For the first administrative review of any order, there will be no assessment of antidumping or countervailing duties on entries of subject merchandise entered, or withdrawn from warehouse, for consumption during the relevant provisional-measures ''gap'' period, of the order, if such a gap period is applicable to the period of review.

Interested parties must submit applications for disclosure under administrative protective orders in accordance with 19 CFR 351.305. On January 22, 2008, the Department published *Antidumping and Countervailing Duty Proceedings: Documents Submission Procedures; APO Procedures,* 73 FR 3634 (January 22, 2008). Those procedures apply to administrative reviews included in this notice of initiation. Parties wishing to participate in any of these administrative reviews should ensure that they meet the requirements of these procedures (*e.g.,* the filing of separate letters of appearance as discussed at 19 CFR 351.103(d)).

Any party submitting factual information in an antidumping duty or countervailing duty proceeding must certify to the accuracy and completeness of that information. *See* section 782(b) of the Act. Parties are hereby reminded that revised certification requirements are in effect for company/government officials as well as their representatives in all segments of any antidumping duty or countervailing duty proceedings initiated on or after March 14, 2011. *See Certification of Factual Information to Import Administration During Antidumping and Countervailing Duty Proceedings: Interim Final Rule,* 76 FR 7491 (February 10, 2011) (''*Interim Final Rule*''), amending 19 CFR 351.303(g)(1) and (2). The formats for the revised certifications are provided at the end of the *Interim Final Rule.* The Department intends to reject factual submissions in any proceeding segments initiated on or after March 14, 2011 if the submitting party does not comply with the revised certification requirements.

These initiations and this notice are in accordance with section 751(a) of the Act (19 U.S.C. 1675(a)) and 19 CFR 351.221(c)(1)(i).

Dated: August 20, 2012.

Gary Taverman,

Senior Advisor for Antidumping and Countervailing Duty Operations.

[FR Doc. 2012–21499 Filed 8–29–12; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 070321067–2100–03]

NIST Federal Information Processing Standard (FIPS) 140–3 (Second Draft), Security Requirements for Cryptographic Modules; Request for Additional Comments

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice and Request for Comments.

SUMMARY: The National Institute of Standards and Technology (NIST) seeks additional comments on specific sections of Federal Information Processing Standard 140–3 (Second Draft), *Security Requirements for Cryptographic Modules,* to clarify and resolve inconsistencies in the public comments received in response to the **Federal Register** (74 FR 91333) notice of December 11, 2009. The draft standard is proposed to supersede FIPS 140–2.

DATES: Comments must be received on or before October 1, 2012.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Dr. Michaela Iorga, 100 Bureau Drive, Mail Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Electronic comments may also be sent to: *FIPS140-3@nist.gov,* with a Subject: ''Additional *Comments-FIPS 140–3 (Second Draft*).''

The current FIPS 140–2 standard can be found at: *http://csrc.nist.gov/publications/PubsFIPS.html.*

FOR FURTHER INFORMATION CONTACT: Dr. Michaela Iorga, Computer Security Division, 100 Bureau Drive, Mail Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930, Telephone (301) 975–8431.

SUPPLEMENTARY INFORMATION: FIPS 140–1, *Security Requirements for Cryptographic Modules,* was issued in 1994 and was superseded by FIPS 140–2 in 2001. FIPS 140–2 identifies requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data), and a diversity of application environments.

In 2005, NIST announced that it planned to develop FIPS 140–3 and solicited public comments on new and revised requirements for cryptographic systems. On January 12, 2005, a notice was published in the **Federal Register** (70 FR 2122), soliciting public comments on a proposed revision of FIPS 140–2. The comments received by NIST supported reaffirmation of the standard, but suggested technical modifications to address advances in technology that had occurred after the standard had been approved. Using these comments, NIST prepared a Draft FIPS 140–3 (hereafter referred to as the ''2007 Draft''), which was announced in the **Federal Register** (72 FR 38566) for review and comment on July 13, 2007.

Using the comments received in response to the July 13, 2007, notice and the feedback on requirements for software cryptographic modules obtained during the March 18, 2008, ''FIPS 140–3 Software Security Workshop,'' NIST developed the ''Revised Draft FIPS 140–3'' (hereafter referred to as ''2009 Draft''), that was announced in the **Federal Register** (74 FR 65753) on December 11, 2009. The 2009 Draft and its Annexes and can be found at: *http://csrc.nist.gov/publications/PubsDrafts.html.*

The comments received in response to the December 11, 2009, request for comments suggested either modifying requirements or applying the requirements at a different security level. Some comments asked for clarification of the text of the standard, and some recommended editorial and formatting changes. None of the comments received opposed the approval of a revised standard.

During the process of addressing the public comments received in response to the Request for Comments published in the **Federal Register** on December 11, 2009 (74 FR 65753), NIST determined that additional feedback is required to resolve gaps and inconsistencies between the comments for particular sections of the ''Second Draft FIPS 140–3.'' As a result, NIST is requesting additional public comments on several sections, as indicated below in the Request for Comments section of this notice, to support comment resolution. Comments on any sections of the ''Second Draft FIPS 140–3'' not identified in the Request for Comments section will not be considered.

