AIR CARGO SECURITY POLICY NEWSLETTER

Credentialing of Transportation Workers and Seafarers

May 25, 2011

Two subjects of interest to the transportation and security community have been recently addressed by the US Government Accountability Office (GAO)

At a hearing of the US Senate Commerce Committee examining the Transportation Worker Identification Credential (TWIC), program, Senator Lautenberg, who chairs the Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security, released an unclassified report from GAO the outlining major homeland security risks posed by the ID program currently in use at maritime facilities.

In a second report prepared for the Committee on Homeland Security for the House of Representatives, GAO reported that efforts to address risks posed by seafarers, can be strengthened.

This report also discusses the lack of implementation of International implementation of International Labor Office (ILO) 185 (only 18 countries have ratified ILO 185, representing 30% of the global seafarer supply). As of January 2011, the United States had not ratified ILO 185 largely due to concerns over a provision for facilitating visa-free shore leave for foreign seafarers.

Transportation Worker Identification Credential (TWIC)

I. The **opening remarks** of Senator Lautenberg set the tone for the TWIC hearing:

> ""*My state is home to the country's most at-risk area for a terrorist attack—a stretch that includes major hubs like the Port of New York and New Jersey, which handled more than $140 billion in cargo last year.*
>
> *To improve security at our ports, nine years ago the government created a worker identification program—known as TWIC—to make sure access to the nation's ports is limited to people who belong there, such as dock workers, cargo handlers and other professionals. After several delays, the program is now up and running, and the government has issued almost two million TWIC cards.*
>
> *But a recent Government Accountability Office investigation raises a disturbing question: Are America's ports actually safer now than they were a decade ago? The GAO has identified serious problems with TWIC—including startling evidence that this program might actually diminish the safety of our ports.*
>
> *At this Committee's request, the GAO conducted covert testing. Investigators were able to fraudulently obtain TWIC cards and use the cards to access secure locations. Not only were they able to access the port facilities, but they were able to drive a vehicle with a simulated explosive into a secure area.*
>
> *Fraudulent and counterfeit cards like the ones used by investigators could also be used as identification at airports or military facilities. The problems don't stop with fraudulent cards. There are also issues with criminal background checks, immigration checks and a lack of safeguards to determine if an applicant even needs a TWIC card.*
>
> *Despite these alarming findings, the Transportation Security Administration has so far failed to close the gaping holes that plague this program. In addition, the Department of Homeland Security, which heads the TSA, has not even conducted a review to determine if the card program helps or hinders security at our nation's ports.*
>
> *Given the critical importance of our ports, it is unacceptable that we are spending hundreds of millions of tax dollars on a program that might actually be making ports less safe. According to estimates, it could cost as much as three billion dollars to deploy the cards over a 10-year period—and this doesn't include the cost of the sophisticated biometric equipment needed to read the cards.*
>
> *We must thoroughly examine and correct the TWIC program and make sure we are focusing our resources where they are needed most—the areas that present the highest risk. So I look forward to hearing from our witnesses about the status of the program and how we can best implement changes to make sure our port security programs are effective and the money we spend is improving safety at our ports*."

II – The following has been extracted from **statement made by Chairman John L. Mica**, Committee on Transportation & Infrastructure Committee U.S. House of Representatives to the TWIC Hearing:

> *"TWIC is turning into a dangerous and expensive experiment in security. Nearly half-a-billion dollars have been spent since the Maritime Transportation Security Act of 2002 directed the Secretary of DHS to issue biometric transportation security cards to maritime workers. Yet today, ten years later, TWIC cards are no more useful than library cards. In fact, the only port that GAO investigators were NOT able to gain access to using fraudulent means was the port that still required port-specific identification for admittance to secure areas.*
>
> *We have also learned from GAO that:*
>
> *1. Individuals can obtain authentic TWICs using fraudulent identification documentation;*
>
> *2. Individuals can gain access to ports using counterfeit TWICs; and that, among other things,*
>
> *3. TSA is unable to confirm that TWIC holders maintain their eligibility throughout the life of their TWIC.*
>
> *This is a troubling scenario and counterintuitive to the purpose of the program. GAO determined that an individual does not have to prove who they say they are when enrolling in the program. In other words, an individual can present a fraudulent identification document with somebody else's name, but provide their own fingerprints to obtain an authentic TWIC card. In this instance, the TWIC card transforms into a biometric key that unlocks our Nation's ports and facilities for any individual with the intent and desire to do us harm.*
>
> *GAO tells us that DHS has not assessed whether or not the TWIC program enhances security or not. In fact, DHS cannot demonstrate that TWIC – as implemented and planned – is more effective than the approach used to secure ports and facilities before 9/11.*
>
> *I believe we must begin to ask if these vulnerabilities in fact make our nation less secure."*

