration the privacy interests of the participants. They should take great care to guard the collected information from excessive use, misuse, or even use in furtherance of a terrorist act. Given that TSA, for the TWIC program, gather highly sensitive personal information about a large number of people directly related to the U.S. transportation industry, EPIC requested that the program authorities observe the obligations stated in the Privacy Act. The Privacy Act objective is to guard citizen privacy interests against government intrusion [14].

Biometric Reliability

Another concern is the biometric technology, the driver behind the TWIC program. The biometric technology is defined as a measurable characteristic or behavioral trait of a live human being that can be used to automatically recognize or verify identity. The two main types of biometrics are physical and behavioral. A physical biometric is a part of a person body, such as fingerprint or hand shape. A behavioral biometric is something that a person does, such as signing or typing. Humans are born with physical characteristics, but behavior characteristics are developed over the time and can be unique and constant, which makes them ideal biometrics. Since biometric data can never be revoked, there are concerns about the protection of biometric data itself. The usage of biometric carries its own risk of security and privacy invasion [15]. Despite the fact that the biometric stored on the TWIC card cannot be stolen, someone biometric template can be stolen by computer hacker or misused by the owner of the system regardless of the safeguards system in place. Also, the method of acquisition of the biometric can allow a malicious individual to attack the security of the biometric system, by interfering with the capture mechanism or by substituting biometric data. Spoofing is a class of attack on a biometric security system where a malicious individual attempts to circumvent the correspondence between the biometric data acquired from an individual and the individual themselves. The exact techniques for spoofing vary depending on the particular types and devices of biometric involved. Typical spoofing techniques involve the use of a dummy silicone fingers, the fake fingerprint based on a gelatin mold and the fake biometrics to confuse the biometric devices [16].

CONCLUSION

The general idea behind the TWIC program is that all transportation workers throughout the USA (workers at air and sea ports, public transit facilities, highway, railroad and pipeline workers, truckers, and operators of any vehicle carrying passengers for hire) would have their biometric data recorded in a central database and be issued a single machine readable card which would be used to control access to all transport facilities. The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) jointly administer the TWIC program. TSA ensures that the identity and information of each TWIC cardholder has been verified; that a threat assessment has been completed on that identity; and that each credential issued is linked to the correct holder through the use of biometric technology. The Coast Guard verify TWIC when conducting vessel and facility inspections and during spot checks using hand-held scanners, ensuring credentials are valid. The program provides a Smart Card, about the size of a credit card, and contains a computer chip (an Integrated Circuit Chip (ICC)), which stores the individual information and biometric data. To obtain a TWIC, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph and successfully pass a security threat assessment conducted by TSA. Vulnerabilities in the TWIC background check process inhibit TSA from providing assurance that individuals with unescorted access to secure maritime facilities have not committed disqualifying criminal or immigration offenses and continue to be eligible. The Coast Guard needs to improve its oversight of the TWIC program to reduce the risk of transportation security incidents. Due to technical problems and lack of awareness of procedures, the Coast Guard did not make full use of the TWIC card's biometric features as intended by Congress to ensure only eligible individuals have unescorted access to secure areas of regulated facilities. In addition, we found the following external challenges: significant delays, defective TWIC cards, program cost, supply chain, small businesses protection, privacy concerns and biometric reliability. Although the TWIC is a powerful security tool, the widespread of detailed information collected by TSA poses the direct risk. Information of participants, in the wrong hands, could enable precisely the safety threat that the program seeks to prevent. EPIC and other privacy groups are closely watching its implementation. Despite the fact that the biometric stored on the TWIC card cannot be stolen, someone biometric template can be stolen by computer hacker or misused by the owner of the system regardless of the safeguards system in place. The method of acquisition of the biometric can allow a malicious individual to attack the security of the biometric system, by interfering with the capture mechanism or by substituting biometric data. Potential attack, called spoofing, is used to break biometric devices to violate the integrity of the system.

REFERENCES

[1]. Transportation Security Administration, Frequently Asked Questions, Web. https://web.archive.org/web/20140810125731/http://www.tsa.gov/stakeholders/frequently-asked-questions-0, 2014.
[2]. Teamsters, Transportation Worker Identification Credential (TWIC), Web. https://teamster.org/transportation-workers-identification-credential-twic-program, 2017.
[3]. General Accounting Office (GAO), Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable, Security Benefits Need to Be Reassessed, Web. https://www.gao.gov/mobile/products/GAO-13-198, 2013.
[4]. Transportation Security Administration, TWIC Card and Reader Technology, Web. https://www.tsa.gov/for-industry/twic-card-reader-technology, 2014.
[5]. Office of Inspector General (OIG), Review of Coast Guard's Oversight of the TWIC Program, Web. https://www.oig.dhs.gov/assets/Mgmt/2018/OIG-18-88-Sep18.pdf, 2018.
[6]. S Parsons, Transportation Worker Identification Credential (TWIC), Web. https://www.aapa-ports.org/files/SeminarPresentations/05_Security_Safety_Parsons_Steve.pdf, 2005.
[7]. A Lipowicz, GAO despite advances, TWIC problems remain, Web. https://web.archive.org/web/20070430192515/http://www.gcn.com/online/vol1_no1/43463-1.html, 2007.
[8]. Automated Biometric Identification System (IDENT), Encyclopedias, Web. https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/ident-automated-biometric-identification-system?, 2004.
[9]. Office of Inspector General (OIG), TWIC Background Checks are not as Reliable as They Could Be, Web. https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-128-Sep16.pdf, 2016.
[10]. A Lipowicz, Delay of Game. More problems beset DHS' beleaguered TWIC program, *Washington Technology*, 2017, 22 (4)
[11]. Department of Homeland Security (DHS), Privacy Impact Assessment (PIA) for the Reader Requirements for U.S. Coast Guard, Web. https://www.dhs.gov/sites/default/files/publications/pia-19-uscg-twicreader-PIA-20130325_0.pdf, 2013.
[12]. D Krapf, TWIC Is Still Useless and a big waste of money, Web. https://web.archive.org/web/20141022024128/http://www.workboat.com/blogpost.aspx?id=15526, 2014.
[13]. D Bryant, Maritime Security & The Useless TWIC, Web. https://www.marinelink.com/news/maritime-security-useless344893.aspx, 2012.

[14]. R Clarke, Cryptography in Plain Text, *Electronic Privacy Information Center-Privacy Law and Policy Reporter*, 1998, 3(2), 24-27. Web. http://www.epic.org/privacy/ssn, 1998.
[15]. L Thalheim, J Krissler & PM Ziegler, Body Check - Biometric Access Protection Devices and their Programs put to the test, *c't Magazine*, 114, 2002.
[16]. T Matsumoto, Gummy and Conductive Silicone Rubber Fingers: Importance of Vulnerability Analysis, *In Y. Zheng (ed.) Advances in Cryptology - ASIACRYPT 2002, Queenstown, New Zealand*, 2002, 5, 574-575.