



July 6, 2006

Docket Management Facility
U.S. Department of Transportation, Room Plaza 401
400 Seventh St., SW
Washington, DC 20590-0001

Re: TSA-2006-24191; Coast Guard 2006-24196

Dear Sir or Madam:

The American Chemistry Council is pleased to provide the following comments on the notice of proposed rulemaking regarding "Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector," 71 Fed. Reg. 29296 (May 22, 2006).

ACC members operate numerous facilities that are subject to the Coast Guard's regulatory program under the Maritime Transportation Security Act (MTSA). Our members will be significantly impacted by the TWIC as currently proposed. ACC member companies have been extremely proactive in implementing security measures at our facilities and have spent over \$3 billion in security enhancements since 9/11.¹

ACC and its members have enjoyed a long and cooperative relationship with the Coast Guard since well before the MTSA was enacted. ACC actively supported enactment of the MTSA, and we have been active participants in its implementation, both through the rulemaking process and more generally. In fact, ACC's Responsible Care® Security Code was the first Alternative Security Program approved for facilities under the MTSA. ACC member facilities regulated under the MTSA have worked successfully with their Captains of the Ports (COTPs) and have actively participated on Area Maritime Security

¹ The American Chemistry Council (ACC) represents the leading companies engaged in the business of chemistry. ACC members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. ACC is committed to improved environmental, health and safety performance through Responsible Care, common sense advocacy designed to address major public policy issues, and health and environmental research and product testing. The business of chemistry is a \$550 billion enterprise and a key element of the nation's economy. It is one of the nation's largest exporters, accounting for ten cents out of every dollar in U.S. exports. Chemistry companies invest more in research and development than any other business sector. Safety and security have always been primary concerns of ACC members, and they have intensified their efforts, working closely with government agencies to improve security and to defend against any threat to the nation's critical infrastructure.



Committees. An employee of an ACC member company has served for many years on the Chemical Transportation Advisory Committee, and is now CTAC's Vice Chair. ACC has also worked with productively with TSA in a variety of contexts.

ACC supports a reliable credentialing system at MTSA facilities, as required by Congress. We believe that the TWIC can be an important tool in furthering security at MTSA-regulated facilities and we support the overall development of this program. We do, however, have serious concerns about the TWIC proposal. While we recognize that the TWIC program will require changes at our members' MTSA-regulated facilities, we also believe that a flexible approach to implementing the TWIC requirements will make the most of these facilities' existing investments. The Conference Committee Statement of Managers for the MTSA emphasized that they had "provide[d] flexibility to the Secretary in administering the transportation security card program to take into account the unique circumstances and risks presented by particular segments of the transportation industry."² USCG and TSA should employ that flexibility to accommodate the actions previously taken at facilities and to avoid requiring unnecessarily expensive and disruptive changes. Our comments below explain in more detail how the two agencies can do that. We look forward to working with them to ensure that the TWIC program provides maximum net benefits to security.

Summary

ACC supports the concept of ensuring sufficient and appropriate vetting of all employees, including the subset of individuals that may require additional credentials for access to secure areas of MTSA-regulated facilities. The TWIC program, if properly developed and implemented, will meet our shared goal of enhancing security protection in these areas. As proposed, however, the TWIC program is far too broad in scope and will result in costs far greater than the already staggering costs estimated by USCG and TSA. ACC's comments will first explain the various factors contributing to these widespread impacts and resulting costs. We will then outline how USCG can appropriately narrow the scope of the program while ensuring adequate security enhancements by allowing facilities to limit application of the TWIC to MTSA-regulated portions of their facilities requiring a higher degree of security protection. We then address a number of other ways in which the proposed program could be improved.

In brief:

- It is critical for the TWIC final rule to clarify that facility owner/operators have broad flexibility to designate which portions of a facility will be deemed "secure areas" and therefore subject to the TWIC, and that USCG will readily approve revised Facility Security Plans (FSPs) containing these designations;

² H.R. Conf. Rep. No. 777, 107th Cong., 2d Sess. 81 (2002).

