DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: [070321067–91333–02]

Announcing Revised Draft Federal Information Processing Standard (FIPS) 140–3, Security Requirements for Cryptographic Modules

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) announces the Revised Draft Federal Information Processing Standard 140–3, Security Requirements for Cryptographic Modules, for public review and comment. The draft standard, designated ''Revised Draft FIPS 140–3,'' is proposed to supersede FIPS 140–2.

DATES: Comments must be received on or before March 11, 2010.

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.* The proposed revised standard can be reviewed electronically at *http://csrc.nist.gov/publications/PubsDrafts.html.* The complete set of all comments received in response to the July 2007 notice and NIST's responses to these comments may be accessed at *http://csrc.nist.gov/groups/ST/documents/CommentsFIPS140–3_draft1.pdf.* 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SUPPLEMENTARY INFORMATION: FIPS 140–1, Security Requirements for Cryptographic Modules, was issued in 1994 and was superseded by FIPS 140–2 in 2001.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.

Under NIST's Cryptographic Module Validation Program (CMVP), over 2000 modules have been tested by accredited private-sector laboratories and validated as conforming to FIPS 140–1 and FIPS 140–2. FIPS 140–2 provided that it be reviewed within five years to address new and revised requirements that might be needed to meet technological and economic changes.

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 for review and comment in the **Federal Register** (72 FR 38566) on July 13, 2007. NIST developed the Revised Draft FIPS 140–3 that is announced in this notice 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 organized by NIST.

Comments and questions regarding the 2007 Draft were submitted by approximately 45 entities, including two U.S. federal government organizations, two government organizations of other countries, thirty private sector and research organizations, ten private individuals, and one or more anonymous reviewers. These comments have all been made available by NIST at *http://csrc.nist.gov/groups/ST/documents/CommentsFIPS140–3_draft1.pdf.*

None of the comments opposed the approval of a revised standard. Some comments asked for clarification of the text of the standard or recommended editorial and formatting changes. Other comments suggested modifying requirements, or applying the requirements at a different security level. All of the suggestions, questions and recommendations within the scope of the FIPS revision were carefully reviewed, and changes were made to the standard, where appropriate. Some reviewers submitted questions or raised issues that are related but outside the scope of this FIPS. Comments that were outside of scope of the FIPS revision were deferred for later consideration in the context of the NIST/CMVP supporting documents.

The primary interests and issues that were raised in the comments included implementability, testability, performance, usability and cost. Detailed technical comments covered issues including the following: Authentication mechanisms; non-invasive attacks; random bit generators (RBGs); randomness of Initialization Vectors (IVs); operating system requirements; zeroization; status indicators; issues regarding the cryptographic module boundary and computing environment; and issues pertaining to self-testing requirements.

The following is a summary and analysis of the comments received and NIST's responses to them:

Comment: The 2007 Draft required the module to directly prevent the selection of weak passwords for password-based authentication mechanisms. Eighteen commenters stated that this requires standardized guidance on weak passwords and Personal Identification Numbers (PINs) and also implies that modules are required to store multi-language dictionaries, which is impractical in many cases.

Response: NIST removed the requirement that the cryptographic module directly prevent selection of weak passwords.

Comment: The 2007 Draft required that default authentication data be unique per module unit delivered if the module employs default authentication data to control access to the module for first-time authentication. Six commenters stated that this is an onerous requirement for vendors who deliver high volume products, and is unnecessary given the requirement to change the authentication data upon first use.

Response: NIST removed the requirement that the default authentication data be unique per module unit delivered.

Comment: The 2007 Draft specified Mitigation of Simple Power Analysis (SPA) attacks at Security Level 4. Eight commenters stated that this requirement should be introduced at a lower level (Security Level 2 or 3) for consistency with tamper evidence requirements, with stronger requirements at Security Levels 3 and 4. Similarly, the 2007 Draft specified that Mitigation of Differential Power Analysis (DPA) attacks is required starting with the Security Level 4. Eight commenters stated that this requirement should be introduced at Security Level 2 or 3.

Response: The tamper evidence mechanisms specified at Security Level

2 provide security against an unprepared attacker. While SPA and DPA attacks leave no physical traces of the attack, they require, in addition to access to the module's power line, minimum equipment to collect the data; therefore, the attacker has to be prepared with appropriate equipment. NIST determined that protection against non-invasive attacks is required starting with the Security Level 3 to provide consistent protection for the modules Critical Security Parameters (CSPs).

Comment: Four comments were received about the manual entry and display of Sensitive Security Parameters (SSP), such as passwords. These comments focused on password change operations, since other requirements apply to password entry for authentication.

Response: The standard does not mandate visual verification of SSPs during manual entry; rather, it permits the option that, when SSPs are long and possibly in hexadecimal representation, they may be temporarily displayed to allow visual verification for improved accuracy. This flexibility is retained in the Revised Draft FIPS 140–3. In addition, the concept of the Trusted Channels and its use for input/output of SSPs at Security Levels 3 and 4 is clarified in the Revised Draft FIPS 140–3.

