Results from the Assessment of the Risk Mitigation Value of the Transportation Worker Identification Credential

February 28, 2020

Homeland Security

Message from the Deputy Secretary

February 28, 2020

I am pleased to present the following report, "Results from the Assessment of the Risk Mitigation Value of the Transportation Worker Identification Credential."

The report was compiled by the U.S. Department of Homeland Security's Science and Technology Directorate pursuant to the *Transportation Security Card Program Assessment* (Public Law 114-278). This report summarizes the results of the independent assessment conducted by the Homeland Security Operational Analysis Center, which is a DHS-sponsored federally funded research and development center operated by the RAND Corporation.

To address the results and findings in this report, the United States Coast Guard and Transportation Security Administration will develop a joint Corrective Action Plan (CAP), including improvement areas that require programmatic action. In accordance with Public Law 114-278, the CAP will be provided to members of Congress.

Pursuant to congressional requirements, this report is being provided to the following members of Congress:

The Honorable Roger Wicker
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Maria Cantwell
Ranking Member, Senate Committee on Commerce, Science, and Transportation

The Honorable Ron Johnson
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary Peters
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Bennie Thompson
Chairman, House Committee on Homeland Security

The Honorable Mike Rogers
Ranking Member, House Committee on Homeland Security

The Honorable Peter DeFazio
Chairman, House Committee on Transportation and Infrastructure

The Honorable Sam Graves
Ranking Member, House Committee on Transportation and Infrastructure

Should you have any questions, please do not hesitate to contact the DHS Office of Legislative Affairs at (202) 447-5890.

Sincerely,

Kenneth T. Cuccinelli II
Senior Official Performing the Duties of the Deputy Secretary
U.S. Department of Homeland Security

Executive Summary

Section 1(b) of the Transportation Security Card Program Assessment Act (Pub. L. 114-278) requires the Department of Homeland Security (DHS) to commission a research organization, such as a national laboratory, a university-based center, or a qualified federally-funded research and development center (FFRDC) to conduct an assessment of the Transportation Worker Identification Credential (TWIC®) Program. The Department delegated this task to the DHS Science and Technology Directorate (S&T), and S&T commissioned the Homeland Security Operational Analysis Center (HSOAC), an FFRDC, to conduct the independent assessment. This report is intended to summarize the findings of HSOAC's independent assessment. As a result, this summary and the assessment may not reflect the views of DHS, S&T, the United States Coast Guard (USCG), and/or the Transportation Security Administration (TSA) in every instance. In accordance with P.L. 114-278, the USCG and TSA are preparing a Corrective Action Plan that provides a response to HSOAC's findings, including improvement areas.

TSA and the USCG jointly manage the TWIC® Program. TWIC was established to help prevent a transportation security incident (TSI)—a security incident that results in a significant loss of life, environmental damage, damage to the transportation system, or economic disruption. All individuals requiring unescorted access to secure areas at Maritime Transportation Security Act (MTSA)-regulated facilities, vessels, and outer continental shelf facilities must have a TWIC card. Transportation workers are issued a TWIC card after completing an application, paying a fee, and being vetted through a security threat assessment (STA) or background check conducted by TSA to determine whether the individual poses a threat to national security, transportation security, or terrorism. The program published a Final Rule in 2016 that would require certain facilities to verify TWIC cards with technology that can access data on the card; however, the TWIC Accountability Act of 2018, Pub. L. 115-230, delayed implementation of the rule until after the United States (U.S.) Department of Homeland Security (DHS) submits this assessment of the TWIC program to Congress.

DHS commissioned HSOAC, a FFRDC, to conduct a comprehensive security assessment of the TWIC program. DHS S&T provided programmatic oversight of the research. HSOAC's analysis focused on the security value of the TWIC program, the vetting process, the use of TWIC at maritime facilities, and the costs and benefits of regulation requiring the use of biometric readers. Additionally, its analysis evaluated DHS's efforts to address deficiencies in the program that have been identified through various Government Accountability Office (GAO) and DHS Office of Inspector General (OIG) reports. HSOAC's assessment included data from TSA, USCG, DHS, previous related research, site surveys of 45 maritime facilities, and interviews of nearly 200 facility personnel.

Summary of Findings

Through Pub. L. 114-278, Congress required DHS to assess 10 specific areas of the TWIC program. These issues are organized into three categories. Table A summarizes the findings of HSOAC's assessment in a high-level report card format, followed by a narrative of additional details summarizing the findings of each area.

Table A. Summary of TWIC Program Assessment

Section of Public Law 114-278	HSOAC Assessment
A. Findings Regarding TWIC Credentialing Process	
i. Review the Appropriateness of Vetting Standards	**Appropriate**
ii. Review the Fee Structure and the Cost of Vetting	**Appropriate**
iii. Redundancy or Duplication with Other Transportation Credentials	**No Duplication**
iv. Appropriateness of Varied Threat Assessments and Access Control	**Appropriate**
B. Findings Regarding Length of Time to Review TWIC Applications	**Appropriate**
C. Findings Regarding the Security Value of the TWIC Program	
i. Addresses Known and Likely Maritime Security Risks	**Addressed**
ii. Potential for a Non-Biometric Alternative	**Addressed**
iii. Impact of TWIC Cards and TWIC Readers	**Moderate**
iv. Cost and Benefits of the TWIC Program	**High Cost**
v. Previous GAO and OIG Concerns	**Addressed**

A. Findings Regarding the TWIC Credentialing Process

i. Review the Appropriateness of Vetting Standards: The TWIC vetting standards are used to determine whether an applicant poses a security threat following appropriate checks against terrorist, criminal history, and immigration databases. HSOAC determined the vetting standards are generally appropriate for this purpose. HSOAC reports some facility operators indicated the vetting standards were insufficient to identify general security risks, while others mentioned the standards exceed their intended purpose or are too stringent. The current vetting standards, set forth in 46 U.S.C. § 70105, including the redress process, attempt to strike a balance between the two perspectives. This balance trends towards a higher risk tolerance given that a single vetting standard must apply to the entire population working in the maritime sector. Facilities may choose to adopt additional criteria.

ii. Review the Fee Structure and the Cost of Vetting: Based on HSOAC's review of the TWIC program's revenue, cost, and carryover data for Fiscal Year (FY) 2016, 2017, and 2018, HSOAC assessed the current fee structure is adequate. TWIC user fees have aligned reasonably well with per-enrollment costs. In FY 2016 and FY 2017, revenue from user fees exceeded average cost per enrollment by 13 to 23 percent. In FY 2018, costs exceeded revenue from user fees by less than 1 percent (approximately $300,000), but the deficit was covered by carryover funds. The current fee is $125.25 for standard enrollment or renewal. Comparable enrollment is available at a reduced rate of $105.25, and replacement cards can be obtained for $60.00. These fees are designed to recover enrollment, vetting, and credentialing costs, as well as the cost of maintaining the TWIC over its five-year validity term.

