

we have explicitly included a reference to the format in § 101.505(b).

One commenter wanted to know who will become the arbiter in the event of a disagreement between a vessel and a facility, or between two vessels, in regards to the Declaration of Security.

We do not anticipate this will be a frequent problem. The regulations do not provide for or specify an arbiter in the event that an agreement cannot be reached for a Declaration of Security. It is important to note that failure to resolve any such disagreement prior to the vessel-to-facility interface may result in civil penalties or other sanctions.

Five commenters suggested that we add language to the requirements for security systems and equipment maintenance in §§ 105.250 and 106.255 to allow facility and OCS facility owners or operators to develop and follow other procedures which the owner or operator has found to be more appropriate through experience or other means.

The intent of the security systems and equipment maintenance requirement is to require the use of the manufacturer's approved procedures for maintenance. If owners or operators have found other methods to be more appropriate, they may apply for equivalents following the procedures in §§ 105.135 or 106.130.

One commenter suggested that the Coast Guard establish additional criteria for certain expensive security equipment (such as access controls, lighting, and surveillance). The commenter said this would be helpful in ensuring a minimum compliance standard for those equipment elements that will be most costly to owners and operators.

Our regulations set performance standards. Some industry standards already exist or are being developed by trade or standards-setting organizations. Owners and operators may assess their own security needs and the measures that best meet those needs, given the particular characteristics and unique operations of their vessels or facilities.

One commenter stated that § 105.255(a) regarding access control should explicitly state that the implementation of security measures should be based on the type of cargo handled and the Facility Security Assessment.

We are not amending § 105.255(a) because, through the development of the Facility Security Assessment and Facility Security Plan, the cargo handled should be a primary consideration of a facility's vulnerability to a transportation security incident. The security measures implemented will be based on the Facility Security Assessment and Facility Security Plan,

which expressly account for the facility's specific operations.

We received nine comments dealing with facility access control as it pertains to identification checks. Seven commenters asked us to add regulatory language to stipulate what will be accepted forms of identification for representatives from Federal agencies, because there is no standardized requirement for these representatives to carry their agency identification at all times and some agencies believe an officer in uniform and carrying a badge should be sufficient identification to gain access to a facility. One commenter suggested that security plans include access control measures specifically aimed at fumigators.

As part of the requirements for access control in § 105.255(e)(3), a facility owner or operator must conduct a check of the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, Federal agency representatives, vendors (such as fumigators), personnel duly authorized by the cognizant authority, and visitors. We have provided minimum standards for identification in § 101.515, which must be met by all persons requesting access. This includes Federal agency representatives, and means that just a uniform will not be sufficient to meet the minimum standard set in § 101.515, and only those badges meeting that standard will be acceptable.

It should be noted that, with respect to Federal agency representatives, 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.

Seven commenters suggested that, instead of requiring disciplinary measures to discourage abuse of identification systems, the Coast Guard should merely require companies to develop policies and procedures that discourage abuse. One commenter opposed provisions of these rules relating to identification checks of passengers and workers. The commenter stated that these provisions threaten constitutional rights to privacy, travel, and association, and are too broad for their purpose. The commenter argued that identification methods are inaccurate or unproven and can be abused, and that the costs of requiring identification checks outweigh the proven benefit.

We recognize the seriousness of the commenters' concerns, but disagree that provisions for checking passenger and worker identification should be withdrawn. Identification checks, by themselves, may not ensure effective access control, but they can be critically important in attaining access control. Our rules implement the MTSA and the ISPS Code by requiring vessel and facility owners and operators to include access control measures in their security plans. However, instead of mandating uniform national measures, we leave owners and operators free to choose their own access control measures. In addition, our rules contain several provisions that work in favor of privacy. Identification systems must use disciplinary measures to discourage abuse. Owners and operators can take advantage of rules allowing for the use of alternatives, equivalents, and waivers. Passenger and ferry vessel owners or operators are specifically authorized to develop alternatives to passenger identification checks and screening. Signage requirements ensure that passengers and workers will have advance notice of their liability for screening or inspection. Vessel owners and operators are required to give particular consideration to the convenience, comfort, and personal privacy of vessel personnel. Taken as a whole, these rules strike the proper