

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.

Five commenters urged us to exempt OSVs and the facilities or OCS facilities they interact with from the Declaration of Security requirements because they do not pose a higher risk to persons, property, or the environment.

We disagree with the commenters, and we believe that the regulated vessels and the facilities that they interface with may be involved in a transportation security incident. In addition, Declarations of Security ensure essential security-related coordination and communication among vessels and facilities.

Two commenters asked us to amend § 106.250(f) to clarify that an expired Declaration of Security (§ 106.250(e)(2) or (e)(3)) must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security.

Although we agree that an expired Declaration of Security must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security, we believe that § 106.250 needs no further clarification. We do not preclude an OCS facility from executing a new Declaration of Security in accordance with § 106.250.

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 balance between implementing the MTSA's provisions for deterring transportation security incidents and preserving constitutional rights to privacy, travel, and association.

Four commenters asked for amendments to §§ 105.255(c)(2) and 106.260(c)(2) to include coordination with aircraft identification systems, when practicable, in addition to coordination with vessel identification systems as a required access control measure.

We agree with the commenters, and have amended §§ 105.255(c)(2) and 106.260(c)(2) to reflect this clarification. Most facilities, including OCS facilities, are accessible by multiple forms of transportation; therefore, coordination with identification systems used by those forms of transportation should enhance security.

One commenter asked if the Coast Guard would issue guidelines on screening.

The Coast Guard intends to coordinate with the Transportation Security Administration (TSA) and the Bureau of Customs and Border Protection (BCBP) in publishing guidance on screening to ensure that such guidance is consistent with intermodal policies and standards of TSA, and the standards and programs of BCBP for the screening of international passengers and cargo. Additionally, TSA is developing a list of items prohibited from being carried on board passenger vessels.

One commenter asked if there is a difference between the terms "screening" and "inspection" as used in § 104.265(e)(2), requiring conspicuously posted signs.

In 33 CFR subchapter H, the terms "screening" and "inspection" fully reflect the types of examinations that may be conducted under §§ 104.265, 105.255, and 106.260. Therefore, both terms are included to maximize clarity.

Eight commenters suggested that access control on board OCS facilities only be required when an unscheduled vessel is forced to discharge passengers for emergency reasons, and that the provisions of § 105.255 and § 106.260 be the responsibility of the shoreside facility and the vessel owner. The commenter stated that the need to duplicate the process at the facility is wasteful. The commenters asked for amendments to § 105.255 and § 106.260 in order to make clear that security controls should be established shoreside.

The Coast Guard believes that access control must be established to ensure that the people on board any vessel or facility are identified and permitted to be there. We recognize that access control and personal identification checks at both the shoreside and OCS facility could be duplicative, and did not intend to require this duplication, unless needed. Our regulations provide the flexibility to integrate shoreside screening into OCS facility security measures. We note, however, that the OCS facility owner or operator retains ultimate responsibility for ensuring that access control measures are implemented. This means that where integrated shoreside screening is implemented, the OCS facility owner or operator should have a means to verify that the shoreside screening is being done in accordance with the Facility Security Plan and these regulations. Even if integrated shoreside screening is arranged, the OCS Facility Security Plan must also contain access control provisions for vessels or other types of transportation conveyances that do not regularly call on the OCS facility or