iii. Redundancy or Duplication with Other Transportation Credentials: In considering whether there are redundant or duplicative transportation credentials, HSOAC found no duplicative credentials. HSOAC did not find any instances where state-issued maritime credentials, and/or port-specific or facility-specific credentials serve duplicative purposes, functions, or standards as TWIC. The TWIC STA is identical to the STA TSA conducts for individuals who receive a hazardous materials endorsement (HME) for state-issued

commercial driver's licenses. Approximately 21 percent of the total HME population and 12 percent of the total TWIC population carry both credentials. While redundancies exisit between HME and TWIC, differences in the purpose, function, and standard, such as issuing entitiy, credential type, and required use (e.g., surface v. maritime transporation) resulted in HSOAC's determination based on their definitions of *duplicative, redundancy*, and *unnecessary redundancy*.

iv. Appropriateness of Varied Threat Assessments and Access Control: TWIC establishes a standard level of acceptable risk based on those who are cleared to have unescorted access authority to maritime facilities and vessels. Nothing precludes industry from implementing a more restrictive access control system to meet their needs, and possession of a TWIC alone does not result in access; the TWIC holder must have a business need to enter. Therefore, it is appropriate that there would be different threat assessments in place at the facility-level, as facilities would apply a standard tailored for their risk tolerance. Facilities also vary in their level of risk. The USCG has created two risk categories based on facility types: Risk Group A facilities and non-Risk Group A facilities; and, also generates a risk score for each facility based on their specific threats, vulnerabilities, and consequences. Given these facility-by-facility differences in the nature of the risk, level of risk, and risk tolerance, it is wholly appropriate that access control systems would vary and be customized to best meet the needs of each facility.

B. Findings Regarding the TWIC Application Process

i. HSOAC evaluated the length of time to process applications for TWICs, including appeals and waivers. TSA provided a report to Congress in February 2019 addressing the concerns raised in Pub. L. 114-278 on the length of time to renew applications. This report illustrates that more than half of recent TWIC applications receive a favorable adjudication result within two days, and 99 percent of adjudications took less than 30 days. TSA determined the average processing time for redress applications in 2018 was 26 days for appeal requests and 47 days for waiver requests. These times are significant improvements over the processing times prior to 2016. The feedback HSOAC received during their interviews with facility security officers supports the findings that the application times have noticeably improved.

C. Findings Regarding the Security Value of the TWIC Program

i. Addresses Known and Likely Maritime Security Risks: The TWIC program is strongest in reducing risks presented by individuals who are known or suspected terrorists who seek to conduct or facilitate an attack on a maritime facility that would require persistent insider access via possession of a TWIC credential. These individuals would be detected by the STA process and denied a TWIC credential, making it difficult for such individuals to gain continual access to a facility. The TWIC program is less effective at stopping threats where an attacker seeks one-time access to the facility to conduct an attack and is not easily deterred in gaining entry. This could include scenarios where an attacker gains access to a facility with the use of a TWIC card-carrying escort or circumvents access control points. A TWIC program with robust access control technology would still fail to detect the threat posed by someone with a "clean" history, such as a homegrown violent extremist (HVE) with no known ties to terrorism.

ii. Potential for a Non-Biometric Alternative: Regarding the evaluation of non-biometric credential alternatives, HSOAC found biometrics are a superior method of identity

verification. Removing biometrics would eliminate the ability to use a portable, stand-alone reader to conduct biometric spot checks. Also, the biometric credential gives flexibility to facilities on how to integrate TWIC into their access control procedures. Without the biometric information, TWIC cards would still have the means for multi-factor authentication options using the saved personal identification number (PIN). Either option would still require facilities to utilize some form of electronic card reader to enable the multi-factor authentication.

iii. Impact of TWIC Cards and TWIC Readers: There is an inherent challenge in implementing and maximizing an effective security control system while minimizing the impact the system has on impeding the flow of people and goods. The TWIC program was introduced more than 10 years ago, and there have been significant improvements in the enrollment process and card quality since its initial introduction. Given this extended evolution, it was difficult for HSOAC to ascertain the challenges, burdens, or operational impact of TWIC on facilities. The greatest impact has been at facilities that had little semblance of an access control program prior to the TWIC program. Given improvements made in the enrollment process, the operational impact of applying for TWICs is not a major concern, based on information gleaned from interviews with facility security personnel, industry representatives, and labor representatives. However, implementation of the TWIC Reader Rule is expected to negatively affect operations due to a combination of factors including the number of facilities affected by the TWIC Reader Rule, increased cost estimates for the readers, unknown reader reliability, and unknown reader availability from suppliers.

iv. Cost and Benefits of the TWIC Program: HSOAC did not complete a true cost and benefit analysis due to an inability to estimate the security benefit of the TWIC program alone. Instead, HSOAC used a break-even analysis, which estimates the annualized costs of the TWIC Reader Rule to be $37.7 million. The Card Reader regulation would have to avert one lower consequence event every 54 years or one higher consequence event every 195 years to equal or offset the costs of the rule. However, HSOAC doubts the benefits of the program would exceed the costs, because historical data does not indicate a high enough frequency of attempted terrorist attacks in the maritime industry to achieve the necessary break-even level of activity.

v. Previous GAO and OIG Concerns: HSOAC also evaluated the extent to which the deficiencies in the TWIC program previously identified by the GAO and DHS OIG have been remedied. Nearly all of GAO and OIG's recommendations related to the program's management have been resolved, improved, or closed. GAO's open recommendations primarily relate to the need to conduct a comprehensive assessment on the TWIC program, and the HSOAC assessment should satisfy GAO's recommendations.

Way Ahead

Section 1(c) of Pub. L. 114-278 requires DHS to deliver a Corrective Action Plan to Congress within 60 days of the assessment's completion to address any deficiencies identified by HSOAC's analysis. The Corrective Action Plan will be developed by USCG and TSA to respond to the findings of the assessment and include an implementation plan, any programmatic reforms, revisions to regulations, or proposals for legislation. DHS OIG will review the Corrective Action Plan within 120 days of receipt to ensure that the plan meets the requirements of the statute and provide Congress with periodic updates on the progress of the Department's implementation of such plan.

