TWIC Pilot Test Reader Usage Scenarios

Version 1.1
February 2, 2009

Purpose:

The purpose of this document is to describe usage scenarios for exercising and gathering data from card readers capable of reading the Transportation Worker Identification Credential (TWIC). Information gathered from these scenarios is intended to meet the requirements of the SAFE Port Act of 2006 which required a pilot program to test the business processes, technology, and operational impacts of deploying TWIC readers to control access to secure areas of Maritime Transportation Security Act regulated vessels and facilities.

This document is intended to be shared with all pilot test participants as well as other parties interested in the TWIC pilot program.

Application:

Recognizing that the ports, facilities, and vessel operators participating in the TWIC pilot do so voluntarily, the application of the scenarios described in this document are intended to represent a goal. The number of pilot test participants will provide redundancy if we cannot gather data for some of the listed scenarios as planned. These scenarios will overlay the specific TWIC reader installation plans for each facility or vessel to fully describe the reader or physical access control system (PACS) usage during the pilot. Detailed test plans will then be completed which will describe how, when, and where data will be gathered in support of the pilot.

Activities covered by these scenarios include obtaining and evaluating:
- Baseline facility or vessel access data;
- TWIC reader functionality in four different processes;
- Accessing card information (name, expiration, and digital photo) using a PIN;
- Maintaining and updating invalidated card information (i.e., "hotlist" and/or Certificate Revocation List); and,
- Maintaining and exporting card reading and/or access control log information.

Access Point Test Processes:

PROCESS 1: VISUAL CARD INPECTION (BASELINE)
- Identity Verification[1]: One factor.
- Card Verification[2]: Visual only.
- Card Validity ("hotlist" check)[3]: Not possible.
- Process: Guard verifies visible card security features in accordance with TWIC rule requirements.

PROCESS 2: CHUID[4] + VISUAL CARD INSPECTION
- Identity Verification: Visual only.
- Card Verification: "One Plus" factor (CHUID alone does not verify the card). Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user's CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from a TWIC card
- Card Validity ("hotlist" check): Possible.
- Process:
  - Present card to reader; TWIC Applet is selected
  - Reader verifies the CHUID signature
  - Reader decodes the FASC-N TLV[5] record and extracts the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue
  - The TWIC reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N.
  - The FASC-N is checked against the hotlist
  - The guard verifies the transaction success and compares card surface facial photo to card presenter

PROCESS 3: CHUID + BIOMETRIC VERIFICATION
- Identity Verification: Two factor.
- Card Verification: "One Plus" factor (CHUID alone does not verify the card). Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user's CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from a TWIC card
- Card Validity ("hotlist" check): Possible.

---

[1] Total number of distinct assurances of an individual's identity.
[2] The determination of whether the card is a TWIC and can be trusted (i.e., not counterfeit or cloned).
[3] Determination that the card has not been revoked or reported lost or stolen.
[4] Card Holder Unique Identifier (CHUID)
[5] "Type-Length-Value" (TLV); a data element field within a protocol

- ▪ <u>Process</u>: The biometric reference template may be read from a TWIC card at each use or stored in the PAC system during PACS registration of the user. This will verify the authenticity of the fingerprint match to the TWIC holder
  - o Present card to reader and TWIC Applet is selected
  - o TWIC reader verifies the CHUID signature
  - o TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the magnetic stripe of a TWIC card, or the contact interface of a TWIC card.
  - o TWIC reader gets the contents of the fingerprint data object and CHUID.
  - o The enciphered fingerprint template is deciphered using the TWIC Privacy Key.
  - o TWIC reader verifies that the digital signature on the CBEFF[6] record was produced by an authorized document signer.
  - o A finger is sampled from the cardholder. If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number.