- The Coast Guard should adequately field test biometric “Smart Card” readers to assure consistent and satisfactory performance prior to requiring their deployment under the program;
- Companies should be allowed to grant facility access to employees and select contractors based upon ID credentials that the company has issued to them after they have obtained a TWIC;
- TSA needs to make clear its intentions regarding implementation of TWIC more broadly in the rail and vehicular contexts;
- USCG and TSA should consolidate all federal transportation worker credentials, and should preempt state regulation of the same subject matter;
- TSA needs to ensure adequate and convenient locations for the enrollment process, and should explore the concept of allowing facilities to be enrollment centers for their own employees and contractors;
- USCG and TSA should reduce the frequency of TWIC verification at MARSECs 1 and 2;
- USCG should not require owner/operators to obtain TWICs due to their access to Security Sensitive Information; and
- DHS should provide or support training on TWIC compliance approaches.

ACC’s recommended changes and clarifications would significantly reduce the cost and burden associated with the proposed rule. Otherwise, we believe the scope of the program, the untested nature of the biometric reader, and the multitude of individuals that will be subject to TWIC requirements will combine to create disruptions and costs far beyond those estimated by USCG and TSA.

In any event, we believe that additional compliance time will be required for the TWIC program, given:

- The need for proper field testing of the biometric readers; and
- The logistical challenge nationwide of processing applications and then issuing TWIC cards to hundreds of thousands of workers.

To adequately complete these steps and provide advance notice to owner/operators about the reliability of the biometric readers, we believe that USCG and TSA should allow an additional 18 months for compliance. This will enable the agencies to address these challenges and to ensure they have a workable program before the regulated community is required to implement its requirements.

I. TWIC AS PROPOSED WILL BE VERY COSTLY AND COULD DISRUPT FACILITY OPERATIONS

A. TWIC Costs Will Be Substantial and Have Been Underestimated

As the rulemaking analysis for this proposal estimates, the TWIC rule will cost about \$1 billion.³ The analysis also estimates that 40% of these costs – \$400 million – will be

³ 71 Fed. Reg. 29433.

experienced in the first year of implementation.⁴ Whatever year it is issued, the TWIC rule will be one of the most expensive regulations imposed that year by the federal government. Thus, its costs deserve heightened scrutiny to ensure that they are (i) accurately estimated; (ii) minimized; and (iii) reasonable in light of the benefits they may (or may not) produce.

The rulemaking analysis also makes clear that facilities will bear the lion's share – almost 40% -- of this cost.⁵ We expect that facilities will actually bear a much higher percentage, as it is likely that facilities will often wind up covering the cost of TWIC card expenses, including employee downtime, travel time and the actual cost of the cards. Thus ACC is particularly concerned about the costs of the rule, as should USCG. And yet, we believe that the proposal underestimates the number of people impacted and the upfront and ongoing costs of this program

For example, the analysis estimates that the cost of Smart Card reader purchase, software and implementation will account for between 36-52% of total facility costs.⁶ Remarkably, the same table includes *nothing* for recurring costs associated with such devices.⁷ This is a huge oversight, as operation and maintenance for such devices is likely to be enormous. Indeed, as discussed in Part II of our comments below, one ACC member that has deployed such devices outdoors has found that they fail, on average, three times per year. Clearly, these machines will have substantial recurring costs – even if facilities purchase multiple backup machines, significant costs will be required to swap in the backups while the malfunctioning machines are repaired. Yet this fact appears to be missing from the regulatory analysis.

Even if the Coast Guard is correct in its estimate that only some 750,000 individuals will require a TWIC, the scale of the effort to implement TWIC will be enormous. For example, a single ACC member facility has 12,000 employees that would need to obtain a TWIC under the proposal. The facility would need to (i) install enough biometric machines to process all of these persons daily, (ii) tie these systems into the existing access control system, and (iii) verify the validity of these persons' TWICs against TSA databases on varying frequencies as required by the rule. In addition to these employees, this plant and other chemical plants can often have huge numbers of contractors working onsite, especially for maintenance "turnaround" operations, where an entire plant or process unit may be shut down, overhauled and restarted. In such cases, as many as 1,800 individuals may be brought onsite for a month or two. Without a substantial surplus of biometric readers, the facility could face significant lines of employees and contractors awaiting approved entry each day.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.* at 29435.