Results from the Assessment of the Risk Mitigation Value of the Transportation Worker Identification Credential

Table of Contents

I. Legislative Language

This document responds to the reporting requirements set forth in the Transportation Security Card Program Assessment Act (P.L. 114-278). For reference, sections 1(b) and 1(c) are quoted in their entirety as follows:

> **Section 1. Transportation Worker Identification Credential Security Card Program Improvements and Assessment.**
>
> (b) COMPREHENSIVE SECURITY ASSESSMENT OF THE TRANSPORTATION SECURITY CARD PROGRAM.—
>
> (1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall commission an assessment of the effectiveness of the transportation security card program (referred to in this section as "Program") required under section 70105 of title 46, United States Code, at enhancing security and reducing security risks for facilities and vessels regulated under chapter 701 of that title.
>
> (2) LOCATION.—The assessment commissioned under paragraph (1) shall be conducted by a research organization with significant experience in port or maritime security, such as—
>
> (A) a national laboratory;
>
> (B) a university-based center within Science and Technology Directorate's centers of excellence network; or
>
> (C) a qualified federally-funded research and development center.
>
> (3) CONTENTS.—The assessment commissioned under paragraph (1) shall—
>
> (A) review the credentialing process by determining—
>
> (i) the appropriateness of vetting standards;
>
> (ii) whether the fee structure adequately reflects the current costs of vetting;
>
> (iii) whether there is unnecessary redundancy or duplication from other federal- or state-issued transportation security credentials; and
>
> (iv) the appropriateness of having varied federal and state threat assessments and access controls;
>
> (B) review the process for renewing applications for Transportation Worker Identification Credentials, including the number of days it takes to review application, appeal, and waiver requests for additional information; and
>
> (C) review the security value of the Program, by—
>
> (i) evaluating the extent to which the Program, as implemented, addresses known or likely security risks in the maritime and port environments;
>
> (ii) evaluating the potential for a non-biometric credential alternative;
>
> (iii) identifying the technology, business process, and operational impacts of the use of the transportation security card and transportation security card readers in the maritime and port environments;
>
> (iv) assessing the costs and benefits of the Program as implemented; and
>
> (v) evaluating the extent to which the Secretary of Homeland Security has addressed the deficiencies in the Program identified by the Government Accountability Office and the Inspector General of the Department of Homeland Security before the date of enactment of this Act.
>
> (4) DEADLINES.—The assessment commissioned under paragraph (1) shall be completed not later than 1 year after the date on which the assessment is

commissioned.

(5) SUBMISSION TO CONGRESS.—Not later than 60 days after the date that the assessment is completed, the Secretary of Homeland Security shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives the results of the assessment commissioned under this subsection.

(c) CORRECTIVE ACTION PLAN; PROGRAM REFORMS.—If the assessment commissioned under subsection (b) identifies a deficiency in the effectiveness of the Program, the Secretary of Homeland Security, not later than 60 days after the date on which the assessment is completed, shall submit a corrective action plan to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives that—

(1) responds to findings of the assessment;

(2) includes an implementation plan with benchmarks;

(3) may include programmatic reforms, revisions to regulations, or proposals for legislation; and

(4) shall be considered in any rulemaking by the Department of Homeland Security relating to the Program.

II. Background

Pursuant to Public Law (Pub. L.) 114-278, the U.S. Department of Homeland Security (DHS) requested the Homeland Security Operational Analysis Center (HSOAC), a federally funded research and development center (FFRDC), to conduct a comprehensive risk assessment of the Transportation Worker Identification Credential (TWIC®) program.[1] TWIC is a biometric credential required for unescorted entry to secure areas of vessels, outer continental shelf facilities, and port facilities regulated by the Maritime Transportation Security Act (MTSA) of 2002. The TWIC program's purpose is to "enhance the security of ports by requiring such security threat assessments of persons in secure areas and by improving access control measures to prevent those who may pose a security threat from gaining unescorted access to secure areas of ports."[2]

Currently, the Transportation Security Agency (TSA), and the United States Coast Guard (USCG) administer TWIC as a multilayered security approach intended to deter and prevent a transportation security incident (TSI) in the maritime domain. TSA is responsible for enrolling applicants, adjudicating the security threat assessment (STA), and issuing the biometric credential. The USCG administers the security program and TWIC access control standards for facility and vessel owners/operators to implement.[3] Facility and vessel operators determine who is authorized to have access to secure areas of their MTSA-regulated facilities or vessels and verify that each individual holds a valid TWIC.

In analyzing the TWIC program and its value in mitigating risk at maritime ports, HSOAC's assessment sought to address the following: 1) TWIC's risk mitigation value in the maritime environment and the appropriateness of vetting standards; 2) whether the fee structure is appropriate for the current costs of vetting; 3) the time required for the issuance of a TWIC card; 4) the duplication or redundancy of the TWIC with other federal and state credentialing programs; 5) the use of TWIC at facilities; and, 6) the costs and benefits of a pending regulation that would require high-risk facilities to use TWIC in conjunction with a biometric, electronic reader (the "TWIC Reader Rule"). The assessment also sought to address the primary question on whether or not the TWIC program is effective at "enhancing security" and "reducing security risks for [MTSA-regulated] facilities." To address the questions in Pub. L. 114-278, HSOAC collected information from a variety of sources, including literature on access control programs and deterrence, USCG databases, the U.S. Government Accountability Office (GAO) and DHS Office of Inspector General (OIG) studies on the TWIC program, and regulation relevant to TWIC, USCG and TSA policy documents. HSOAC also conducted 195 interviews with facility operators and traveled to 164 facilities at 45 port areas.

MTSA-regulated facilities and vessels are required to identify, authenticate, and authorize individuals who have unescorted access to their secure area. The TWIC card serves to fulfill some, but not all, of these purposes. The TWIC card provides identifying information (a holder's

---

[1] Section 1(a) of Pub. L. 114-278 also required a separate assessment of the TWIC program by the Transportation Security Administration. That report is being delivered to Congress separately. Section 1(b) assigned this assessment to the Secretary of DHS, who assigned the Science and Technology Directorate (S&T) the responsibility for carrying out this assessment. S&T awarded a task for the analysis underlying this report to its HSOAC FFRDC, operated and managed for DHS by the RAND Corp. The findings here rely on the work performed by HSOAC; the ultimate observations, recommendations, and way ahead will be contained in the Corrective Action Plan.

[2] TWIC Final Rule, 72 Federal Register 3492 (Jan. 25, 2007).

[3] U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-07 (Jul. 2, 2007), 4.1 Enforcement Strategy. As of Dec. 11, 2018, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2007/NVIC%2003-07.pdf.

name) and provides three possible means for authentication—a visible photo printed on the card, a unique personal identification number (PIN), and fingerprints stored on the integrated chip.

As initially conceived, the TWIC program requires the use of biometrically-enabled credentials and biometric, electronic card readers. The 2006 Notice of Proposed Rulemaking (NPRM) for the TWIC program included both components, but in response to comments received on the proposed rule, DHS decided to implement the TWIC program in two phases. The first rulemaking (2007) set forth the STA standards and process for issuing TWIC credentials, and required MTSA-regulated vessels and port facilities to "use TWIC as an access control measure."[4] The 2007 rulemaking did not prescribe a particular method of inspecting or validating TWIC; it provided only that owners and operators of MTSA-regulated facilities and vessels "change their existing access control procedures to ensure that merchant mariners and any other individual seeking unescorted access to a secure area of their vessel or facility has a TWIC."

The second rulemaking of TWIC is still ongoing. In March 2013, USCG published a NPRM that would require owners and operators of certain MTSA-regulated facilities and vessels to use electronic readers designed to work with TWIC as an additional access control measure. Based on comments provided to this NPRM, a pilot program conducted at some maritime facilities using electronic readers, and an economic regulatory analysis, the USCG issued the "Transportation Worker Identification Credential (TWIC)-Reader Requirements," final rule in 2016[5]. This second rulemaking, referred to throughout this report as the "TWIC Reader Rule", focused on the requirements for verification and authentication of TWIC cards. Rather than applying it to all MTSA-regulated facilities as initially envisioned, the USCG determined the requirement for biometric, electronic readers would be limited to vessels and facilities deemed at "high risk" for a potential transportation security incident.