The full statement of Representative Mica can be accessed at:

http://republicans.transportation.house.gov/Media/file/112th/CGMT/2011-05-10--Mica_Statement_for_Record_Senate_TWIC_Hearing.pdf

III – What GAO found

The GAO report on TWIC was entitled - Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives.

GAO summarised its findings as follows:

> "*Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program, which requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities. As requested, GAO evaluated the extent to which (1) TWIC processes for enrollment, background checking, and use are designed to provide reasonable assurance that unescorted access to these facilities is*

limited to qualified individuals; and (2) the effectiveness of TWIC has been assessed. GAO reviewed program documentation, such as the concept of operations, and conducted site visits to four TWIC centers, conducted covert tests at several selected U.S. ports chosen for their size in terms of cargo volume, and interviewed agency officials. The results of these visits and tests are not generalizable but provide insights and perspective about the TWIC program. This is a public version of a sensitive report. Information DHS deemed sensitive has been redacted

Internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of Maritime Transportation Security Act (MTSA)-regulated facilities is restricted to qualified individuals. To meet the stated program purpose, TSA designed TWIC program processes to facilitate the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls designed and in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. GAO found that internal controls in the enrollment and background checking processes are not designed to provide reasonable assurance that (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC-holders have maintained their eligibility.

Further, internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of MTSA-regulated facilities during covert tests conducted by GAO's investigators. During covert tests of TWIC use at several selected ports, GAO's investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (i.e., reasons for requesting access). Conducting a control assessment of the TWIC program's processes to address existing weaknesses could better position DHS to achieve its objectives in controlling unescorted access to the secure areas of MTSA-regulated facilities and vessels.

DHS has not assessed the TWIC program's effectiveness at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned, is more effective than prior approaches used to limit access to ports and facilities, such as using facility specific identity credentials with business cases. Conducting an effectiveness assessment that further identifies and assesses TWIC program security risks and benefits could better position DHS and policymakers to determine the impact of TWIC on enhancing maritime security. Further, DHS did not conduct a risk-informed cost-benefit analysis that considered existing security risks, and it has not yet completed a regulatory analysis for the upcoming rule on using TWIC with card readers. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments as the basis for

evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program, could help DHS ensure that the TWIC program is more effective and cost-efficient than existing measures or alternatives at enhancing maritime security"

GAO recommended:

"1: To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, the Secretary of Homeland Security should perform an internal control assessment of the TWIC program by (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. This assessment should consider weaknesses we identified in this report among other things, and include: (1) strengthening the TWIC program's controls for preventing and detecting identity fraud, such as requiring certain biographic information from applicants and confirming the information to the extent needed to positively identify the individual, or implementing alternative mechanisms to positively identify individuals; (2) defining the term extensive criminal history for use in the adjudication process and ensuring that adjudicators follow a clearly defined and consistently applied process, with clear criteria, in considering the approval or denial of a TWIC for individuals with extensive criminal convictions not defined as permanent or interim disqualifying offenses; and (3) identifying mechanisms for detecting whether TWIC holders continue to meet TWIC disqualifying criminal offense and immigration-related eligibility requirements after TWIC issuance to prevent unqualified individuals from retaining and using authentic TWICs.

2: To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, the Secretary of Homeland Security should conduct 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.

3: To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, the Secretary of Homeland Security should use the information from the internal control and effectiveness 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.

4: To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining

whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, the Secretary of Homeland Security should direct the Commandant of the Coast Guard to design effective methods for collecting, cataloguing, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities".

The full GAO TWIC report can be accessed at: http://www.gao.gov/new.items/d11657.pdf.