⁷ *Id.*

B. TWIC Requirements Will Aggravate Worker Shortages

Our members already experience significant difficulties hiring enough trained and certified hazmat truck drivers, due to the costs and logistical difficulties involved in obtaining commercial drivers' licenses with hazardous materials endorsements. The TWIC program would add an additional licensing step, approval period and card purchase for drivers. This will exacerbate the trend of fewer drivers being willing to obtain these credentials, and will result in even slower services and higher costs. Other maintenance workers may well choose to stop working at MTSA-regulated facilities rather than obtain a TWIC.

This problem will particularly be true in rural areas, and in lines of work where contractors tend to be sole proprietorships, "mom and pops," or individuals hired out of union halls. It will also be severe in the Gulf Coast, where the chemical industry is concentrated, and where the market for qualified employees is extremely competitive in the wake of Hurricanes Katrina and Rita.

C. Delays in New Employee Hires

The proposal warns employers to give current or prospective employees "at least 60 days notice" of the need to obtain a TWIC. Where a new employee does not already have a TWIC, any hiring action could be delayed by two months while the facility and the prospective new employee waited for the new employee's TWIC to be issued. In some cases, it may be feasible for a new employee to be escorted in his or her new job functions, but in many other cases that will not be feasible. Simply telling a prospective hire that he or she will need to wait 60 days before being hired is unrealistic. Other firms that do not require a TWIC will often prove a better option for that individual. This leaves the facility owner/operator with unattractive choice of either losing a potential qualified candidate or paying him or her for a considerable amount of downtime while awaiting a TWIC card.

The Congressional Statement of Managers regarding the MTSA is quite short and addresses only a handful of issues. Indeed, virtually the entire discussion of Section 70105 (regarding TWIC) concerns the conferees' concerns "that transportation security cards are processed in an expeditious manner in order to prevent undue disruptions at our nation's ports."⁸ The conferees expected that DHS would be able to issue a TWIC "within seventy-two hours of receipt of the application."⁹ Clearly, 60 days is many more than three. Accordingly, the Coast Guard and TSA should do all within their power to expedite the issuance of TWICs within no more than 30 days of application. In addition, and particularly if this is not possible, USCG and TSA should authorize temporary unescorted access while an individual's application is pending, similar to the interim clearances that individuals can obtain while awaiting a Secret-level security clearance.

⁸ Conference Report, *supra* note 2, at 81.

⁹ *Id.*

D. TWIC Requirements Will Likely Lead Some Facilities to Discontinue Maritime Operations

While maritime operations are integral to the function of many ACC-member companies' facilities, at other, it may be feasible to shift those operations to rail or truck. The costs and burdens of TWIC compliance discussed above are leading some of those members to consider whether maritime operations at those facilities are worthwhile any longer. The Coast Guard should seriously and carefully consider whether, in such cases, safety and security in transit would be advanced by such a switch.

II. BIOMETRIC READERS NEED TO BE FIELD TESTED AND VALIDATED BEFORE FULL IMPLEMENTATION OF THE PROGRAM

It is unclear to what extent, during the technology evaluation portion of the TWIC program, USCG conducted testing on the reliability, accuracy and durability of the biometric readers. As these readers will be the linchpin nationwide to providing a quick and accurate scan of hundreds of thousands of people every day before they enter an MTSA workplace, it is essential that they be proven in the field well before facility owner/operators are required to purchase and deploy them.

The reliability and accuracy of the readers will hinge on whether the multiple units deployed at a facility can move people through the security system quickly and verify their credentials so that personnel are not required to "re-swipe" the cards to be read. Testing for reliability and accuracy should focus on ensuring that multiple units at a facility "communicate" with each other and the governmental database to facilitate people moving through various areas of the plant without having to stop and have their credentials verified multiple times.

The durability of the units will be extremely important, as they will often be operated in outdoor conditions, many of which will be harsh marine environments. One ACC member has reported that in limited use of biometric readers, a 300% repair rate annually is typical. If this becomes the norm for these systems, it virtually guarantees that multiple back-up systems will be required to keep a single facility access point operating, along with considerable ongoing maintenance costs, unless better systems can be developed, tested and deployed. USCG testing in these real-world cases, prior to requiring these units' use, is the only way to ensure that the TWIC program will work properly. Absent testing in advance, USCG will impose what could amount to a significant trial and error period that will neither enhance security nor keep costs manageable.