The TWIC Reader Rule was scheduled to go into effect in August 2018, but the TWIC Accountability Act of 2018, Pub. L. 115-230, prohibited the USCG from implementing the rule until after DHS submits this HSOAC assessment of the TWIC program to Congress. This rulemaking would require facilities and vessels deemed "high risk" to use a biometric electronic reader to authenticate the TWIC card, validate the TWIC against the Canceled Card List (CCL), confirm the cardholder's identity using biometrics, and maintain a record of individuals with unescorted facility access. USCG analysis found two groups of facilities to be high risk: large passenger facilities and Certain Dangerous Cargos (CDC) facilities. There are 525 facilities and one vessel that would be affected by the final TWIC Reader Rule, but this number could be significantly greater depending on type, quantity, or handling of CDCs at a facility.

For its part in the TWIC program, TSA is responsible for enrolling applicants, adjudicating the STA, and producing and issuing the TWIC card. Applicants may apply for a TWIC card at one of the hundreds of enrollment centers located nationwide, which are operated by an authorized service provider contracted to TSA. An applicant's information is checked against multiple sources: Applicant fingerprints are transmitted to the Federal Bureau of Investigation's (FBI) Criminal Justice Information Service for a criminal history records check; TSA's Transportation Vetting Center checks biographic information from the applicant against multiple databases;

[4] DHS issued the final rule implementing TWIC as a transportation security card program on Jan. 25, 2007. U.S. Department of Homeland Security, "Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License" (TWIC final rule), 72 Fed. Reg. 3492 (Jan. 25, 2007). The TWIC electronic reader requirements were carved out of this 2007 final rule.
[5] Transportation Worker Identification Credential (TWIC) – Reader Requirements (Final rule), 81 Federal Register 57653 (August 23, 2016).

applicant immigration and biographic information is compared against the United States Citizenship and Immigration Services' (USCIS) Systematic Alien Verification for Entitlements (SAVE) database to confirm that they are in an eligible immigration status; and TSA continuously compares applicant information against the terrorist screening database. TSA also maintains a list of cards that have been canceled because they have been lost, stolen, or revoked due to a loss of eligibility.

Facility operators ultimately have day-to-day responsibility for ensuring TWIC cards are verified and managing access control programs. The USCG requires owners/operators of MTSA-regulated vessels or facilities to maintain a facility or vessel security plan that, among other security measures, articulates TWIC policies and procedures.[6] Among other things, "the vessel or facility must conduct a positive verification of the TWIC before allowing unescorted access to a secure area."[7] Port facility and vessel operators make the final determination of whether an individual is granted access to secured areas. Authorized access thus requires three functions to be performed: verify an individual has undergone a STA, establish identity, and establish the individual's business purpose.

[6] 33 CFR 104.405; 33 CFR 105.405; U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-07 (Jul. 2, 2007). As of Dec. 11, 2018, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2007/NVIC%2003-07.pdf.

[7] U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-07 (Jul. 2, 2007), 3.3 Vessel and Facility Guidance. As of Dec. 11, 2018, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2007/NVIC%2003-07.pdf.

III. Results

Section (b)(3)(A)(i). Review of the Appropriateness of Vetting Standards

In order to determine whether vetting standards are appropriate, HSOAC analyzed their suitability for the intended purpose. As required by MTSA, TSA's STA screens applicants for terrorism and other security threat information, certain criminal offenses, and immigration status. There is a waiver process for those who meet certain disqualifying criteria. TSA monitors TWIC holders continuously for connections to terrorism, and in the future will also monitor them for new criminal activity through the FBI Rap Back service. The TWIC STA and credential remains valid for five years, unless the holder loses eligibility through loss of immigration status or based on new information gleaned from recurrent vetting. If the TWIC is revoked, it is added to the CCL. Approximately 98 percent of individuals who apply for a TWIC are deemed eligible for one. HSOAC was unable to determine how many individuals decided not to apply for a TWIC, because they did not meet the eligibility standards.

The individuals HSOAC interviewed consisted primarily of facility operators and security managers who ~~might~~ represent the diversity of opinions about the TWIC program and facility operations. Interviewees presented varying views of the vetting standards. Some interviewees argued that the standards are insufficient to identify individuals who present a general security risk. These industry respondents were often speaking based on their expectations of the TWIC program - to reduce the risk that an employee would harm other individuals at the facility, damage material at the facility, or steal from the facility. Some interviewees said the vetting standards provided little benefit in relation to an active shooter threat, which respondents described as more likely than terrorism. Facilities that felt the standards were insufficient would therefore contract for a separate criminal record check (performed by a commercial vendor) to identify criminal offenses that are not disqualifying for a TWIC, or perform other types of checks—such as drug tests—to determine whether someone presented a security or safety risk.

Some facility operators found TWIC's standard sufficient, particularly for those with limited levels of access at their facility. Of approximately two-thirds of facility operators HSOAC interviewed, the facility conducted a separate background check for at least some part of the population. Given that HSOAC's interview sample consisted of a higher proportion of high-risk facilities, it is reasonable to expect a higher proportion of low-risk facilities who accept TWIC as the vetting standard.

Determining whether standards are appropriate requires a clear understanding of what TWIC is and is not intended to do. Recognizing that the Federal Government may have a different objective than industry also means there may be inherent tradeoffs between how stringent the criminal history standards are and how satisfied stakeholders are with the TWIC program. While not quantifiable, most facility security officers and security managers interviewed by HSOAC felt the TWIC program improves security to the maritime environment.

Overall, the TWIC vetting standards and redress process carry out the requirements of the MTSA and attempt to strike a balance between the two camps. This balance trends toward a higher risk tolerance given that a single vetting standard must be applied to the entire population working in the maritime sector - a population of around two million - and that facility operators may choose to adopt additional criteria beyond TWIC vetting standards to satisfy their specific security needs.

Section (b)(3)(A)(ii). Review of Fee Structure and Cost of Vetting

Pub. L. 114-278 asked whether the fees for TWIC are commensurate with the costs of the vetting process. HSOAC reviewed the costs of the TWIC program in relation to the fee charged to applicants, to determine whether costs were adequate given the costs of vetting. HSOAC performed this analysis using enrollment, fee revenue, and cost data covering Fiscal Year (FY) 2016, 2017, and 2018. HSOAC found TWIC user fees have aligned reasonably well with per-enrollment costs. In FY 2016 and 2017, TWIC revenue exceeded costs, and the surplus was used as a carryover to maintain liquidity from year to year. In FY 2018, revenue fell short of costs, but the deficit was covered by carryover funds. In each year, user fees remained within 25 percent of the underlying per-enrollment costs.