Request for Comments: Even though NIST has resolved a majority of the issues raised by the public comments on the ''2009 Draft,'' NIST is requesting additional comments only on the following sections and sub-sections to resolve gaps and inconsistencies between the comments.

4.2.2 Trusted Channel—the comments suggested that NIST should not mandate the implementation of a trusted channel at Security Level 3 and

4 for all modules. NIST is proposing deletion of the requirement, but to allow for adequate, comparable security, is proposing the addition of an optional ''Remote Control Capability.'' The proposed Remote Control Capability section would specify requirements addressing the module's ability to process logons, send service requests to, and receive service responses from a remote module without compromising security. If the Remote Control Capability is supported, this section would mandate the use of a Trusted Channel at Security Level 3 and 4. NIST would appreciate comments on the proposed approach.

4.3.1 Trusted Role—the comments raised a variety of different concerns, reflecting different interpretations of the purpose of the Trusted Role. To address these concerns NIST is proposing the deletion of the Trusted Role and replacement with a Self-initiated Cryptographic Capability, configured and activated by the Crypto Officer that would be preserved over rebooting or power cycling of the module. The capability would provide the module with the ability to perform cryptographic operations including Approved and Allowed security functions without external operator request. NIST would appreciate comments on the proposed approach.

4.7 Physical Security—Non-Invasive Attacks—the comments received suggest substantial changes that would either weaken or strengthen the impact of these requirements. Comments received included stronger security requirements for Security Level 3 and 4, making the section mandatory for all cryptographic modules, including the Security Level for this section as part of the overall Security Level, while other comments suggested not addressing non-invasive attacks within the standard. NIST would appreciate general and specific comments on the requirements to address non-invasive attacks.

4.8.4 Sensitive Security Parameter (SSP) Entry and Output—the comments received raised a variety of different concerns, reflecting different interpretations of the requirements on SSPs that are entered into or output from a module. SSP entry and output requirements depend on whether the SSP is entered or output manually or electronically, and whether the SSP is distributed manually or electronically. New technologies have called into question this taxonomy of SSP entry and output methods. NIST would appreciate comments on the most appropriate way to categorize these methods, and the appropriate requirements for each method.

Annex B, Section: Operator Authentication Mechanisms—the comments received indicated that the specification for the strength of the operator's authentication method was incomplete, particularly with respect to biometrics. For biometric authentication, NIST proposes the use of a Liveness Detection method associated with the Session False Match Rate for one attempt and the Generalized False Accept Rate for multiple attempts in one minute. NIST would appreciate comments on the proposed approach.

Comments on sections not specifically listed in this notice will not be considered.

Prior to the submission of the FIPS 140–3 to the Secretary of Commerce for review and approval, it is essential that consideration is given to the needs and views of the public, users, the information technology industry, and Federal, State and local government organizations. The purpose of this notice is to solicit such views on specific sections of the ''2009 Draft.''

Authority: Federal Information Processing Standards (FIPS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 and the Federal Information Security Management Act of 2002 (Pub. L. 107–347).

E.O. 12866: This notice has been determined not to be significant for the purpose of E.O. 12866.

Dated: August 24, 2012.

Willie E. May,

Associate Director for Laboratory Programs.

[FR Doc. 2012–21461 Filed 8–29–12; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 120817356–2356–01]

Request for Comments on U.S. Technical Participation in the 14th Conference of the International Organization of Legal Metrology (OIML)

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) seeks comments concerning U.S. technical participation in the 14th Conference of the International Organization of Legal Metrology (OIML). This conference is held once every four years and was last held in 2008.

Interested parties are requested to review and submit comments on the 24 OIML Recommendations and Documents on legal measuring instruments that will be presented for ratification by the Conference. Comments may also be submitted on other issues relevant to the Conference.

DATES: Written comments should be submitted to the NIST International Legal Metrology Program no later than Friday, September 21, 2012, at 5 p.m. Eastern Time. The 14th OIML International Conference of Legal Metrology will be held in Bucharest, Romania, Wednesday, October 3 through Thursday, October 4, 2012.

ADDRESSES: Written comments should be sent to the International Legal Metrology Program, Office of Weights and Measures, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 2600, Gaithersburg, MD 20899–2600. Comments may also be submitted via email to *ralph.richter@nist.gov.*

FOR FURTHER INFORMATION CONTACT: Mr. Ralph Richter, International Legal Metrology Program, Office of Weights and Measures, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 2600, Gaithersburg, MD 20899–2600; telephone: 301/975–3997; fax: 301/975–8091; email: *ralph.richter@nist.gov.*

SUPPLEMENTARY INFORMATION:

Background

The International Organization of Legal Metrology (OIML) is an intergovernmental treaty organization in which the United States and 56 other nations are members. Its principal purpose is to harmonize national laws and regulations pertaining to testing and verifying the performance of legal measuring instruments used for equity in commerce, for public and worker health and safety, and for monitoring and protecting the environment. The harmonized results promote the international trade of measuring instruments and products affected by measurement.

The U.S. Department of State has delegated technical participation in OIML to the National Institute of Standards and Technology. NIST coordinates participation of U.S. manufacturers, users of weighing and measuring instruments, legal metrology officials and other U.S. stakeholders in the technical work of OIML by circulating draft voluntary standards