III. FACILITY OWNER/OPERATORS SHOULD BE FREE TO DETERMINE THE SECURE/RESTRICTED AREAS SUBJECT TO THE RULE

As the foregoing demonstrates, TWIC threatens to be a highly costly and disruptive rule. By far, the single most powerful tool to allow facilities to mitigate those costs and disruptions is to provide them with broad discretion to define the “secure areas” at their facilities where a TWIC will be required for unescorted access. By properly focusing the TWIC on those areas that need enhanced security, the overall cost and implementation burdens of the rule will be significantly reduced and the most critical areas will be afforded the enhanced security measures envisioned by this proposal. This single change will have a cascading effect that will directly reduce the impact and cost of numerous other program elements, ranging from time and resource requirements, to the number of employees required to obtain the cards, to the day-to-day logistics of processing people in the program.

The unavoidable question that arises in this connection is what constitutes the “secure area” referenced in the TWIC proposal and how that differs from the “restricted area” referenced in the existing MTSA rules. Thus far, the answer to that question is highly unclear.

The MTSA requires TWIC cards for unescorted access to the “secure areas” of a facility.¹⁰ However, the statute does not define the term, directly or indirectly,¹¹ and the current MTSA regulations do not even use it. Conversely, the statute does not use the regulatory term “restricted area.” Thus, the Coast Guard has discretion under the statute to define “secure area” and “restricted area” to mean the same thing or different things.

The proposal suggests that the Coast Guard intends for these terms to mean different things, since it does not equate secure and restricted areas, but instead would result in free-standing definitions of each term.¹² However, the proposal also suggests that “secure area” may be broader than “restricted area,” and may encompass any areas for which access controls are required.¹³ This would be a disaster from the perspective of

¹⁰ 46 U.S.C. § 70105(a)(1).

¹¹ Outside of 46 U.S.C. § 70105 (concerning TWICs), the only place the MTSA uses the term “secure area” is in § 70103(c)(3)(C)(ii), where it says facility plans must “include provisions for . . . establishing and controlling access to secure areas of the . . . facility.” But this reference does not answer the question of what areas should be considered “secure areas.” For one thing, it is not clear that Congress intended the “secure areas” in 46 U.S.C. § 70105 to be the same “secure areas” referred to in § 70103. For another, the fact that access controls must be implemented for “secure areas” does not prevent the Coast Guard from also requiring a lower degree of access control in other areas of the facility. Indeed, the Part 105 rules do establish a two-level set of access controls, with some degree of access control for the entire facility and a greater degree for “restricted areas.” Compare 33 C.F.R. § 105.255 with § 105.260.

¹² Compare the definition of “restricted area” in current 33 C.F.R. § 101.105 with the definition of “secure area” proposed for that section at 71 Fed. Reg. 29438.

¹³ The proposed definition of “secure area” is “the area . . . at a facility over which the owner/operator has implemented security measures for access control” 71 Fed. Reg. 29438. Also, the proposal integrates TWIC into the general provisions regarding access control found in 33 C.F.R. § 105.255, not the specific

costs, and also clashes with common sense, since any risk-based, layers-of-protection approach to security would lead to the conclusions (i) that there are many areas of a facility that require some degree of access control, but (ii) only the most sensitive areas require the degree provided by TWIC.

By contrast, Coast Guard personnel at the TWIC public meetings and in private conversations have generally suggested that “secure area” and “restricted area” are intended to be defined synonymously. They have further advised that the solution to the cost and logistical challenges of TWIC is for a facility to determine a way to narrow the scope of its “restricted area”.

Equating “secure area” with “restricted area” would still be quite problematic for many ACC member facilities. For purposes of the MTSA, many facility owner/operators decided to adopt a comprehensive view of what would be designated as a “restricted area” in their FSPs. This typically meant that “restricted areas” were established as the entire facility (i.e. the perimeter fence line). ACC members’ facilities are often quite large – sometimes measured in square miles – and include corporate offices, manufacturing process, rail and truck yards, storage facilities, etc., in addition to the area of the site that triggers the MTSA. Increased security measures are in place across these facilities, including restricted access and physical security. In most cases, however, the dock or other vessel interface that triggers MTSA jurisdiction is significantly removed from other operations at the facility.