Table 1 compares fees and costs for each enrollment type. In FY 2016 and 2017, user fees exceeded average cost per enrollment by 13 to 23 percent. In FY 2018, user fees aligned more closely with the underlying costs. Fees for standard enrollments, renewals, and comparable enrollments fell short of per-enrollment costs, but the margin was less than two percent. The fee for replacement cards continued to exceed per-enrollment cost, but the margin shrank to nine percent in FY 2018.

Table 1. Transportation Worker Identification Credential User Fees and Costs per Enrollment

	Standard Enrollment	Renewal	Comparable Enrollment	Replacement Card
FY 2016 User Fee	$ 128.00	$ 128.00	$ 105.25	$ 60.00
FY 2016 Cost per Enrollment	$ 111.83	$ 111.83	$ 92.42	$ 49.54
FY 2017 User Fee	$ 125.25	$ 125.25	$ 105.25	$ 60.00
FY 2017 Cost per Enrollment	$ 110.58	$ 110.58	$ 91.59	$ 48.99
FY 2018 User Fee	$ 125.25	$ 125.25	$ 105.25	$ 60.00
FY 2018 Cost per Enrollment	$ 126.35	$ 126.35	$ 106.64	$ 54.96

NOTE: Comparable enrollments are offered to applicants with an active Hazardous Materials Endorsement on a commercial driver's license.

Source: HSOAC Analysis

Although the $125.25 enrollment fee is higher than the typical cost of a commercial background check, the fee covers additional services that are not part of commercial checks. The TWIC STA includes recurrent vetting against terrorist and other government watchlists, immigration status verification, recurrent criminal vetting, printing and mailing a biometric credential, and administering appeals and waivers. In contrast, most commercial background checks are a one-time service limited to a public records criminal check. In terms of costs, the TWIC STA is cost efficient compared to private background checks.

Section (b)(3)(A)(iii). Unnecessary Redundancy or Duplication

In assessing whether there are unnecessarily redundant or duplicative transportation credentials, HSOAC defined "duplicative" as the same in purpose, function, and standard. HSOAC defined "redundant" as similar in purpose, function, and standard. HSOAC defined "unnecessarily redundant" as providing a similar-risk reducing effect without providing additional benefits. As part of this analysis, HSOAC also analyzed maritime credentialing in the private sector and reviewed whether other state, local, or county governments have programs similar to TWIC.

HSOAC determined there are no Federal Government credentials duplicative of TWIC. The TWIC STA is identical to the STA TSA conducts for individuals who receive a hazardous

materials endorsement (HME) for state-issued commercial driver's licenses. Approximately 21 percent of the total HME population and 12 percent of the total TWIC population carry both credentials. However, these programs are not unnecessarily redundant, as they serve different purposes. The HME requires a knowledge-based test on hazardous materials and driving safety history, and TWIC includes a biometric credential. The 2018 TSA Modernization Act, once implemented, will further reciprocity by permitting states to issue an HME for TWIC holders without requiring enrollment, a new STA, or pay the fee for the HME. HSOAC concluded that HME and TWIC credentials are not unnecessarily redundant as each confers different benefits to users, and HME holders must have knowledge of how to handle hazardous materials. Currently, no states issue a state-wide maritime credential. There are some port authorities—operated at the state, county, or municipal level—that issue a port-specific credential.

Private facilities often issue a facility-specific or company-specific credential. The TWIC primarily serves as an identification badge and proof of the STA, while these port-specific or facility-specific credentials primarily served to establish business purpose at facilities or relate to company-related business (such as managing timekeeping). HSOAC does not consider these credentials redundant of TWIC as they have different purposes, functions, and standards.

Section (b)(3)(A)(iv). Appropriateness of Varied Federal and State Threat Assessments and Access Controls

TWIC establishes a baseline for acceptable risk to national security, transportation security, and terrorism. The Statute establishes the vetting criteria, which falls roughly into three bins:

- National security related information, including ties to terrorism;
- Past felony criminal history; and
- Legal immigration status.

Industry may have different objectives in conducting an employee threat assessment (background check) than the Federal Government has for the TWIC program, and facilities vary in their level of risk. Therefore, it is appropriate that there would be different threat assessments in place at the Federal and facility levels, in that facilities would apply standards tailored for their levels of risk tolerance. For example, a port authority might conduct its own check to determine whether a port worker who operates equipment has a conviction for driving under the influence, when that conviction is not generally relevant to the security evaluation TSA conducts for TWIC under the TWIC statute. HSOAC did not examine the extent to which other background checks differ from the TWIC STA. Also, is it important to note that TSA does not have the authority to prohibit ports or facilities from conducting their own checks for suitability or other criteria.

Facilities also vary in their levels of risk tolerance, which would affect their levels of investment in security measures. Given these facility-by-facility differences in nature of the risk, level of risk, and risk tolerance, it is appropriate that their access control systems would vary, and be customized, to best meet the needs of each facility. TWIC provides facilities options in how it can be integrated into existing access control systems. TWIC also allows facility operators greater flexibility in customizing an access control system that is appropriately suited to risk type, risk level, and risk tolerance of the facility.

Section (b)(3)(B). Length of Time to Review TWIC Applications

Pub. L. 114–278 asked about the length of the process for renewing applications for TWICs, but given that there is no renewal-specific process for the TWIC program—the application process is

the same for new or former TWIC holders—the assessment's authors considered this question in the context of the application process for all applicants.

TSA submitted a report to Congress in 2019 reflecting an analysis of the STA process.[8] TSA's analysis found that 50 to 55 percent of applicants have their applications adjudicated favorably by the system within two days, receiving their TWIC card three to four days later. Most of the remaining cases are adjudicated within 30 days of application. Less than one percent of all adjudication cases require more than 30 days to reach a preliminary determination of qualification. TSA determined that the average processing time for redress applications in 2018 was 26 days for appeal requests and 47 days for waiver requests. These times are significant improvements over the processing times prior to 2016. The feedback that HSOAC received during their interviews with facility security officers supports the findings that the application times have noticeably improved.

Section (b)(3)(C)(i). Known and Likely Maritime Security Risks

The threat environment for the maritime domain is diverse, with threats coming from varied sources such as Nation-state actors, terrorists, and transnational criminal organizations. Trends in foreign terrorist activity toward opportunity-driven attacks suggest that security measures, such as access control programs, could deter radicalized actors who would not be capable of carrying out a sophisticated attack. The analysis found that threats that could cause a transportation security incident are assessed to be less likely to occur today than they would have been at the inception of the TWIC program, and that the terrorism threat is low. The threat has not gone away, but shifted towards a focus on soft targets and simple tactics that do not require advanced skills or outside training[9].

The TWIC program is strongest in reducing the risk presented by individuals who are known or suspected terrorists who seek to conduct an attack on a maritime facility that would require persistent insider access via possession of a TWIC. The TWIC program is similarly effective in reducing the risk from a worker with a disqualifying criminal history who may be willing to otherwise engage in additional criminal activity that could impact the safety and/or security of a MTSA-regulated facility if they were granted unescorted access.

