# Comments Received on NIST's Request for Information regarding *"Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs"*

*Federal Register Notice 2015-19743 (8/12/2015)*
*Comment Period Closed: 9/28/2015*

## Schaffer, Kim B (Fed)

**From:** Scholl, Matthew (Fed)
**Sent:** Thursday, July 19, 2018 4:07 PM
**To:** Schaffer, Kim B (Fed)
**Subject:** FW: Comments on ISO 19790
**Attachments:** Comments on the use of ISO.docx

**Importance:** High

---

**From:** Dawn Adams <dadams@ewa-canada.com>
**Organization:** EWA-Canada
**Date:** Monday, September 28, 2015 at 7:03 PM
**To:** UseOfISO <useofiso@nist.gov>
**Cc:** 'Erin Connor' <econnor@ewa-canada.com>
**Subject:** Comments on ISO 19790

Comments from EWA-Canada, An accredited FIPS test lab.

Regards,
Dawn

Dawn Adams
PA and CST Lab Manager
EWA-Canada
1223 Michael Street, Suite 200
Ottawa , Ontario
Canada, K1J 7T2

Email: dadams@ewa-canada.com
Phone: 613-230-6067 extension 1249
www.ewa-canada.com

**Comments on the use of ISO / IEC 19790**

(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?

No – but they have been discussing whether the federal market is sufficient for the FIPS endeavors since it takes so long to complete a validation that the product is not always marketable in a timely fashion.

(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?

There has been interest in an ISO evaluation.

(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?

It is comparable but has a different philosophy. It better accommodates a global market and is not US – centric.

(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?

The globalization of the ISO standard is a definite asset, however much will depend on the after effects of the adoption. If the vendors believe this is an international standard but the CMVP programmatically changes it to suit the US federal government, the global appeal of the standard is negated. Vendors are concerned that there will be the ISO standard and the NIST version of the ISO standard which would not be acceptable or useful.

(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?

Yes – they are as specific as the FIPS standard.

(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?

No – we already have the standard and are accredited to test to this standard by our national accreditation body.

(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?

The FIPS standard as it currently exists is not considered to be a first principles document. Implementation Guidances (IGs) have been used to transform the standard without going through the FIPS review process. This has made the program somewhat difficult in that it can be changed by a NIST Special PUB (SP) or an IG and the vendor has little or no say in these decisions. The SPs and IGs change often so the "standard" is a moving target. This is very difficult for vendors and labs. It makes the program unpalatable.

There are two main issues in adopting the ISO 19790 standard to replace FIPS 140-2:

1) What happens to all of the IGs? Many are outdated and contradictory.
2) How global will the NIST ISO standard be? Will there be any kind of mutual recognition between the CMVP and other bodies that already use the ISO standard to test cryptographic modules?

Customer's comments:

I see following benefits of using ISO/IEC 19790:2014 in part or as whole for FIPS 140-2 cryptographic algorithm and cryptographic module testing, conformance, and validation activities:

- This would help developer implement consented international requirements for wider market addressability.
- This would help position certified products in non-USA countries.
- This may help consolidate number of security certifications required by customers (low probability?).

Most Customers want to know how the program will change the ISO standard, to what degree, how it will interfere with their development and sales and would it be worthwhile doing two validations of the same product. They are also very concerned about the application of IGs to the ISO standard. There is concern that the ISO standard will become unrecognizable and that the validations done elsewhere will not be recognized.

Since ISO 19790 references ISO standards for evaluation techniques and for algorithms, how important and to what effect will the NIST SPs and IGs be used?

We are already accredited by a recognized accreditation body to conduct ISO 19790 testing. How will we be impacted if NIST adopts this standard as a FIPS replacement standard? Will the CMVP be able to change the standard without using the ISO process? This is what seems to be indicated. No one really cares if a national body has specific requirements. The standard has to stay intact though and must be allowed to be the first principles document currently missing in the CMVP.