While the plantwide “restricted area” approach made practical sense for some facilities’ development of FSPs, the view that “secure areas” are coextensive with “restricted areas” would now mean that all of the operations at these facilities would be subject to the additional requirements of TWIC. This would result in enormous waste and overkill, as, for example, TWICs could be required for accounts payable clerks who in their entire careers may never set foot near the maritime activities that trigger the MTSA.

USCG could solve the problem about TWIC coverage in either of two ways. The most direct and reliable solution would be to clarify in regulatory text that “secure areas” need not be coextensive with “restricted areas,” and could be narrower. As noted above, neither the MTSA itself, the existing MTSA rules, nor the purposes of the TWIC proposal require these terms to mean the same thing, or that “secure area” be a broader term than “restricted area.” The final TWIC rule could clarify these two points. ACC believes this is the preferable approach.

Alternatively, if the Coast Guard believes that “secure area” and “restricted area” are coextensive, it should merge the two concepts, and allow facilities to modify their FSPs to limit “restricted areas” to specific vessel interface operations that warrant a higher degree of security protection. In such instances, facility owner/operators would be able

provisions regarding restricted areas found in § 105.260. Indeed, the proposal does not make any changes to § 105.260.

to provide heightened physical security and restricted access (including TWIC) to these more security-sensitive areas, while continuing to apply existing security measures for the rest of the plant.¹⁴

To highlight the dramatically different impacts that could result from different applications of TWIC coverage, ACC offers several specific examples:

- At one ACC member facility, the entire facility is currently identified as a “restricted area.” Around 4,000 personnel a day enter the plant. However, only 400 – 500 personnel currently enter the plant’s vessel interface areas on a daily basis. Security measures are significant, and access is restricted, for the entire facility. However, only about 10% of the facility’s workers will ever enter the vessel interface area of the site. It would be costly and difficult for the facility to install biometric readers and screen each of the 4,000 employees every day. It would also be a waste of resources to require everyone entering the broader facility to obtain a TWIC, since 90% of them would never enter the vessel interface area. Importantly, it would not just be a waste of the facility’s resources. TSA and DOJ’s resources would also be wasted, as 90% of the time these agencies devoted to processing employees of this plant would have been spent unnecessarily. This waste would, of course, impact all other TWIC applicants, as time that could have been spent processing their applications would be spent on those of people who did not even need a TWIC.
- In a second example, a facility has a single barge loading dock where fewer than 100 employees work. The overall facility has implemented security access measures as part of its global security identification process for all employees and contractors. The facility could easily restrict physical access to the barge loading operation. Unless the plant can limit the application of the TWIC program to that area, everyone at the facility would be required to obtain a TWIC, and the company would have to scrap and replace its existing security access system, which was installed at great expense after 9/11.
- A third ACC member facility employs 2,000 people. Only two of these individuals are required to enter the barge dock that triggers MTSA jurisdiction. The barge dock is already fenced to limit access to it. Allowing this facility to

¹⁴ ACC is not necessarily arguing that the “restricted/secure area” must be exactly coextensive with the minimum area of a plant that is subject to MTSA jurisdiction – indeed, the restricted/secure area might well be smaller, consistent with the current definition of “restricted area” as being the area “identified by the [FSA] or the operator that require[s] limited access and a higher degree of security protection.” 33 C.F.R. § 101.105. If USCG took the view that the “restricted/secure” area for TWIC purposes could not be smaller than the minimum area of MTSA jurisdiction, then USCG would need to revisit its interpretation that MTSA jurisdiction must extend outward from the vessel interface to the first valve within containment. *See, e.g.*, USCG, NAVIGATION AND VESSEL CIRCULAR NO. 0303 (May 27, 2004), Enclosure 8, at 5. In many cases, that valve is quite far from the vessel interface and is situated with other, non-maritime-related operations.

limit the TWIC program to the barge dock would reduce the need for TWICs by two orders of magnitude, from 2,000 to two employees.