The TWIC program is less effective at stopping threats where an attacker (or attackers) seeks one-time access to the facility to conduct an attack and is not easily deterred in gaining entry. The TWIC program may provide some additional ability to detect these threats, but the ability to prevent such a threat is dependent on other mechanisms of the access control program, such as the guard, physical access control system (PACS), or deployable physical barriers.

A TWIC program with robust access control technology would still fail to detect the threat posed by someone with a "clean" history (i.e., someone who was not known to authorities). The most likely terrorist attack within the United States today is seen as coming from homegrown violent extremists (HVE). As HVEs are often self-radicalized using terrorist propaganda available online, they may elude the attention of intelligence and law enforcement authorities. They also work independently or in a small group, to carry out attacks on soft targets using simple tactics. HVEs have been more successful than foreign terrorists, despite fewer resulting casualties. The

[8] TSA; "Transportation Worker Identification Credential Appeal Timelines," February 1, 2019.
[9] Nicholas J. Rasmussen, director, National Counterterrorism Center, Office of the Director of National Intelligence, "World Wide Threats: Keeping America Secure in the New Age of Terror," testimony before the U.S. House of Representatives Committee on Homeland Security, November 30, 2017.

vulnerabilities of HVEs are not unique to TWIC, but remain a potential threat in the port environment nonetheless. The TWIC program may provide some deterrence against HVEs from attempting an attack on a regulated facility for fear of being discovered during the application process, but the current STA vetting standards may otherwise fail to identify a HVE.

Section (b)(3)(C)(ii). Potential for a Non-Biometric Alternative

In considering the potential for a non-biometric credential alternative, HSOAC considered the benefits brought by the current storage of biometric information (two fingerprints) on the integrating circuit chip of the TWIC card.[10] Biometrics have been found a superior method of identity verification, as the technology provides a reliable, sophisticated mechanism for dual-factor authentication that is not easily defeated. Without the biometric information, TWIC cards would still have the means for dual-factor authentication options using the saved PIN. However, the knowledge factor authentication methods, such as PINs and passwords, does have several disadvantages to biometrics. A TWIC card could be used by another individual if they were also provided with the PIN or password to the card. This leaves visual inspection of the card as the only way to catch a potential bad actor using this method to access a facility. PINs and passwords are also easily forgotten, which would require administrative procedures to handle such cases.

The stored biometric also gives flexibility to facility operators in how to integrate TWIC into their access control procedures. Facilities that sought to use biometric verification methods could still collect biometric information at time of enrollment, however the facility could not verify that the individual who initially applied for a TWIC card was the same person who was vetted by the STA. Removing the biometrics would also eliminate the ability for portable, stand-alone readers to be used to conduct spot checks using biometrics, currently in use by TSA, USCG, and facility operators.

Section (b)(3)(C)(iii). Impact of TWIC Cards and TWIC Readers

The transportation security card program was introduced over 10 years ago, and there have been significant improvements in the enrollment process and card quality since its initial introduction. Given this extended evolution, it was difficult to ascertain what the operational impact of the introduction of the transportation card program has been. This impact is further varied depending on facility practice prior to the introduction of the TWIC program. For some facilities that had little semblance of an access control program prior to the introduction of the TWIC program, the establishment of clear access control procedures was an obvious security benefit. However, for those that already had robust access control measures, differences brought by the program appear to be less apparent.

Given improvements made in the enrollment process, the operational impact of applying for TWICs did not appear to be a major concern for workers based on information received from the interview results. Operational impacts of the current implementation of the TWIC program primarily relate to: (a) the durability of the TWIC card and, (b) the necessity of a TWIC holder physically having their credential, which may introduce redundancies for facilities that want to use a PACS and facility-specific credential, along with extra costs when a credential holder forgets or loses their card.

[10] Several other biometric alternatives to fingerprints are available, but a comprehensive analysis of other biometric alternatives was not conducted by HSOAC.

HSOAC's cost analysis conducted as part of their assessment shows that the costs of TWIC readers are higher than originally estimated, largely due to the number of readers needed by each facility to comply with the regulation. This finding, in combination with the fact that the TWIC Reader Rule could affect many more facilities than originally estimated, suggests that the TWIC Reader Rule could put a high cost burden on an industry that is unlikely to be recovered in benefit. Industry has also had mixed experiences in the reliability of reader technology. The partial delay in implementing the TWIC Reader Rule per Pub. L. 115-230, has contributed to volatility in the demand for TWIC readers. Some of the readers previously identified as on the Qualified Technology List are outdated or no longer available.

HSOAC found that perceptions of TWIC varied widely among the users and facility operators with whom they spoke during their port and security visits. Interviewees' positive comments about the benefits of TWIC included that it provides a background check, standardization of identification, and a security deterrent. Negative comments centered on perceptions that TWIC was a regulatory requirement rather than a security benefit, and that it incurred additional costs.

HSOAC observed that the use of TWIC and the management of access control points varied at the facilities visited. The number of accessing individuals, the frequency of the same individuals passing through access points, the dispersion over time of accessing individuals, and the technology investments already being made by the facility all appeared to be important factors in these differences between facilities and the impact on access control programs. The variation in the TWIC verification methods that were observed seemed to result from differences in the characteristics of the facilities themselves, which affect facility vulnerability, potential attack consequences, and thus decisions on where to invest in security measures. Many facilities used other credentials in addition to TWIC. While visual inspection is currently all that is required per TWIC regulations, approximately half of the facility operators interviewed used electronic verification for TWIC, often in the form of a PACS. Eight percent of the facilities are already using biometric systems, either fingerprints, facial recognition, or vascular scans of the hand as part of their PACS. Some facilities found that using the TWIC card in coordination with a PACS system and biometric identity verification could both enhance security and bring operational efficacies. This finding suggests that enhanced biometric assurance measures are not necessarily at odds with operational efficiency; although, these facilities were high-traffic container facilities, and elements of their operating model do not necessarily apply to all facilities.

Section (b)(3)(C)(iv). Cost and Benefit of the TWIC Program

Ideally, in the case of the TWIC Reader Rule, the benefits of the regulation could be quantified by estimating how much the regulation reduces the probability of a terrorist attack. By combining this incremental reduction in the probability of a terrorist attack with monetary estimates about the consequences of an attack, one could produce an estimate of the economic value of the benefits of the regulation and compare it directly to the costs of the regulation. However, data does not exist to estimate the current (or baseline) probability of a terrorist attack and the potential reduction in that probability due to the regulation. Terrorist attacks in general are very infrequent events, which is particularly true in the maritime sector.

Since a true cost and benefit analysis could not be completed, HSOAC used a break-even analysis similar to the 2015 regulatory analysis on the TWIC Reader Rule that was conducted by the USCG. The U.S. Office of Management and Budget (OMB) recommends a "break-even" or "threshold" analysis when it is not possible to quantify or monetize a regulation's benefits.[11]

[11] U.S. Office of Management and Budget, Circular A-4, September 17, 2003

This analysis can help to frame the question in a different way by asking: how large would the benefits have to be to equal or exceed the costs of the regulation? When it is not possible to quantify benefits, the annualized costs represent the threshold at which the annualized benefits would "break even" with the costs of the regulation. The break-even threshold can be expressed in terms of the number of undesirable events that would have to be avoided each year for the benefits of a regulation to equal the costs.