**Subject:** RSA Feedback
**Date:** Monday, September 28, 2015 at 6:19:06 PM Eastern Daylight Time
**From:** Wieland, John
**To:** UseOfISO@nist.gov

Dear Sir/Madam,

RSA has the following comments regarding the use of the ISO 19790:2012 standard for FIPS 140 validation:

---

1. Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?
   [RSA] - RSA is not aware of any customers asking for the ISO standard, but we routinely get asked about FIPS-140-2 validation. This is the main market for our product.
2. Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?
   [RSA] - More customers ask more application specific questions and need more clarity on the usage of the FIPS-140-2 standard.
3. Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?
   [RSA] - Technically the requirements for ISO 19790 and FIPS 140-2 are similar so the risk that a module developed from the standard is not secure is the same for both documents. Also the risk that a document doesn't adequately describe how to develop a module is the same for both documents. Both documents need detailed information from an implementation guidance.
4. Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?
   [RSA] - Technically the requirements are similar. The risk that a module developed to meet the ISO standard not being secure is not modified by the document. The risk of failing to develop a module that is what is required by the standard is still determined by the use of the Implementation Guidance.
5. Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?
   [RSA] - The requirements in ISO 19790:2012 still require the application of additional implementation guidance.
6. Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?
   [RSA] – No.
7. Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic

modules?
[RSA] – No.

RSA would prefer that the entire document be used and the national certification authorities apply profiles to the standard that define their requirements for security parameters

RSA continues to have an issue with the use of the implementation guidance to substantially modify the requirements of the standard. The implementation guidance should not include a mixture of guidance and requirements. A process should be put in place to allow for modifications to the standard while still maintaining the separate implementation guidance. Modifications to the requirements should also be managed using a transition process.

---

Regards,
John Wieland

**John Wieland**
Senior Software Engineer
RSA, The Security Division of EMC
PH: +61 7 3032 5238 | FAX: +61 7 3032 5299 | Email: john.wieland@rsa.com
Level 11 Central Plaza 1, 345 Queen Street, Brisbane QLD 4001 | www.rsa.com

September 28, 2015

Via e-mail to UseOfISO@nist.gov

National Institute of Standards and Technology,
Information Technology Laboratory,
ATTN Use of ISO/IEC 19790,
100 Bureau Drive, Mail Stop 7730
Gaithersburg, MD 208

**Re: Intel comments in response to NIST's Solicitation for Comments on 'Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs'**

Intel Corporation appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) Solicitation for comments on the *Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs.* We are submitting a few general comments below.

***(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?***

There is industry consensus that international standards are preferred over national versions, since the development and maintenance process provides options for international collaboration and greater transparency of the standardization process worldwide.

While FIPS 140-2 is not consistently used outside of the US, with a few exceptions, there is somewhat greater support for the ISO/IEC 19790 in various contexts. Some test labs were reported to certify to ISO/IEC 19790, e.g., Japan, Korea, and Spain.

Our vision is for internationally standardized cryptographic algorithms that are accepted globally, and one certification process that is accepted everywhere. Harmonization with other cryptographic verification schemes, notably Common Criteria, would enhance the value and increase the usability of ISO/IEC 19790.

In reality, national preferences for cryptographic algorithms and a national security evaluation process are not always aligned with this vision.

Significant work is necessary to increase trust in NIST algorithms and certification approaches and to improve global adoption of the security evaluation practices based on internationally standardized NIST approaches. A movement to ISO/IEC 19790:2014, with effective, well defined, and painless transition, would be a step in the right direction.

***(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?***

The differences between FIPS 140-2 and ISO/IEC 19790 are numerous, but not pervasive. These differences have been documented in multiple sources, by test labs and others (see, e.g., in http://atsec-information-security.blogspot.com/2012/10/isos-cryptographic-module-work.html). Such differences as support for degraded mode in ISO/IEC 19790 or new requirements for developer testing of cryptographic modules have been highlighted as important. For example, ISO/IEC 19790 provides much clearer information on the correct response to self-tests in degraded model while tests in FIPS 140-2 are specified but the response to a test failure is not adequately specified.

In order to provide a well-documented response to question (3), comprehensive analysis and comparison of the two documents and references within them is required, but such analysis is out of scope for the format of these comments.

***(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?***

Multinational corporations have a duty to their shareholders to effectively and efficiently serve all of its customers across the globe. Creating globally recognized standards around critical aspects of technological advancements means consistent and interoperable solutions can be developed and deployed worldwide. The US has historically been recognized as the leader in developing useful and technically sound standards focused on the global good. Recent events have caused that assumption to be re-evaluated by world governments and, to a lesser extent, by the international standards bodies. Product producers are now being faced with the need to implement potentially multiple ways to accomplish the same tasks due to national distrust of another nation's standards. Nationally based standards can cause fragmentation, increased weaknesses, reduced market access and increased costs to both consumers and producers. It is essential to ensure that producers are not required to develop and deploy incompatible solutions in the global ecosystem as it will be a source of constant weakness. Therefore, Intel encourages the use of ISO/IEC 19790:2014, but with a well-defined transition process.

