

already completed a risk assessment using a risk assessment tool other than those listed in § 101.510 must conduct a new assessment using one of those tools. Three commenters asked that the Coast Guard provide a list of security assessment tools that would satisfy all DHS and Coast Guard requirements.

The Coast Guard does not intend to approve security assessment tools or incorporate such tools by reference because we prefer to allow flexibility for industry to develop their own tools to meet their specific needs. We have provided a list of examples of security assessment tools in § 101.510; however, this list is not exhaustive. We do not require owners or operators to conduct security assessments using these tools as long as the assessments meet the requirements of these regulations. To clarify that the list in § 101.510 represents some, but not all, assessment tools available for facilitating security assessments, we have amended it to include the word "may."

It should be noted that the list in § 101.510 includes a no-cost, user-friendly, web-based, vulnerability-self-assessment tool designed by TSA. This tool was developed by TSA in coordination with other Federal agencies and members of academia and industry as a means to assist vessel and facility owners and operators in completing the security assessments mandated by these maritime security regulations. Any information entered into the tool will not be accessible by TSA or any other Federal agencies unless the owner or operator formally submits this information to TSA. TSA, in coordination with the Coast Guard, is developing guidance that will assist users of the TSA tool. At this time, TSA does not intend to publish a Notice of Proposed Rulemaking requiring the use of this tool.

One commenter asked for clarification of the terms "self assessments," "security assessments," "risk/threat assessments," and "on-scene surveys."

Risk/threat assessments and self assessments are not specifically defined in the regulations, but refer to the general practices of assessing where a vessel or facility is at risk. The assessments required in parts 104 through 106 must take into account threats, consequences, and vulnerabilities; therefore, they are most appropriately titled "security assessments." This title also aligns with the ISPS Code. To clarify that §§ 101.510 and 105.205 address security assessments required by subchapter H, we have amended these sections to change the term "risk" to the more accurate term "security." "On-scene

surveys" are explained in the security assessment requirements of parts 104, 105, and 106. As explained in § 104.305(b), for example, the purpose of an on-scene survey is to "verify or collect information" required to compile background information and "consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations." An on-scene survey is part of a security assessment.

One commenter stated that the temporary interim rule requirement to institute a photo identification card system for crewmembers is unreasonable because it will cost over \$2,000 and will be obsolete when the Transportation Worker Identification Credential (TWIC) requirement is enacted. One commenter stated that some ports are already establishing credentialing programs of varying complexity and scope and emphasized the need for the national TWIC program to be implemented as soon as possible.

The temporary interim rule does not require vessel or facility owners or operators to have a photo identification card system that is vessel or facility specific. The personal identification requirements of § 101.515 are well within the scope of the majority of current identification systems such as driver's licenses and union cards. Vessel and facility owners or operators can use any personal identification that meets the requirements of § 101.515; they do not have to develop their own card systems. Section 101.515 was meant to provide a temporary solution to the criteria for personal identification to facilitate access control until the TWIC criteria could be implemented. TSA is working closely with other agencies of DHS (e.g., the Coast Guard), agencies of DOT (e.g., MARAD), and other government agencies to develop the TWIC and its use to ensure that it can be a practical personal identification system for the transportation community.

Two commenters stated that our regulations will require employers to reissue identification cards when individuals grow beards or mustaches because the photo will not "accurately depict the individual's current facial appearance."

Facial hair may not necessarily alter the depiction of an individual on picture identification so much that the individual is no longer identifiable. If the individual depicted on the identification has changed his or her appearance to the extent that the individual is no longer accurately depicted, then a new identification card would be required.

One commenter suggested that commuter ticket books or badges could serve as a form of required identification for passengers on board ferries.

Personal identification remains a requirement in these regulations, as described in § 101.515, to ensure, if needed, the identification of any passenger. A ticket book or badge that meets the requirements of § 101.515 could serve as personal identification. To ease congestion for ferry passengers, we have included alternatives to checking personal identification as described in § 104.292. These alternatives, if used, can expedite access to the ferry while maintaining adequate security.

After further review, and based on comments from several other agencies and Coast Guard field units, we have amended § 101.515 by adding a new provision to clarify that the identification and access control requirements of this subchapter must not be used to delay or obstruct authorized law enforcement officials from being granted access to the vessel, facility, or OCS facility. Authorized law enforcement officials are those individuals who have the legal authority to go on the vessel, facility, or OCS facility for purposes of enforcing or assisting in enforcing any applicable laws. This authority is evident by the presentation of identification and credentials that meet the requirements of § 101.515, as well as other factors such as the uniforms and markings on law enforcement vehicles and vessels. Delaying or obstructing access to authorized law enforcement officials by requiring independent verification or validation of their identification, credential, or purposes for gaining access could undermine compliance and inspection efforts, be contrary to enhancing security in some instances, and be contrary to law. Failure or refusal to permit an authorized law enforcement official presenting proper identification to enter or board a vessel, facility, or OCS facility will subject the operator or owner of the vessel, facility, or OCS facility to the penalties provided in law. In addition, an owner or operator of a vessel (including the Master), facility, or OCS facility that reasonably suspects individuals of using false law enforcement identification or impersonating a law enforcement official to gain unauthorized access, should report such concerns immediately to the COTP.

Two commenters stated concerns regarding standards for seafarers' identification cards and other identifying documents. One commenter stated that the Coast Guard must ensure