PROCESS 4: CHUID + BIOMETRIC VERIFICATION + CARD AUTHENTICATION

- ▪ <u>Identity Verification</u>: Three factor (same as for a Federal government PIV card).
- ▪ <u>Card Verification</u>: Card is verified through a digital signature check.
- ▪ <u>Card Validity (CRL, or "hotlist" check)</u>: Performed through the Certificate Revocation List (CRL) card authentication process; or hotlist check.
- ▪ <u>Process</u>:
  - o TWIC reader selects the PIV Applet.
  - o TWIC reader follows the challenged response sequence outline in the reader specification in Appendix A2 page 47.
  - o TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the magnetic stripe of a TWIC card, or the contact interface of a TWIC card.
  - o TWIC reader gets the contents of the fingerprint data object and CHUID.
  - o The enciphered fingerprint template is deciphered using the TWIC Privacy Key.
  - o TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer.

---

[6] Common Biometric Exchange File Format (CBEFF)

       o A finger is sampled from the cardholder. If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number.

Hotlist Download Test Process:

If a TWIC's validity is established by comparing the FASC-N segment of a card's CHUID to the FASC-N segment on the hotlist, the hotlist must first be downloaded from the TWIC hotlist website. The hotlist is only as current as the last time the hotlist was downloaded for use by a PACS. Since the maximum interval between hotlist updates is anticipated to be covered in the final TWIC reader rule, pilot test data must be obtained regarding the effort involved in downloading the list so that the interval chosen is justified by the benefits derived from the effort required. Therefore, pilot test participants will be asked to download the hotlist at various intervals to obtain this data. The following paragraph describes the hotlist download requirements and proposed download intervals.

> **HOTLIST DOWNLOAD**: Reader transactions that incorporate a check against the hotlist are performed either at the PACS or the reader**.** The hotlist shall be loaded into the TWIC reader or PACS at different intervals to assess the impact of updating the information on both portable and fixed TWIC readers. The download frequency should be tested at daily, 72 hours; weekly; or, based on a situation (i.e., change in MARSEC level). It is assumed that network attached fixed readers will be automatically updated at the frequency specified. (Note: the hotlist itself is updated daily).

Log Keeping:

Most TWIC readers retain the data needed to produce a log of times of verification, name, etc. Since it is possible that the TWIC reader rule will require that the owner / operator produce a log of when identity was verified we are considering recording names, CHUIDs, dates, and times of those individuals granted unescorted access to MTSA regulated vessels and facilities. Additionally, owners and operators opting to use recurring unescorted access should consider recording names of the persons to whom recurring unescorted access has been granted. This activity has been included in certain scenarios.

PIN Use:

Since TWIC holders are likely to be required to occasionally use the Personal Identification Number (PIN) checking this function is included in the scenarios.

TWIC Reader Test Scenarios

Attachment 1 and Attachment 2 to this document describe the test scenario goals for each facility and vessel operation participating in the TWIC pilot.

Attachment 1 is a table listing each test facility and vessel operation and the reader test processes and hotlist update intervals that the government wishes to evaluate. The proposed timeframe for each test is also listed.

Attachment 2 provides specific scenario descriptions for each of the vessel operations in the TWIC pilot. Because most vessels do not have defined access points, and because the use of readers between passenger access areas (i.e., non-secure) and secure or restricted areas aboard vessels, such as the pilot house or engine room, is not realistic, more specific guidance is required to accomplish test goals.

Attachment 1: TWIC Pilot Test Facility and Vessel Operation Master Test Scenario Plan

Attachment 2: TWIC Pilot Test Vessel Operation Test Scenario Detailed Plan

TWIC Pilot Test Facility and Vessel Operation
Master Test Scenario Plan

The following table shows the projected test scenarios for each facility or vessel operation participating in the TWIC pilot test. Most of the test scenarios have a goal of testing readers in more than one of the reader processes described in detail the TWIC Pilot Test Reader Usage Scenarios. The processes are:

        Process 1—Visual Card Inspection
        Process 2—CHUID + Visual Card Inspection
        Process 3—CHUID + Biometric Verification
        Process 4—CHUID + Biometric Verification + Card Authentication

Process 1 is the baseline process and therefore is not listed separately in the test scenarios for readers.

Also included in the table are hotlist download intervals proposed for evaluation at each facility.

Definitions of terms used in Table 1. :

        Every entry.................Verify the identity of every worker entering the secure area using the method specified for the reader process indicated.
        Randomly...................On a randomly selected day within the time period specified (i.e., once every two weeks; monthly; etc.) verify the identity of every worker entering the secure area using the method specified for the reader process specified for the time of the random check. On all other days during the period identity must be verified using the procedures required by the visual enforcement regulation.

