SUNSI Review Complete
Template = ADM-013
E-RIDS=ADM-03
ADD: Paul Goldberg, Adelaide Giantelli, Paul Michalak, Gina Davis

COMMENT (6)
PUBLICATION DATE: 11/14/2019
CITATION 84 FR 64113

PUBLIC SUBMISSION

As of: 2/20/20 7:44 AM
Received: February 18, 2020
Status: Pending_Post
Tracking No. 1k4-9f3g-od5j
Comments Due: February 18, 2020
Submission Type: Web

Docket: NRC-2018-0170
NUREG-2155, Revision 2, “Implementation Guidance for 10 CFR Part 37, Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material"

Comment On: NRC-2018-0170-0001
Guidance for Implementation of Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material

Document: NRC-2018-0170-DRAFT-0006
Comment on FR Doc # 2019-25163

Submitter Information

Name: Anonymous Anonymous
Address:
578 N. Indiana Ave.
Crown Point, IN, 46307
Email: David.Tebo@TeamInc.com

General Comment

We offer the following comments regarding the draft issuance of NUREG-2155, Rev. 2. The following comments are specifically in respect to the guidance offered in NUREG 2155 Rev. 2 draft concerning 10 CFR 37.53(b) regarding disabling of the vehicle. The guidance currently provides examples of acceptable vehicle disabling methods including "trailer hitch locks, wheel locks ("boots"), steering wheel locks (clubs) or methods to disable the vehicle's engine". It further states "the licensee cannot consider the removal of a standard key from a vehicle's ignition sufficient for disabling a vehicle's engine because a vehicle can be started without the key using, for example, a duplicated key or hot-wiring techniques".

The regulation currently states, "Licensees shall not rely on the removal of an ignition key to meet this requirement". NUREG 2155 use of the terminology "standard key" is vague and should include more clarity to perhaps define the "standard key" as an ignition key only employing a conventional notched lock and tumbler ignition locking method. Current security methods employed in more and more newer model vehicles (our research indicates most all vehicles manufactured since 2012) utilize sophisticated secure coded linked electronic communication methods (i.e. chip) imbedded in a key like holder. In many cases the vehicles are also considered keyless since nothing must be inserted into the vehicle ignition in order to start the vehicle. These systems are far superior to the old key tumbler ignition systems since the vehicle computer system must recognize this "chipped" device (key) and only that device (key) in order to start and allow mobilization of the

vehicle.

As stated in answer A.1. to the 37.53(b) regulation in the NUREG, NRC has acknowledged these new advances in ignition/key technology as being able to provide additional barriers that would cause delay. However, the guidance also states a licensee would need to request exemption from 37.53(b) for each specific vehicle, including addressing the possibility of hot-wiring or other techniques to defeat the system.

Discussions held with at least one major vehicle manufacturer (GM) indicates, based on their experience, vehicle thieves no longer consider or utilize hot-wiring techniques due to the sheer number of wires incorporated in the newer model vehicles. Finding and identifying the correct wire to cut takes too much time. Typical techniques now include removal of the ignition switch and replacement with one of their own allowing the prospective thief to utilize his own key to start the vehicle. However, with the computer encoded chipped key system, the vehicles computer would need to be reprogrammed to recognize the new ignition/key system. Although there are apparently methods available to reprogram the computer system, doing so requires access to the computer and time to reprogram. Therefore, even replacing the ignition switch does not provide a means to immediately steal a vehicle. Licensees should however address methods (i.e. procedures) for controlling access to and preventing unauthorized duplication of the computer encoded chipped keys since a duplicate computer encoded key can be used to start and subsequently steal the vehicle. For example, licensees could have procedures in place that establish protocol for only authorized individuals to acquire a duplicate key for a specific vehicle.

Lastly, for large licensees, the number of vehicles requiring exemption could place a huge burden not only on the licensee but also on NRC, in submitting and replying to each specific exemption for each specific vehicle. For example, a licensee possessing 500 vehicles in their fleet would need to request 500 separate exemption requests under the current guidance. Any newly acquired replacement or additional vehicles would also require additional exemption requests to be filed.

We therefore request the revision to the NUREG-2155 guidance recognize the new computer encoded key and keyless technologies as acceptable means of disabling the vehicle and providing a viable means of delaying the effort without the need for requiring exemption. The newer technology has been in place for enough time for sufficient information to be acquired as indicated above and has proven to provide the required means of disabling the vehicle and delaying the effort. The need for exemption should no longer be necessary, and considering the potential burden, be removed from the guidance and requirements.