ACC conversations with USCG headquarters officials lead us to understand that USCG would support the second solution described above: allowing facility owner/operators to modify their FSPs as described above – maintaining a significant level of security for the entire facility, while enhancing security for narrower area of the site.¹⁵

ACC greatly appreciates USCG's understanding of this need and its informal support for facilities changing their FSPs along these lines. However, USCG needs to clearly state that recommendation in the final rule, as historically facilities have encountered strong pushback from their COTPs when they have attempted to amend their FSPs to narrow their "restricted areas." Formalizing the position that USCG is now advocating would provide certainty to facility owner/operators that USCG supports this needed flexibility and that revised plans will be expedited through USCG review. It would also provide clear direction to COTPs and USCG field personnel. ACC's suggests the following preambular language to accomplish this purpose:

"Facility owner/operators are encouraged to review, and revise as necessary, their Facility Security Plans to apply TWIC requirements to those portions of the site that (i) trigger MTSA regulation, (ii) can be reasonably separated through access controls from other parts of the facility; and (iii) require a higher degree of security protection. USCG will review and approve these changes to the FSP so long as the facility demonstrates that (i) it can maintain existing security at the balance of the facility, and (ii) restricted access controls (including TWIC access controls) have been provided for the area that will have heightened security."

IV. REGULAR FACILITY EMPLOYEES AND SELECT CONTRACTORS SHOULD NOT NEED TO USE A TWIC FOR SITE ACCESS

Day to day, the vast majority of people entering facilities will be the best-known and most trusted ones; i.e., regular employees and permanent or long-time contractors, many of which have worked for or with the company for decades. These individuals generally already have company-issued credentials which they are required to present in order to enter the facility. ACC agrees that all employees and contractors should have to obtain a TWIC to ensure their suitability for access to restricted areas; i.e., they should be subject to criminal, immigration and security/terrorism checks.

¹⁵ Many ACC members use the Responsible Care Security Code ASP, approved by the Coast Guard on Dec. 7, 2004. Once the TWIC rule is finalized, ACC will submit a revised ASP with a TWIC Addendum, as envisioned in proposed 33 C.F.R. § 101.121. ACC requests clarification regarding the steps that member companies using the ASP would be expected to take under the TWIC rule. At present, facilities using the ASP prepare operating procedures or other implementation documents that describe how a facility applies the ASP to its particular operations. Facilities do not submit these to USCG. ACC proposes that a facility using the ASP would revise its implementation documentation to discuss how it will adapt the ASP TWIC addendum to its situation, but that a facility would not need to submit this revised document to USCG.

We also believe, though, that once employees and contractors have obtained a TWIC, these personnel should be able to use a regular company ID for plant access, and should not have to present a TWIC each time. Companies have already invested enormous sums of money in their current access control systems, and should not have to completely revamp them to cope with every person entering the facility presenting a TWIC card. Requiring everyone to present a TWIC if they want unescorted access to secure areas of a facility will also lead to substantial backlogs and delays, as discussed above. A more reasonable approach would be to accept company-issued IDs from those who have them, and to maintain a more limited TWIC reader capacity for all other persons seeking unescorted access to secure areas of a facility.

At bottom, the function that TWIC really accomplishes is verification and evaluation of identity: it provides a high degree of assurance that the person claiming to be X really is X, and that X is the kind of person who should be allowed into a secure area. To provide the next step in the process -- ensure that only such persons actually gain access to a secure facility -- USCG should allow integration between TWIC and existing company access-control systems. For example, a company could, through its FSP:

- Require all of its employees and select contractors seeking unescorted access to secure areas of the facility to obtain a TWIC;
- Require such persons to submit the TWIC to the company for verification, in exchange for which the company would supply the person with a company-issued ID card; and
- Grant such persons unescorted access to secure areas based on those IDs.

As for periodic verification of such persons' TWICs, below ACC proposes that USCG and TSA reduce the frequency of such verifications at MARSECs 1 and 2. With less frequent verifications, employees and contractors being granted access with company-issued credentials could return to the facility with their TWICs as needed for verification. Under the proposed, weekly verification schedule for MARSEC 1, this may be barely feasible. Alternatively, a company could choose to retain possession of the persons' TWICs and verify them as frequently as rule requires (depending on MARSEC level). In any case, if such verification revealed that such a person's TWIC had been revoked, the company's access control system would automatically revoke the person's company-issued ID and the person would no longer have unescorted access to secure areas.