Table 1: TWIC Master Scenario Plan

Port or Vessel	Facility	Reader Process To Be Tested	Frequency of Reading TWIC	Hotlist Download Frequency	Comment
Los Angeles	Vopak Terminal	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Pacific Cruise Ship Terminal	3	Every entry; except baggage handlers—once at beginning of each shift.	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Same; plus randomly once every two weeks for one month.		
	Eagle Marine Services / American President Lines (APL)	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Same; plus randomly once every two weeks for one month		

Port or Vessel	Facility	Reader Process To Be Tested	Frequency of Reading TWIC	Hotlist Download Frequency	Comment
Long Beach	Total Terminals International (Hanjin)	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Stevedoring Services of America (SSA) Terminal—Pier A	3	Every entry	Test weekly download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	BP Pipelines Terminal	4	Every entry; plus randomly once every two weeks for one month.	Daily	Produce reader log(s) for facility at period to be specified.
	California United Terminals (CUT)	3	Every entry	Test daily download; and 72 hour interval download	CUT's participation depends on availability of POLB PSG funds.
		4	Every entry; plus randomly once every two weeks for one month.		
	Sea Launch Facility	4	Every entry; plus randomly once every two weeks for one month.	Daily	Produce reader log(s) for facility at period to be specified.
	Metropolitan Stevedore Berth 212	2	Every entry	Weekly	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Catalina Express* --San Pedro, Berth 95 --Long Beach; Queen Mary and Catalina Landing * Details are in Attachment 2	2	Check every TWIC-holding employee periodically. Produce log. Check TWIC-holding crew (master; engineer) prior to first embarkation daily.	Weekly	Produce reader log(s) for facility at period to be specified.
		4	Same as above; plus randomly once every two weeks for one month.	Test daily download; and 72 hour interval download	

Port or Vessel	Facility	Reader Process To Be Tested	Frequency of Reading TWIC	Hotlist Download Frequency	Comment
Brownsville	Harbor Master's Office	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Transmontaigne (Oil)	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Interlube (Side gate)	4	Every entry; plus randomly once every two weeks for one month	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
	Oil Dock 5, 3	4	Every entry; plus randomly once every two weeks for one month	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
	Dock 10, 11, 12, 13, 15	2	Every entry; plus randomly once every two weeks for one month.	Weekly	Produce reader log(s) for facility at period to be specified.
		3	Every entry	Daily	

Port or Vessel	Facility	Reader Process To Be Tested	Frequency of Reading TWIC	Hotlist Download Frequency	Comment
New York / New Jersey	APM	3	Every entry	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month.		
	Maher Terminal	4	Every entry; plus randomly once every two weeks for one month.	Test daily download; and 72 hour interval download	Produce reader log(s) for facility at period to be specified.
	Berth 23 and 25 (Roll-on; roll-off operation)	3	Every entry; plus randomly once every two weeks for one month.	Weekly	Produce reader log(s) for facility at period to be specified.
		4	Every entry; plus randomly once every two weeks for one month	Weekly	
	Berth 10 and 12 (Public Port Authority Docks)	2	Every entry; plus randomly once every two weeks for one month.	Weekly	Produce reader log(s) for facility at period to be specified.
		3	Every entry; plus randomly once every two weeks for one month.	Weekly	
Staten Island Ferry	St. George Terminal; Staten Island See details in Attachment 2	2	Every entry	Weekly	Note: Access / check points are prior to boarding ferries. Portable readers may be used aboard the ferries for periodic random checks. Produce reader log(s) for facility at period to be specified.
		3	Every entry	72 hrs.	
		4	Every entry; plus randomly once every two weeks for one month	Daily	