Comment: Twenty-one comments were received regarding conflicts in the specifications pertaining to Random Bit Generator (RBG) entropy sources and difficulties in satisfying the RBG self-testing requirements during conditional self-tests.

Response: NIST considered all comments related to the Random Bit Generator (RBG) Entropy Source Test, and removed the RBG Entropy Source Test from the list of required conditional self-tests in the Revised Draft FIPS 140–3. For consistency, the Revised Draft FIPS 140–3 defines the minimum entropy as the min-entropy defined in NIST SP 800–90, ''Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)'', as amended, and points to it for additional requirements.

Comment: Thirty-one commenters stated that ambiguities in the Operating System Requirements for Modifiable Operational Environments needed to be clarified. Depending on how the various terms were interpreted these requirements might be impossible to satisfy.

Response: The entire section 4.5.1 ''Operating System Requirements for Modifiable Operational Environments'' has been re-written to improve clarity.

Comment: Three comments were received indicating that thorough review of the 2007 Draft required access to all annexes pertaining to the standard.

Response: All annexes (A through F) pertaining to the Revised Draft FIPS 140–3 have been made available for concurrent review with the Revised Draft FIPS.

Comment: One comment was received recommending a key status indicator to show whether the module is keyed, not keyed, or zeroized.

Response: The Revised Draft FIPS requires a physical or logical status indicator, but only for self-tests and error states.

Comment: Two comments were received noting that zeroization for physical security reasons must occur in a sufficiently small time period to prevent the recovery of sensitive data, but no such constraints were indicated in the 2007 Draft.

Response: NIST updated the Revised Draft FIPS to specify that zeroization shall be immediate and non-interruptible and shall occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroization is initiated and the actual zeroization completed.

Comment: Two comments were received stating that operating system requirements disallowed most debuggers and suggested an exception for maintenance mode.

Response: NIST restored the maintenance role and allowed debuggers when operating in maintenance mode. The operating system shall prevent all operators and running processes from modifying running cryptographic processes (*i.e.,* loaded and executing cryptographic program images) only when not in the maintenance mode. In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (*i.e.,* operator-initiated).

Comment: The 2007 Draft defined the cryptographic module's electrical power as a physical port. Two comments were received regarding the requirements applicable to the power port in order to restrict unintended information flow.

Response: NIST defined a ''power interface'' for the cryptographic module and replaced all references to ''power port'' with ''power interface'' in the Revised Draft FIPS. No additional requirements related to power interfaces were added. Clarifications triggered by questions related to this topic will be addressed in standard's supplementary documentation such as the ''FIPS 140–3 Implementation Guidance''.

Comment: Six comments were received regarding the specified false acceptance rate (FAR) of 1 in 10∧8 for authentication mechanisms in the 2007 Draft, and noted that the 2007 Draft was silent with respect to false rejection rate (FRR). Some comments suggested that the engineering tradeoffs required to achieve an FAR of 10∧8 will have a strongly negative impact on usability.

Response: NIST reviewed the requirements for group authentication mechanism and acknowledges the impact of such requirement on usability and on the FRR of cryptographic modules using multi-factor authentication mechanisms. The requirement was removed from the Revised Draft FIPS and will be addressed in the Implementation Guidance or other supplemental documentation.

Comment: Eleven comments were received regarding the self-testing requirements specified by the 2007 Draft. The commenters considered the requirements inappropriate for devices with aggressive power conservation modes, such as newer portable devices and embedded devices.

Response: NIST reviewed the self-test section and redefined the cases when the pre-operational self-tests must be performed.

Comment: One comment was received highlighting a conflict between self-tests for random bit generators (RBGs) and NIST Special Publication (SP) 800–90.

Response: NIST reviewed the self-test section and removed the conflicting requirement from the continuous RBG test section of the draft.

In addition to the public comment period, NIST hosted a public workshop on March 18, 2008 to obtain additional feedback on requirements for software crypto modules. The FIPS 140–3 Software Security Workshop addressed a range of topics, including the following: single user mode at Security Level 1; the logical boundary of a software module; the modifiable operational environment; audit logs; software integrity tests; ''firmware'' modules; security strength of a crypto module; and the number of security levels for software modules. Based on the combination of public comments and the discussions at the FIPS 140–3 Software Security Workshop, NIST implemented further changes to rationalize and simplify the security levels in the Revised Draft FIPS 140–3. In particular, the Revised Draft FIPS 140–3 specifies four security levels instead of five, reintroduces the notion of firmware cryptographic module and

defines the security requirements for it, limits the overall security level for software cryptographic modules of Security Level 2, and removes the formal model requirement.