The MTSA gives USCG the discretion to accomplish ACC's proposed distinction between verification of identity and access control. Specifically, the statute provides that a person seeking unescorted access to a secure area of a facility must "hold[] a transportation security card issued under this section and is authorized to be in the area in accordance with the [facility's approved security] plan."¹⁶ Under ACC's proposal, these requirements would be satisfied: employees and select contractors would have to obtain a TWIC that would be verified on the same schedule as anyone else's TWIC, and they

¹⁶ 46 U.S.C. § 70105(a)(1)(A).

would need to be authorized to be in the secure area in accordance with the approved FSP, which would require them to submit (and maintain) the TWIC in order to obtain a company-issued ID, which would thereafter serve as their access key.

ACC recognizes that the difference between the TWIC proposal and ACC's is that the TWIC provides on site verification of identity by a biometric feature. However, facilities can provide a sufficiently high degree of identity verification of their own employees and select contractors by virtue of daily familiarity with these people. The additional degree of assurance provided by a TWIC is not required for such individuals. For anyone not issued a company ID, then the TWIC would obviously continue to be necessary for unescorted access.

V. TSA NEEDS TO CLARIFY ITS INTENT REGARDING IMPLEMENTATION OF TWIC IN THE RAIL AND VEHICULAR CONTEXTS

TSA has the authority to require TWICs for persons involved in hazmat transport by both rail and road. The proposal notes that, in many facilities, railroad operations terminate within (or pass through) restricted areas, and in even more cases, commercial trucks enter into restricted areas.¹⁷ The proposal also clarifies that such employees would need to obtain TWICs.¹⁸ The proposal also solicits comments on the benefit of expanding the TWIC program to other modes of transportation. As discussed above, many facilities are likely to define their secure/restricted areas narrowly, so as to limit the number of facility personnel and contractors who would have to pass through TWIC access points. While doing so will save many facilities money over the long term, establishing such new secure/restricted areas will often involve significant up-front capital costs for fencing and other access controls. If TSA proceeds in the near future to require all hazmat transport personnel to obtain TWICs and all receiving facilities to process such personnel through TWIC access points, the effort to narrow the secure/restricted areas may have been wasted. How facilities define their secure/restricted areas will often depend on what they will ultimately need to do regarding rail and vehicle access control. There may be no point in defining new, small secure/restricted areas if facilities just have to expand them again to encompass other transportation modes.

It would be extremely beneficial if TSA were to clarify its intent regarding TWIC in the rail and vehicular contexts, and to do so no later than issuance of the final TWIC rule.

VI. USCG AND TSA SHOULD CONSOLIDATE ALL FEDERAL TRANSPORTATION WORKER CREDENTIALS, AND SHOULD PREEMPT STATE REGULATION OF THE

¹⁷ 71 Fed. Reg. 29405.

¹⁸ *Id.*

SAME SUBJECT MATTER

As TSA considers expanding TWIC to other modes of transportation, it should be guided by the principle that there should be a single federal background check process and credential for hazardous material transportation workers. For example, TSA should integrate – to the maximum extent permitted by law – the TWIC program and the PATRIOT Act process for security threat assessments for hazardous materials endorsements for commercial drivers licenses. Likewise, TSA and Customs and Border Protection should integrate TWIC and CBP's Free And Secure Trade card program. The proliferation of different transportation credentials helps no one.

Relatedly, TSA and USCG should provide that TWIC would preempt any state programs for checking backgrounds or badging transportation workers. The preamble to the final MTSA rules, issued in 2003, discussed how the Coast Guard “reviewed the MTSA with a view to whether we may construe it as non-preemptive of State authority over the same subject matter.”¹⁹ It explained the Coast Guard's determination that, in the area of facility security, the MTSA preempted state rules that actually conflict with it or that “would frustrate an overriding need for Federal uniformity.”²⁰ As the Coast Guard declared there, “owners or operators of facilities . . . must have one uniform, national standard that they must meet.”²¹ While the TWIC program was not part of those rules, the TWIC program clearly is mandated by MTSA, and the Coast Guard's prior preemption discussion did not split hairs regarding the different requirements of the MTSA. To the contrary, the TWIC program is another example of the MTSA's “equipment[] and operating requirements” that the Coast Guard previously concluded must be preempted due to the overriding need for federal uniformity on the topic.²² Many, if not most, MTSA-regulated facilities are owned by companies with operations in multiple states, and their employees and contractors also are likely to work in, or move between, multiple states. As the original MTSA preamble explained, it would be “an unreasonable burden” for such companies and individuals “to comply with varying requirements . . . from state to state.” For these reasons, USCG and TSA should reaffirm the Coast Guard's 2003 findings regarding preemption and should rescind statements to the contrary in the TWIC proposal.²³