Testimony to the hearing by Stephen Lord, GAO Director for Homeland Security and Justice Issues can be found at: http://commerce.senate.gov/public/?a=Files.Serve&File_id=bd45b9aa-0397-4162-a991-508b727fb1a3

Seafarers Credentials

I – ILO C185

The International Labor Convention (ILO) C108 – Seafarers Identity Document adopted on 13 April 1958 allowed countries ratifying the Convention to issue Identity documents to seafarers of any nationality.

Ratifying countries would not require visas for seafarers holding such an identity document. Thus seafarers would be allowed shore leave and to join and leave their vessels without the need of visa formalities. Following ratification, C108 came into force on 19 February 1961. The Convention was ratified by 59 countries, the first being Tunisia on 26 October 1959 with 5 nations denouncing it.

Notably, one of the non-signatories was the United States of America (USA) and this along with other requirements on the part of the USA has meant that many owners insist that seafarers joining their vessels must hold dual USA C1/D visas. This is an onerous burden on shipping and on seafarers particularly so for those entering the industry as a first time seafarer. Among other non-signatories are China and the Philippines.

On 19 June 2003, C185 was adopted by the by ILO member governments. This convention had an entry into force date of 19 February 2005 with the first signatory being France followed by Hungary on 17 April and 19 August of 2004 respectively. Countries ratifying C185 are permitted to issue Seafarers Identity Documents (SID) to their own nationals only. However, they can issue SIDs to non-nationals who have been granted the status of permanent residence in the country.

With the coming into being of C185, C108 was closed for ratification with the last two countries to do so being India and Turkey on 17 January and 7 February of 2005. Under the C185 ratification terms, countries ratifying it, automatically denounce C108 in other words they must no longer recognize the provision of C108. Only a mere 18 countries have ratified C185 with one making a declaration of applicability and no denouncers. Like C108 before it, C185 allows seafarers who have been issued an SID to enjoy shore leave as well as joining, transferring to from or leaving their vessels without the need of a visa, but subject to certain conditions.

Countries that ratified C108 still recognize SIDs issued under it and some may even recognize SID's issued under C185, for example the United Kingdom as a visit to www.ukvisas.gov.uk/en/ecg/seafarers will adequately demonstrate.

However, there are also flies in the ointment with Brazil being hailed as one of them. Beware the seafarer who goes on shore leave with their C108 SID as they are fined unless they hold a visa in their passport for doing so.

C185 provides for essentially the same facilities as the 1958 Convention, namely “shore leave” enabling seafarers to go ashore in foreign ports after perhaps weeks or even months on board, and facilities for joining their ship or for transit across a country for professional reasons. The much needed changes of 2003 relate to the identification of the seafarers. They have radically enhanced the security features as well as the uniformity of the Seafarers’ Identity Document (SID) that countries are required to issue to their seafarers and lay down minimum requirements with respect to the countries’ processes and procedures for the issuance of SIDs.

In addition to the normal physical features for a modern machine-readable identity document, the new SID carries a fingerprint-based biometric template, which was adopted with the agreement of the world’s shipowner and seafarer organizations and must conform to an international standard enabling the biometric templates on a SID issued by one country to be correctly read by devices used in other countries. In addition, the border authorities around the world will be able to check the authenticity of a SID produced by a seafarer, as the new Convention enables them to verify information in the SID either by reference to the national electronic database in which each issued SID must be stored or through the national focal point of the country of issuance, who must be available 24 hours a day, seven days a week. The country issuing SIDs must in addition arrange for an independent evaluation of the administration of its issuance system to be carried out at least once every five years. The evaluation report is reviewed in the framework of the ILO with a view to the maintenance of a list of the countries that fully meet the minimum requirements laid down by the Convention.

Table 1 – 18 countries that have Ratified C185

	Ratification date
Albania	11:10:2007
Azerbaijan	17:07:2006
Bahamas	14:12:2006
Bosnia and Herzegovina	18:01:2010
Brazil	21:01:2010
France	27:04:2004
Hungary	30:03:2005
Indonesia	16:07:2008
Jordan	09:08:2004
Kazakhstan	17:05:2010
Republic of Korea	04:04:2007
Lithuania	14:08:2006
Madagascar	06:06:2007
Republic of Moldova	28:08:2006
Nigeria	19:08:2004
Pakistan	21:12:2006
Russian Federation	26:02:2010
Vanuatu	28:07:2006
Yemen	06:10:2008