Port or Vessel	Facility	Reader Process To Be Tested	Frequency of Reading TWIC	Hotlist Download Frequency	Comment
Magnolia Marine Transport	CATHERINE BERRY (Towboat)	3	Upon every embarkation (when vessel is a secure area due to cargo) <u>unless</u> operating under Recurring Access procedures. See details in Attachment 2.	TBD based on portable reader capability.	Master or designated Security Officer will conduct TWIC checks. Recurring Access procedures may apply.
		4			
	DOROTHY LEE (Towboat)	3			
		4			
	Vicksburg Administrative Office	4	Check every TWIC holding employee at least once each quarter. Verify that checks were done aboard vessel for remote crew members.	Weekly	Produce reader log(s) for facility at period to be specified.
Watermark Cruises	Administrative Office See details in Attachment 2.	2	Check every TWIC-holding employee at least once each week. Check TWIC-holding crew (master; engineer) prior to first embarkation daily	Weekly	Designated Security Officer will conduct TWIC checks. Recurring Access procedures may apply.

Produce reader log(s) for facility at period to be specified. |
		3		Daily	
		4		72 hrs	
	Annapolis City Dock See details in Attachment 2.	2	Check every TWIC-holding employee at least once each week. Check TWIC-holding crew (master; engineer) prior to first embarkation daily	Weekly	
		3		Daily	
		4		72 hrs.	

TWIC Pilot Test <u>Vessel Operation</u> Test Scenario Detailed Plan

Verification of the identity of vessel crews using card readers presents a unique challenge because:

(1) Except for very large cargo or passenger vessels there are no access points through which all personnel must pass. This makes fixed readers, or gates, impractical or impossible.

(2) Crews must often pass between public or non-secure spaces and secure or restricted spaces, thereby making the use of readers on vessel doors or hatches—such as access to the pilot house or engine room—impractical. Furthermore, readers with interlocks to these spaces would create an unacceptable safety risk.

(3) TWIC-holding crew members and non-TWIC holding crew members as well as passengers embark using the same access points and are intermingled in public access and non-TWIC crew areas. This further complicates the use of readers for access control aboard vessels.

During the TWIC pilot we will explore several procedures for verifying crew identities using portable and fixed TWIC readers. Identity verification will be evaluated using two procedures, varying them as necessary for each vessel's operating environment.

(1) <u>Periodic Administrative Identity Verification</u>: Vessel owners / operators will verify that TWIC-holding crew members and employees possess a valid TWIC at least once during a specified period. This could be accomplished in any location. The verification in this case is not tied to granting access on a specific occasion such as embarking a vessel. Vessel owners / operators will be required to keep a log of when the checks were accomplished. (Most reader can store the information necessary to produce the log). For example, if identity verification were required once a month, at sometime during each month each TWIC holder must present their card for verification using the process being tested at the time, and a record acceptable to the Coast Guard maintained. The procedure requires that means other than verifying a TWIC is used to ensure that only TWIC holders have access to areas of the vessel where a TWIC is required. Locks, keys, guards, spot checks, etc. that are normally used in operating the vessel would continue to be used in this scenario.

In this scenario portable readers could be used, or fixed readers in a location convenient to crews, such as administrative offices, or a time-clock station, could be used.

(2) Embarkation Identity Verification: Vessel owners / operators will verify that TWIC-holding crew members and employees possess a valid TWIC prior to, or at the time of, embarking the vessel. A guard or the operator's security officer will verify identity at a point where it can be assured that the crew member completes the check. For vessels operating independently the master or designated security officer will ensure the checks are completed.

In most cases portable readers will be required to complete an Embarkation Identity Verification.

As the TWIC pilot progresses other identify verification procedures may be developed and tested.

Specific Vessel Operation Scenarios:

Catalina Express:

Locations:
(1) Berth 95 San Pedro Terminal; Administrative Office
(2) Catalina Landing Terminal; Long Beach; Administrative Office
(3) Queen Mary Terminal; Long Beach

Each location should plan to have the following readers:
- Fixed reader on ground floor in crew area next to existing time and attendance clock station.
- Portable reader(s); administrative office and/or vessels
- Note: Readers are not required for the equipment closets that are restricted areas since access to these areas is available only to those who have TWICs which will be verified during the scenarios specified.