VII. TSA NEEDS TO ENSURE ADEQUATE AND CONVENIENT LOCATIONS FOR THE ENROLLMENT PROCESS

ACC is quite concerned about the logistics and cost of having such a significant number of employees and contractors needing access to an enrollment facility. This will be an even greater challenge during the initial phase of the program, when at least 750,000 people across the country will all be working through this process simultaneously for all

¹⁹ 68 Fed. Reg. 60468 (Oct. 22, 2003).

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *I.e.*, 71 Fed. Reg. 29436.

practical purposes. Further, we anticipate that, in many instances, the companies will end up paying employees to enroll in TWIC on company time, and at the company's expense. The fewer the number of TWIC enrollment centers, the more complicated and costly this process will be. The proposal does not identify where these centers will be located, and any situation where significant travel is required will be quite costly and disruptive of normal operations. These problems will be compounded by employees having to make two separate trips to the center, one to apply for a TWIC and one to pick up the card upon approval. ACC strongly encourages USCG to consider utilizing mobile enrollment centers that would provide some relief by minimizing the time and effort required to enroll and to obtain the cards. ACC also supports the proposal, advanced by Shell and NPRA, of allowing facilities to become the enrollment centers for their own employees and contractors, if they choose to do so.

VIII. THE PROPOSED VERIFICATION SCHEDULE IS TOO FREQUENT

The proposal has facilities verifying the validity of TWICs with TSA weekly for MARSEC 1 and daily for MARSECs 2 and 3. This is unduly frequent. By contrast, DOD's rules for validating the credentials of people approved to have access to classified information only require annual validation. The Coast Guard and TSA should reevaluate this frequency for MARSECs 1 and 2.

IX. TWIC AND SENSITIVE SECURITY INFORMATION

The National Maritime Security Advisory Committee cautioned the Coast Guard that it would be "impractical" to require all individuals with access to Sensitive Security Information (SSI) to have a TWIC, and the proposal "agree[d]" with this point, noting that the MTSA only requires the TWIC to apply to "an individual with access to sensitive security information *as determined by the Secretary*."²⁴ The preamble went on to say that the Coast Guard interpreted this language to allow that "only certain individuals who will require access to SSI hold a TWIC," adding that "[t]hese individuals are clearly identified by position in the NPRM."²⁵ In the case of facilities, these are the Facility Security Officer and other personnel with security duties.²⁶ The preamble also requested comment on whether owner/operators should have to obtain a TWIC because of their access to SSI.

ACC shares the concern expressed by the Advisory Committee, given the very broad regulatory definitions of SSI. Not all SSI is so sensitive that persons with access to it require the kind of background verification that TWIC will provide. ACC supports the proposal that FSOs and facility personnel with security duties obtain a TWIC. However, we strongly oppose requiring owner/operators – or anyone else, for that matter – to obtain a TWIC solely due to such persons' access to SSI.

X. Training

²⁴ 71 Fed. Reg. 29407, quoting 46 U.S.C. § 70105(b)(1)(E) (emphasis added).

²⁵ *Id.*

²⁶ Proposed 33 C.F.R. §§ 105.205, 105.210.

It will be essential, as the TWIC program is rolled out, for DHS to provide or support training for facility personnel charged with TWIC responsibilities. This is particularly true for the “backup processes” for making access control decisions if part of the TWIC system fails.²⁷ This training should not be mandatory “guidance,” but rather should aid facilities and their personnel in understanding the range of resources and approaches available to them.

* * *

ACC appreciates the opportunity to provide these comments regarding the TWIC program. If you have any questions regarding them, please do not hesitate to contact Ted Cromwell at 703-741-5246.

Sincerely,

Michael P. Walls
Managing Director
Regulatory & Technical Affairs

²⁷ See 71 Fed. Reg. 29414.