II - GAO report on actions to address risks posed by seafarers

The following is an extract from the findings of GAO:

> *“The State Department and two components of the Department of Homeland Security (DHS), Customs and Border Protection (CBP) and the Coast Guard, are responsible for preventing illegal immigration at U.S. seaports and identifying individuals who are*

potential security risks. The International Labor Organization (ILO) adopted the Seafarers' Identity Documents Convention (ILO 185) to establish an international framework of seafarer identification documents and reduce their vulnerability to fraud and exploitation. GAO was asked to examine (1) measures federal agencies take to address risks posed by foreign seafarers and the challenges, if any, DHS faces; (2) the challenges, if any, DHS faces in tracking illegal entries by foreign seafarers and how it enforces penalties; and (3) the implementation status of ILO 185. GAO reviewed relevant requirements and agency documents on maritime security, interviewed federal and industry officials, and visited seven seaports based on volume of seafarer arrivals. The visits provided insights, but were not projectable to all seaports.

Federal agencies use a layered security strategy to address foreign seafarer risks, but opportunities exist to enhance DHS seafarer inspection methods. Federal actions include: (1) State Department screening of seafarer non-immigrant visa applicants overseas and (2) DHS advance screening of commercial vessels' seafarer manifests and admissibility inspections of all arriving seafarers. CBP conducts cargo vessel admissibility inspections on board the vessel without the benefit of tools to electronically verify a seafarer's identity or immigration status because of a lack of available connectivity to network communications in the maritime environment. DHS has prioritized the acquisition of a mobile version of this technology capability but expects it to take several years before the technology is developed and available. CBP agrees that obtaining this capability is important but has not assessed the risks of not having it. Until CBP obtains the capability, identifying the risks and options to address them could better position CBP in preventing illegal immigration at seaports. DHS faces challenges in ensuring it has reliable data on illegal entries by foreign seafarers at U.S. seaports and has not adjusted related civil monetary penalties. First, both CBP and Coast Guard track the frequency of absconder (a seafarer CBP has ordered detained on board a vessel in port, but who departs a vessel without permission) and deserter (a seafarer CBP grants permission to leave a vessel, but who does not return when required) incidents at U.S. seaports, but the records of these incidents varied considerably. The Coast Guard reported 73 percent more absconders and almost double the deserters compared to CBP for fiscal years 2005 through 2009. As a result, the data DHS uses to inform its strategic and tactical plans are of undetermined reliability. Second, CBP is responsible for imposing civil monetary penalties on vessel operators whose seafarers illegally enter the United States; however, as of December 2010, CBP and DOJ had not met legal requirements for adjusting the penalties for inflation. Officials reported taking steps to meet these requirements, but have not developed a plan with timelines for doing so. Such a plan would better position CBP and DOJ to demonstrate progress to comply with legal requirements. International implementation of ILO 185 has been limited--18 countries, representing 30 percent of the

global seafarer supply, have ratified ILO 185--and key ILO mechanisms to promote compliance are not expected to be in place until later this year. As of January 2011, the United States had not ratified ILO 185 largely due to concerns over a provision for facilitating visa-free shore leave for foreign seafarers. Perspectives varied among the four federal agencies GAO interviewed within DHS and the departments of State, Transportation, and Labor. Within DHS, the Coast Guard reported that it supported U.S. ratification, while CBP stated that ILO 185's lack of oversight did not serve U.S. law enforcement interests. The U.S. has recently undertaken an interagency review to consider ratification but has no timeline for completion. GAO recommends that DHS assess risks of not electronically verifying cargo vessel seafarers for admissibility, identify reasons for absconder and deserter data variances, and, with the Department of Justice (DOJ), develop a plan with timelines to adjust civil monetary penalties for inflation. DHS and DOJ concurred with GAO's recommendations.

GAO recommendations:

"To facilitate better agency understanding of the potential need and feasibility of expanding electronic verification of seafarers, to improve data collection and sharing, and to comply with the Inflation Adjustment Act, the Secretary of Homeland Security should direct the Commissioner of CBP to assess the national-security and other risks faced by CBP in the absence of technology to provide electronic verification as part of CBP's admissibility inspections for cargo vessel seafarers and identify options for addressing these risks and their costs".

The full GAO TWIC report can be accessed at:

http://www.gao.gov/new.items/d11195.pdf