If the ISO/IEC 19790:2014 is used exclusively, changes will be needed to the testing and validation process that will impact current and future certification holders. NIST needs to define and document the activities associated with the transition from NIST FIPS 140-2 to ISO/IEC 19790:2014. It will be necessary for NIST to develop a public transition plan to affect the move to ISO/IEC 19790:2014, and for the test labs to provide practical guidance.

***(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?***

The requirements in ISO/IEC 19790:2014 are sufficiently clear. However, both frameworks make an assumption that these requirements will be used to create a Hardware Security Module or a similar device. This approach is at variance with the nature of most modules that are created today (see also our answer to 7).

***(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?***

No. Intel recognizes there is a cost to development of standards. When standards are referenced in regulation, we support an approach that would make referenced standards available for no-cost review. An example of this approach is the ANSI Incorporation By Reference Portal (see http://ibr.ansi.org/).

***(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?***

Our answer to this question explores the focus of the current framework rather than specific gaps. Identification of major gaps follows from the general discussion presented here.

The discreet device HSM (Hardware Security Module) model that both ISO/IEC 19790:2014 and FIPS 140-2 are using is insufficient to represent the modules that are commonly built today.

A module certification to either standard doesn't provide value along the chain of device integration and doesn't enable certification of integrated modules down the line. Module certification needs to be repeated at each new module boundary, including the modules within, while system integrators may not have access to the modules necessary to achieve that certification.

One requirement that is especially at variance with the competing environment today is the role based requirement for user intervention. On chip hardware security devices often operate without user intervention performing essential security functions such as generating random numbers, performing key management, signing and attesting to provide services to other parts of a chip. The role based requirements in the two certification frameworks are written very much in terms of organizations where the roles are assigned to humans.

Many small or embedded devices also operate without a user interface. Credentials and identities are provisioned at manufacturing time. Both FIPS 140-2 and ISO 19790:2014 fail to accommodate such devices by requiring interfaces with role based authentication that do not exist on such devices.

Since the technology direction towards the growing numbers and diversity of form factors is clear, the assumptions built into ISO/IEC 19790:2014 and FIPS 140-2 will become increasingly less relevant.

**Subject:** Comment regarding the ISO 19790:2012 document
**Date:** Monday, September 28, 2015 at 4:43:50 PM Eastern Daylight Time
**From:** Kelvin Desplanque (kdesplan)
**To:** UseOfISO
**Priority:** High
**Attachments:** image001.png

ISO/IEC 19790:2012(E) – Section 7.5 - Software/Firmware security – Security Level 2 – 1st Bullet – Numbered Page 30 – "The software and firmware components of a cryptographic module shall [05.13] only include code that is in executable form (e.g. **no** source code, object code or **just-in-time compiled code**);"

Does this imply that no Java byte code can be included inside the Cryptographic boundary of a SL2 Module? I am confused since in Section 7.6.1 – Operation environment general requirements – In the 1st paragraph is says, '*The operating system is considered to include, when applicable, the virtual machine(s) (system and/or process) and the runtime environment (e.g. Java Runtime Environment – JRE).*' Why allow a JRE to part of the OE but potentially exclude Java bytecode? After all Java bytecode is considered to be JIT (Just-In-Time) compiled code.