The following significant substantive differences between this Revised Draft FIPS 140–3 and the current FIPS 140–2 standard are noted: Inclusion of a separate section for software security; limiting the overall security level for software cryptographic modules of Security Level 2; requirement for modules to mitigate against the non-invasive attacks when validating at higher security levels; introduction of the concept of public security parameters; allowing modules to defer various self-tests until specified conditions are met; removing the formal model requirement; and strengthening the requirements for integrity testing.

The Revised Draft FIPS 140–3 can be found at *http://csrc.nist.gov/publications/PubsDraft.html,* and is available for public review and comment.

Prior to the submission of this proposed revised standard 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.

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 be significant for the purpose of E.O. 12866.

Dated: December 7, 2009.

Patrick Gallagher,

Director.

[FR Doc. E9–29567 Filed 12–10–09; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

International Trade Administration

Mission Statement; Solar Energy Trade Mission to India, February 15–19, 2010

AGENCY: Department of Commerce.

ACTION: Amendment.

Mission Description

The United States Department of Commerce, International Trade Administration, U.S. and Foreign Commercial Service (CS), is organizing the second Solar Energy Trade Mission to India from February 15 to 19, 2010. Led by a senior Department of Commerce official, the mission will continue to build on the Department's efforts to open the burgeoning Indian solar market to U.S. firms and to position U.S. companies to seize export opportunities as India gears up to rapidly expand its solar energy capabilities. Ideal trade mission participants will be representatives of leading U.S. manufacturers of solar technology, including utility-scale technologies such as photovoltaic and concentrated solar power, and manufacturers of products such as solar street lighting, solar home lighting, and solar water pumping systems. The mission will also be open to a limited number of representatives of trade associations, councils and groups in the solar energy sector. The mission will visit three cities: New Delhi, Bangalore, and Mumbai, where participants will receive market briefings and meet with key government decision makers and prospective private sector partners during customized, one-on-one meetings.

Commercial Setting

India is facing a critical shortage of energy. Due to its sustained economic growth, the country suffers from an energy deficit, which stands to worsen as India's economy and population continue to grow. As a result of the energy shortage, Indian consumers face frequent periods of power outages, and prices for electricity are high. In addition to the need for more capacity, the Indian government at both state and national levels has begun to recognize the threat posed by global climate change. As such, the Government of India (GOI) acknowledges that some of the country's energy needs must be met with cleaner sources of power. All of these issues have compelled the GOI to move forward with an action plan to address its energy needs.

In 2008, the GOI released its National Action Plan on Climate Change (NAPCC), part of which addressed energy needs and particularly focused on solar energy as an area of development. Concurrent with the development of the NAPCC, three Indian states—Rajasthan, Gujarat, and Karnataka—have progressively launched their own efforts to develop solar projects. Since the NAPCC was initially released, CS India has aggressively worked to facilitate the development of the nascent Indian solar market, focusing on the aforementioned states. In March 2009 the first U.S. Solar Energy Trade Mission to India took place, which brought 14 U.S. companies to India, along with Deputy Assistant Secretarial leadership from the Departments of Commerce and Energy, and a board member from the U.S. Export-Import Bank. The mission successfully introduced U.S. solar energy technology to relevant Indian officials, and, as a result of the mission, U.S. firms have signed memoranda of understanding to develop 5MW solar projects in Rajasthan. Prior to this trade mission Indian officials acknowledged that they were not familiar with U.S. solar technologies, and that they believed European firms had more proven products. The trade mission helped to highlight the strength and cost effectiveness of U.S. technologies—a crucial step for positioning U.S. firms in this market.

As a follow-up to the first trade mission, in July 2009 CS India organized a solar finance roundtable in Mumbai, which brought together key government decision makers from Rajasthan, project finance bankers, and two U.S. energy developers. Lack of project finance options had emerged as a stumbling block to the development of utility-scale solar power projects in Rajasthan. Roundtable participants addressed critical issues such as power purchase agreements, renewable energy purchase obligations, transmission line issues and tariff structures, and the Rajasthan government officials confirmed that they would put the policy mechanisms in place to make the solar projects financially viable.

Building on the positive momentum to date, CS India approached the U.S. Trade and Development Agency to fund an orientation visit to the U.S. by officials from Rajasthan. The visit, which will take place during October 2009, will coincide with Solar Power International, the largest solar industry trade show in the United States. By attending this show the Indian officials will be exposed to the variety and depth of U.S. solar technologies, and they will visit demonstration sites to see firsthand the integration of solar energy into the U.S. power grid.

The second Solar Trade Mission to India will continue to build on the above efforts and will help keep U.S. firms at the forefront of this emerging market. In particular, the mission will continue CS India's extensive efforts to positively influence policy and will allow U.S. manufacturers to weigh in with Indian officials as crucial government decisions are soon to be made that will impact the direction this market will take.