HSOAC found that the 2015 regulatory analysis miscalculated the average cost per facility from the pilot program data and calculated the average number of facility access points-based on a sample of facilities that was not representative of the facilities subject to the final rule.[12] This led the 2015 regulatory analysis to underestimate the likely costs of the TWIC Reader Rule. The regulatory analysis also took the maximum consequence score across three different attack modes, terrorist assault team, truck bomb, and passenger/passerby explosives/improvised explosive device (IED), when calculating benefits, which could significantly overestimate the benefits of the regulation and bias estimates in the break-even analysis. The resulting HSOAC cost estimate is between 1.6 and 1.7 times higher than the 2015 regulatory analysis, but values are discounted and presented in year 2012 dollars to ease comparison between both studies.

HSOAC's analysis estimates the annualized costs of the TWIC Final Reader Rule to be $37.7 million (using a seven percent discount rate). Table 2 summarizes the total industry costs of the final reader rule by year based on the additional cost information collected. This does not include governmental costs, as the incremental government costs associated with the reader requirements are minimal compared to the overall costs of implementing and operating the TWIC program. The USCG estimates the total additional government costs are approximately $100,000 on an undiscounted basis and will be incurred during the first two years of the rule.[13]

Table 2. Industry Costs of the TWIC Reader Rule by Year ($2012 millions)

Year	Capital Costs	Maintenance Costs	Operational Costs	Additional Costs	Total
1	$105.4	$0.0	$1.5	$2.5	$109.5
2	$105.0	$2.8	$1.7	$2.5	$112.0
3	$0.0	$5.6	$0.4	$2.5	$8.5
4	$0.0	$5.6	$0.4	$2.5	$8.5
5	$0.0	$5.6	$0.4	$2.5	$8.5
6	$15.9	$5.6	$0.4	$2.5	$24.4
7	$15.9	$5.6	$0.4	$2.5	$24.3
8	$0.0	$5.6	$0.4	$2.5	$8.5
9	$0.0	$5.6	$0.4	$2.5	$8.5
10	$0.0	$5.6	$0.4	$2.5	$8.5
Total Cost	$242.2	$47.3	$6.1	$25.5	$321.0
Annualized Cost	$30.0	$4.5	$0.7	$2.5	$37.7

NOTE: Costs by year are not discounted. Annualized costs are calculated using a seven percent discount rate.

Source: HSOAC Analysis

To estimate the magnitude of the benefits required to equal or offset the costs of the Final Reader Rule, HSOAC analyzed the break-even threshold by considering three attack modes in the

[12] See Appendix G for the HSOAC Assessment for additional information

[13] U.S. Coast Guard, Office of Standards Evaluation and Development, Regulatory Analysis and Final Regulatory Flexibility Analysis for the Transportation Worker Identification Credential (TWIC) - Reader Requirements Final Rule, November 2015. Chapter 4.

Maritime Security Risk Analysis Model (MSRAM) which the USCG assesses for how improvements in access controls could plausibly avert a terrorist attack: terrorist assault team, truck bomb, and passenger/passerby explosives/improvised explosive device (IED). The benefit is equal to prevention of the consequence cost, which primarily consists of the estimated loss of life and significant injuries resulting from each attack scenario. The results are summarized in Table 3, along with the 2015 results for comparison.

Table 3. Comparison of 2015 Regulatory Analysis and HSOAC Break-even Analysis

2015 Regulatory Analysis				Revised Break-even Analysis				
Maximum Consequence (in millions)	Annualized Cost[1] (in millions)	Required Avoidance Rate (events per year)	Required Frequency of Attacks Averted	Maximum Consequence (in millions)		Annualized Cost[1] (in millions)	Required Avoidance Rate (events per year)	Required Frequency of Attacks Averted
$5,014.1	$21.9	0.004	One event every 229 years	Passenger/ Passerby Explosives /IED	$2,027.2	$37.7	0.019	One event every 54 years
				Truck Bomb	$3,287.2		0.011	One event every 87 years
				Attack by Terrorist Assault Team	$7,341.4		0.005	One event every 195 years

[1] Annualized costs are calculated using a seven percent discount rate.

Source: HSOAC Analysis

Since HSOAC's cost estimates were higher than those in the 2015 regulatory analysis, the benefits would also need to be higher to justify the costs of the regulation. This implies the required avoidance rate is higher than previously calculated in the 2015 regulatory analysis. It also implies TSIs would have to be averted more frequently as a direct result of the regulation to equal or offset the costs. HSOAC estimates that the annualized cost of acquiring and installing TWIC readers is $37.7 million (using a seven percent discount rate). For the relatively higher consequence event—a terrorist assault team has an average maximum consequence of $7.3 billion—this implies that the regulation would have to avoid 0.005 events each year, or one event every 195 years to equal or offset the costs. For the relatively lower consequence event—a passenger/passerby explosive/IED has an average maximum consequence of $2.0 billion—this implies that the regulation would have to avoid 0.019 events each year, or one event every 54 years to justify the costs.

Given the relative infrequency of terrorist attacks in the maritime environment historically, it is not possible to determine whether the TWIC Reader Rule would equal or exceed the break-even thresholds calculated in this study to justify the regulation on a cost–benefit basis. Although break-even analysis does not affirm whether a proposed regulation is appropriate or not, the more stringent break-even threshold HSOAC calculated does present a substantive challenge to the estimated or perceived benefit of the regulation.

Section (b)(3)(C)(v). Previous GAO and OIG Concerns

There have been nine reports on the TWIC program from the GAO and DHS OIG between 2004 and when Pub. L. 114-278 was issued. Several aspects of the TWIC program have been challenged during the life of the program. Table 4 highlights consistent themes raised in past GAO and OIG reports.

Table 4. Themes from Prior GAO and OIG Reports on TWIC

Themes	GAO-05-106	GAO-06-982	GAO-07-756	GAO-10-43	GAO-11-657	GAO-12-60	GAO-13-198	GAO-13-629	OIG-16-128
Failure to Assess the TWIC's Effectiveness at Reducing Risk					X		X		
Lack of Adherence to Management Best Practices (internal controls, planning, etc.)	X	X		X	X		X	X	X
Lacking Communication between Federal Government and Industry	X	X					X		
Lacking Identity Assurance in the TWIC Enrollment Process					X				X
Excessive Length of Time for TWIC Enrollment/Issue		X		X				X	
Questions Regarding the Appropriateness of Eligibility Standards for TWIC Card Holders		X				X			
Inability to Conduct Continuous Vetting for Criminal History of TWIC Holders					X	X			
Weaknesses of the TWIC Reader Pilot				X		X	X		
Cost of Readers Not Fully Calculated		X					X		
Reliability of TWIC Reader Technology		X					X		
Possible Value of Alternative Credentialing Models			X			X	X		
Possible Redundancies of a TWIC Credential			X			X			

Source: HSOAC Analysis

All of the recommendations from previous GAO and OIG reports on the TWIC program have been formally closed with the exception of three from GAO-11-657. GAO's open recommendations primarily relate to the need to conduct a comprehensive assessment on the TWIC program—recommendations this study aims to satisfy. Those questions focus on the extent to which TWIC, as currently implemented and as envisioned under the TWIC Reader Rule, enhances the security posture of maritime facilities. As discussed at great length in this report, such a question is not simple to answer. The TWIC program as currently implemented can enhance the security posture of MTSA-regulated facilities by limiting access through improved identity assurance and vetting for suspected terrorists, for certain criminal offenses, and for legal immigration status. The extent to which TWIC enhances a specific facility's security posture depends on what access control procedures they were conducting prior to TWIC's introduction or would do in TWIC's absence. It also depends on the extent to which the facility takes advantages of options provided by the TWIC program beyond simply visual inspection of the TWIC card.