Test Scenarios:
(1) Conduct Embarkation Identity Verification for each TWIC-holding crew member each time the crew member embarks the vessel. Test period to be brief; only long enough to obtain sample test data.
(2) Conduct Embarkation Identity Verification for each TWIC-holding crew member at the first embarkation of the day or shift of the crew member. Test period to be brief; only long enough to obtain sample test data.
(3) Conduct a Periodic Administrative Identity Verification for each TWIC-holding crew member or employee at a period to be determined (i.e., weekly; monthly; quarterly). Produce log of checks. Note: This test is intended to replicate Recurring Access procedures.

The length of each scenario will be as mutually agreed by TSA, the Coast Guard, Port of Long Beach, and Catalina Express officials.

Card authentication and hotlist updating will be as per Table 1 in Attachment 1.

Staten Island Ferry, St. George Terminal:

Locations:
(1) St. George, Staten Island; readers as per plans
   a. Vessel Maintenance Area Gate (Across from the passenger parking lot)
   b. Main employee access gate
   c. Passenger loading area door: (Loading areas are restricted when vessels aren't in terminal)

   Note: No fixed readers are planned for the ferries. Portable units should be used for periodic spot checks.

Test Scenarios:
(1) Conduct Embarkation Identity Verification for each TWIC-holding crew member each time the crew member embarks the vessel. Since all crew members enter through existing secure dock area access control, they will have their TWIC verified, and satisfy this requirement, as they enter the secure area gate.
(2) Conduct a Periodic Administrative Identity Verification for each TWIC-holding crew member or employee at a period to be determined (i.e., weekly; monthly; quarterly). This is in addition to the TWIC check upon entering the existing secure area. This verification is in addition to the access point check accomplished in scenario 1.). Produce log of checks.
(3) Random on board spot checks by Staten Island Ferry security officers using portable readers.

   The length of each scenario will be as mutually agreed by TSA, the Coast Guard, New York City Department of Transportation, and Staten Island Ferry officials.

   Card authentication and hotlist updating will be as per Table 1 in Attachment 1.

Magnolia Marine:

Locations:
(1) Vicksburg Administrative Office
(2) CATHERINE BERRY
(3) DOROTHY LEE.

   The Vicksburg office may use fixed or portable readers, but must have at least one operable portable reader for vessel checks.

The two vessels in the pilot test must have at least one portable reader.

Test Scenarios:
(1)   Conduct a Periodic Administrative Identity Verification for each TWIC-holding crew member or employee at a period to be determined (i.e., weekly; monthly; quarterly).). Produce log of checks. Note: This test is intended to replicate Recurring Access procedures.
(2)   Conduct Embarkation Identity Verification for each TWIC-holding crew member each time the crew member embarks the vessel. Test period to be brief; only long enough to obtain sample test data.
(3)   Conduct Embarkation Identity Verification for each TWIC-holding crew member at the first embarkation of the day or shift of the crew member. Test period to be brief; only long enough to obtain sample test data.

The length of each scenario will be as mutually agreed by TSA, the Coast Guard, and Magnolia Marine officials.

Card authentication and hotlist updating will be as per Table 1 in Attachment 1.

Watermark Cruises:

Locations:
(1)   Annapolis Administrative Office
(2)   City Dock, Annapolis
(3)   Various vessels (harbor tour vessel; charter vessels)

The Annapolis office may use fixed or portable readers, but must have at least one operable portable reader for vessel checks.

The vessels in the pilot test must have at least one portable reader.

Test Scenarios:
(1)   Conduct a Periodic Administrative Identity Verification for each TWIC-holding crew member or employee at a period to be determined (i.e., weekly; monthly; quarterly).). Produce log of checks.
(2)   Conduct Embarkation Identity Verification for each TWIC-holding crew member each time the crew member embarks the vessel.
(3)   Conduct Embarkation Identity Verification for each TWIC-holding crew member at the first embarkation of the day or shift of the crew member.

The length of each scenario will be as mutually agreed by TSA, the Coast Guard, and Watermark officials.

Card authentication and hotlist updating will be as per Table 1 in Attachment 1.

<u>Notes:</u>

Per NVIC 03-07 (3)(3)(a), "In all cases, the TWIC must be verified at a minimum of at least once a day, unless underway on a vessel where the entire vessel is a secure area. Owners/operators can require verification more frequently than once per day if desired."