Regards,
Kelvin

**Kelvin Desplanque**
ENGINEER TECHNICAL MARKETING
Government Certification CoGS - Canada
kdesplan@cisco.com
Phone: **+1 613 788 7216**
Mobile: **+1 613 355 7352**

**Subject:** With Reference to "Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs"

**Date:** Tuesday, September 1, 2015 at 6:33:03 AM Eastern Daylight Time

**From:** Kelvin Desplanque (kdesplan)

**To:** UseOfISO

**CC:** Honeycutt, Diane

**Attachments:** image001.png

With reference to "*Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs*" on URL https://www.federalregister.gov/articles/2015/08/12/2015-19743/government-use-of-standards-for-security-and-conformance-requirements-for-cryptographic-algorithm in the Federal Register, in both the ***ADDRESSES*** and ***SUPPLEMENTARY INFORMATION*** sections, reference is made to "**ISO/IEC 19790:2014**". Should this not be "**ISO/IEC 19790:2012**" ? Or perhaps you meant to make reference to "**ISO/IEC 24759:2014**" since the link on the aforementioned page, http://www.iso.org/iso/catalogue_detail.htm?csnumber=59142, is pointing there. So far as I know, ISO has not published a "**ISO/IEC 19790:2014**" document (see http://www.iso.org/iso/home/search.htm?qt=19790&sort=rel&type=simple&published=on) .

Could you clear up any misunderstandings that I might be having?

Regards,
Kelvin

CISCO

**Kelvin Desplanque**
ENGINEER TECHNICAL MARKETING
Government Certification CoGS - Canada
kdesplan@cisco.com
Phone: **+1 613 788 7216**
Mobile: **+1 613 355 7352**

# InfoGard Comments on Use of ISO 19790

InfoGard Laboratories, Inc. (InfoGard) supports the use of the ISO/IEC standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by Federal Information Processing Standard (FIPS) 140-2. The use of all or part of the ISO/IEC standards for testing, conformance and validation of cryptographic algorithms and modules is in the best interest of the program at this point in time. It's vital that an updated standard is put in place. Since the ISO 19790 requirements are 3 years old, InfoGard recommends another public comment period to allow the community to comment on any requirements that might need modification.

In response to the specific feedback requested:

(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?
As a testing and conformance organization, obviously FIPS 140-2 validations are a common request. We have customers who are extremely interested in pursuing an ISO 19790 validation, but only if it becomes the next FIPS 140 standard. If not, we do not anticipate that our customers would seek ISO 19790 validations. As of today, there are a few customers who have had training on the ISO 19790 requirements, but no validations have been pursued.

(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?
Our customers want to be proactive in preparing for the new requirements so they are interested in testing to the ISO 19790 standard only if it is still slated to be the next FIPS 140. There have been no changes in terms of what the markets we serve are asking for. Our customers want to ensure that they can continue to sell their products to the US federal government.

(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?
ISO 19790 specifies tests that provide equal evidence of conformance in all areas of FIPS 140-2. The specificity of the requirements, the general language in which the ISO requirements are written, and the evidence of conformance equal that of FIPS 140-2.

(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?
Generally, no.

(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?
N/A – InfoGard does not develop cryptographic modules.

(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?
No.

(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?

The majority of potential gaps are currently addressed in the FIPS 140-2 Implementation Guidance (IG). It is not clear which, if any, of the IGs would be carried forward or reassessed. If the IGs will not be applicable to ISO 19790, several gaps addressed there will exist in the new standard.

Also, several outdated requirements are included in the ISO standard that need to be reassessed; for example, physical security requirements related to single-chip modules.

gemalto

28 September 2015

**Response to the Request for Information 2015-19743 Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs**

Gemalto wishes to express our overall support for the adoption of ISO/IEC 19790:2012 as an open, international community-developed standard. Itis hoped that ISO/IEC 19790:2012 will provide the cryptographic module community with a complete, clear, and transparent conformance standard that will continue to evolve with time and need.

*NIST is also interested in comments on the possible uses of ISO/IEC 19790:2014 that range from use of only selected sections, continuing with a FIPS requirement that cites a baseline version of the ISO/IEC 19790:2014, and/or full use of the ISO/IEC standard.*

> While there is significant overlap in the requirements of FIPS 140-2 and ISO/IEC 19790:2012, there are also a number of area where ISO/IEC 19790:2012 introduces new or modified requirements from those that have been in place for many years. Notwithstanding any of the options for use of ISO/IEC 19790:2012 above, an extended transition period which includes a period in which both standards co-exist would provide labs, vendors, and customers with the necessary time to adapt and would reduce the impact on the market.
>
> Before any transition to the use of ISO/IEC 19790:2012 in whole or in part; it is hoped that areas where simultaneous conformance to ISO/IEC 19790:2012 and FIPS 140-2 is difficult to achieve have been fully rationalized and open to public comment as part of the transition. We therefore recommend that NIST create an industry engagement group/forum to work through challenges in the transition and to ensure that future develops of the ISO standard stay as closely aligned with NIST views as possible to avoid a future branch in the two standards.

