

interested parties and agencies to ensure that such a requirement would not have a negative impact on OEM efforts to improve vehicle security.

ETI commented that OEMs have known for many years that security could not be used as an excuse to require the vehicle to be towed to the dealership for a special process and thus deny the aftermarket from participating in computer replacement or reprogramming. ETI further commented that there is no need to delay this requirement until 2007, as suggested by at least one OEM. ETI commented that OEMs have had ample time to design vehicle ignition systems that can be started after a computer change or reprogramming event.

American Honda commented that vehicle theft is of particular concern to Honda given that Honda vehicles have a particularly high theft rate in the U.S. and abroad. Honda has committed significant resources to reducing vehicle theft for its vehicles and recent data indicates that the theft rate for Honda vehicles has been significantly reduced since immobilizer systems have been installed on Honda vehicles. Honda attributes the success of their immobilizer systems to the considerable control process they incorporate to protect the proprietary information with their licensed dealers. Honda is concerned that they would not be able to put in place similar controls for the aftermarket and would be left with no course of action against third parties if security agreements were violated. Honda commented that they have been in contact with law enforcement agencies, the insurance industry and the National Highway Traffic Safety Administration to gather their expert opinions on the matter and encourages EPA to do the same.

American Honda commented that because of the issues outlined above, they strongly oppose the proposed requirement to release information to the aftermarket on how to obtain information to reinitialize Honda vehicles, other than instructing the customer to return to a licensed Honda dealer. The Aftermarket Consortium reiterated its support for making anti-theft and re-initialization procedures available to the aftermarket, including those companies that rebuild ECUs. They state that without the ability to initialize the system, the aftermarket service provider cannot complete the repair of the vehicle. Currently 900,000 rebuilt ECUs are sold annually. If rebuilding facilities are not able to initialize the anti-theft system, they will not be able to provide these services. They state that they are well aware of

the concerns regarding the integrity of the anti-theft system. However, many companies allow the initialization of the system using a "black box" that avoids the need to reveal anti-theft codes.

The Service Technicians Society (STS) submitted written comments in support of making anti-theft and re-initialization procedures and information available to aftermarket service providers, so that the motorist can drive away from the service facility after an OBD check or repair is made.

The Highway Loss Data Institute (HLDI) submitted written comments voicing their opposition to the release of any information related to anti-theft systems to the aftermarket. HLDI commented that their organization has monitored the effectiveness of anti-theft devices for many years. Their data indicates a significant decrease in automobile theft with the installation of vehicle anti-theft systems. HLDI further commented that the release of this information to the aftermarket would seriously compromise the effectiveness of anti-theft systems. HLDI is concerned that it would be difficult to confine the release of the information only to the aftermarket and the release of this information would inevitably increase access to people involved in vehicle theft. HLDI is also concerned about the premium discounts some insurance providers make available to vehicle owners. HLDI commented that insurers would be forced to reassess the appropriateness of these discounts if OEMs must publish the codes and other information necessary to reinitialize an anti-theft system. Finally, HLDI commented that EPA should rescind any provision that requires OEMs to make available anti-theft information available to the aftermarket.

Written comments were received by the Advocates for Highway and Auto Safety (Advocates) after the close of the August 27, 2001 comment period. In their comments, the Advocates expressed concern for any provision that would require the release of anti-theft information. In particular, the Advocates are concerned about the posting of anti-theft system codes and other sensitive information on the World Wide Web. Even if the information can be encrypted, this will not ensure that the information will not fall into the hands of vehicle thieves. The Advocates recommend that EPA refrain from adopting the portions of the proposal that would require the publication of anti-theft codes and information by the OEMs. Further, the Advocates comment that EPA consult with NHTSA and other interested parties regarding other means to achieve

EPA's goal. The Advocates commented that one option might be to require that anti-theft and emission-related functions be separately configured so that the maintenance and repair of one system does not affect the other.

*EPA Decision:* As stated in the preamble to the proposal, EPA is sensitive to finalizing any provision that would jeopardize the intent of any OEM anti-theft system. However, we also believe that vehicle design on at least some OEM vehicles would prevent an aftermarket technician from completing an emissions-related repair without the ability to re-initialize a vehicle's anti-theft system. As we noted in the proposal, re-initialization is critical to the ability of an aftermarket technician to complete an emission-related repair. A vehicle that cannot be driven away from the shop has not been fully repaired. Therefore, this information and/or the ability to perform this service must be made available to the aftermarket in a timely and cost effective manner. In order to allow OEMs maximum protection of the integrity of their anti-theft systems, EPA will finalize the following provisions for the availability of anti-theft system information. OEMs shall make available computer or anti-theft system initialization information necessary for the proper installation or repair of on-board computers or the repair or replacement of any other emission-related part on motor vehicles that employ integral vehicle security systems. OEMs are not required to make this information available on the OEM's Web site unless they choose to do so. However, the OEM's Web site shall contain information on obtaining the information and/or the ability to perform re-initialization.

Beginning with the 2008 model year, we require that all OEM systems will be designed in such a way that no special tools or processes will be necessary to perform re-initialization. In other words, EPA expects that the re-initialization of vehicles can be completed with generic aftermarket tools, a pass-through device, or an inexpensive OEM-specific cable. This model year cut-off is consistent with the requirement to complete the phase-in of the SAE J2284-3 CAN requirement as discussed in section 18 of this document. We believe it is reasonable to allow for additional leadtime through the 2007 model year to allow those OEMs who need additional time to reconfigure their vehicle systems in such a way that the release of anti-theft information can be accomplished without posing a threat to the integrity of the system and without special tools or an OEM-specific tool. Therefore, an