The first of these open items relates to the need for DHS to perform an internal control assessment of the TWIC program, which is also called for in Pub. L. 114-278 section A. The GAO finds this recommendation was partly addressed by previous HSOAC research for TSA on this topic, with outstanding issues related to the need to evaluate "the use of TWIC, including the Coast Guard's role in TWIC enforcement." GAO, however, calls for a further "internal control assessment inclusive of TWIC use and the interrelationship between acquiring a TWIC and using it in the maritime environment." GAO further states that this assessment should "assess

information systems controls and related risks for reasonably assuring that use of TWIC with readers and associated systems used for access control decisions are reliable and not surreptitiously altered by cyber intrusions or attack." HSOAC's assessment did not look at the cyber vulnerabilities of access control systems, as this was determined to be outside the scope of their study, and cyber vulnerabilities were not a key theme of past GAO reports. Access control systems are proprietary systems of facilities or their contract providers.

The second open item relates to similar concerns of the need for "an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks." HSOAC's assessment addressed the general value of the TWIC program, as well as their analysis of the costs and benefits of using TWIC readers. GAO further calls for this assessment to review "the federally managed single credential approach in contrast to federally regulated decentralized options, such as the Secure Identification Display Area (SIDA) airport credentialing model, the HME for truck drivers (wherein an endorsement is added to a driver's license), the Federal Government's own agency-specific credentialing model which relies on organizational sponsorship and credentials with agency-specific security features, or any combination thereof." HSOAC's analysis includes a discussion of alternative credentialing models to address this item.

The last open recommendation relates to the cost and benefit of readers, which HSOAC addressed in their assessment, and which the results are included in this report. GAO recommends DHS use the TWIC assessments as "the basis for evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks as part of conducting the regulatory analysis on implementing a new regulation on the use of TWIC with biometric card readers." As previously discussed above, HSOAC's analysis indicates that the benefit of implementing readers will most likely not exceed the cost of doing so. Further, their study suggests that there is not a one-size-fits-all solution for improving security at maritime facilities, given their broad differences in risk and operations. The current process of facility-specific security assessments and security plans is designed to enable flexible solutions specific to each facility's needs. Greater identity assurance methods may be appropriate for some facilities given their risk profile. Transparent management of the TWIC program with a focus on how to effectively support TWIC's stakeholders could incentivize industry to maximize TWIC's potential security benefit.

IV. Conclusions

The TWIC program was originally conceived shortly after the attacks on 9/11 with the objective of reducing the risk of a terrorist attack on critical infrastructure in the maritime transportation system by restricting unescorted access to only those transportation workers who have been vetted through a STA. The regulations effect a population of 2.3 million transportation workers, 3,300 facilities, and 14,000 vessels. TWIC has made significant programmatic improvements over the past five years as supported by the number of findings and recommendations from previous GAO and OIG reports that have been addressed or implemented. The TWIC program as currently implemented appears to pay for itself with the revenue generated by the user fees covering the expenses of conducting the STAs, issuing cards, and other administrative costs.

HSOAC's efforts to provide a straightforward answer to the question of TWIC's risk mitigation value are complicated by the fact that TWIC cannot be empirically separated from the access control programs in which it is integrated. Additionally, the threshold of acceptable risk was unclear, which left HSOAC without a clear standard to judge TWIC's success. However, HSOAC's assessment was able to draw several conclusions regarding TWIC's ability to mitigate risk:

- TWIC cannot mitigate *all* risks in the maritime environment, but TWIC can significantly influence risk where known individuals gaining physical access to the facility through entry points is necessary.
- TWIC is only a component of a facility's overall access control program, and TWIC's ability to mitigate threats is directly related to the quality of the access control program.
- TWIC does mitigate some risks of attack scenarios that could only be successfully carried out by an "insider" who would need persistent, unescorted access to the facility.
- TWIC's deterrent value pushes potential bad actors away from attempting complex attacks with consequences that would exceed the TSI threshold.
- TWIC is strongest when it provides flexibility and options to the maritime industry, such as changes to USCG regulations to allow facility operators to integrate TWIC into their PACS, TSA's development of a mobile application that allows cards to be checked against the CCL, the provision of waivers for individuals who have disqualifying criteria but are found not to be a security risk, and the provision for facility specific data to be stored on the TWIC card.

Lastly, HSOAC determined the TWIC Reader Rule has several benefits such as alleviating human error in the process of matching an authentic, valid card to the owner of the credential by utilizing a combination of biometric and information technology. However, this capability does not come without added costs to industry, and HSOAC's analysis suggests the benefits of the TWIC Reader Rule are unlikely to exceed the associated costs of the regulation as proposed. A more favorable break-even point could be achieved by reducing the costs of compliance by requiring facilities to use an electronic reader, but not require biometric identity assurance. Program costs could also be lowered by changing the regulation to reduce the number of facilities that are subject to the TWIC Reader Rule.

In accordance with Section 1(c) of Pub. L. 114-278, USCG and TSA are developing a Corrective Action Plan to address the deficiencies identified by HSOAC's analysis of the TWIC program, as appropriate. DHS OIG will review the plan to ensure it meets the requirements of the Pub. L. and provide Congress with periodic updates on the progress of DHS's implementation of such plan.

V. Appendix A - List of Acronyms

Acronym	Definition
CCL	Canceled Card List
CDC	Certain Dangerous Cargos
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigations
FFRDC	Federally Funded Research and Development Center
FY	Fiscal Year
GAO	Government Accountability Office
HME	Hazardous Materials Endorsement
HSOAC	Homeland Security Operational Analysis Center
HVE	Homegrown Violent Extremist
IED	Improvised Explosive Device
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act
NPRM	Notice of Proposed Rulemaking
OIG	Office of Inspector General
OMB	Office of Management and Budget
PACS	Physical Access Control System
PIN	Personal Identification Number
Pub. L.	Public Law
SAVE	Systematic Alien Verification for Entitlements
SIDA	Secure Identification Display Area
STA	Security Threat Assessment
TSA	Transportation Security Administration
TSI	Transportation Security Incident
TWIC	Transportation Worker Identification Credential
U.S.	United States
USCIS	United States Citizenship and Immigration Services
USCG	United States Coast Guard