The following are general.responses to the NIST questions:

*(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?*

> Many customers demand FIPS 140-2 validations in cryptographic products and are monitoring progress of ISO/IEC 19790:2012adaption with interest at this time only. An immediate concern is how a transition to the standard will impact the timeliness of products with validated cryptographic modules to market and if additional delays will be introduced as a result.

*2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?*

> Changes in what the market is asking for tend to be more closely aligned with changes in the cryptographic algorithm standards approved for use rather than in the underlying module conformance standard. This is especially true when the market perceives newer standards to have reduced the cryptographic strength of an algorithm as has happened with the removal of nlen=4096 from the RSA algorithm.

gemalto

*(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?*

We believe that ISO/IEC 19790:2014 provides improved testing to demonstrate conformance as it is not as dependent on the IG from the scheme, leading to a more cohesive and readable document which can be referenced to developers.

*(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?*

ISO/IEC 19790:2012 has a significant overlap with the requirements of FIPS 140-2 so the risk is comparable. Life-cycle assurance is a new area of risk management for a cryptographic module conformance standard.

*(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?*

Yes, the requirements in ISO/IEC 19790:2012 are specific enough to develop a cryptographic module that can demonstrate conformance to this standard.

*(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?*

The citation of an ISO standard that has a fee for access would not inhibit our use of this standard nor do we anticipate is to be a significant issue for many of our customers. In general, however, free access to the standard would allow for greater public transparency into the program and its requirements. If there will be requirements that are not mirrored in a FIPS standard but cited only in ISO/IEC 19790:2012, it is requested that consideration is given for adding ISO/IEC 19790:2012 to the ISO list of Freely Available Standards: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

*(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?*

There are no gaps that we currently see, but the additional restriction in the Integrity test requirement presents a challenge to us, especially in our products that require very fast time to ready customer requirements. We feel that the requirement for software and firmware components of a hardware module should be similar to FIPS 140-2, where a 16-bit EDC is allowed.

September 28, 2015

Motorola Solutions Inc. (MSI) comments on the potential replacement of FIPS 140-2 with ISO/IEC 19790:2012.

Follow are responses from MSI to the RFI posted by NIST at: https://www.federalregister.gov/articles/2015/08/12/2015-19743/government-use-of-standards-for-security-and-conformance-requirements-for-cryptographic-algorithm

1. *Have your customers or users asked for either ISO/IEC 19790:2012 or FIPS 140-2 validations in cryptographic products?*

   Yes, some of our customers have asked for and require FIPS 140-2 validations on our products.

2. *Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?*

   Yes, some of our markets have asked for and require FIPS 140-2 validations on our products.
   We are seeing an increase in the number of customers, both domestically and internationally, inquiring about FIPS 140-2 validation in our products.

3. *Do you think the ISO/IEC 19790:2012 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?*

   Requires further study.

4. *Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?*

   We believe there may be a risk in vendor selection due to the cost requirement on the ISO standard.

   This cost requirement also puts a burden on the customer to have access to the standards so they may be able to understand what the products they purchased really support. Today there is no such barrier since FIPS 140-2 is freely available.

5. *Are the requirements in ISO/IEC 19790:2012 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?*

   As with FIPS 140-2, MSI believes that a supporting Implementation Guidance document would be greatly beneficial.

6. *Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?*

   While MSI would prefer a fee free standard, no, this would not inhibit MSI. We do feel that it may inhibit other vendors and customers.

7. *Do either FIPS 140-2 or ISO/IEC 19790:2012 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?*

   Requires further study.

8. *Miscellaneous*

   Can you give examples of vendors who have certified to these ISO documents? Both domestically and internationally.

**Subject:** Comments on ISO 19790
**Date:** Monday, September 28, 2015 at 1:07:07 PM Eastern Daylight Time
**From:** Deboyser, Fabien
**To:** UseOfISO
**CC:** Dieguez, Ignacio, Burns, Robert

Dear NIST,

In response to your RFI regarding the usage of the potential use of ISO 19790 standards.

Please find our answer to your questions.

*1- Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?*
*2- Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?*

Our market is FIPS 140-2 oriented. We didn't so far received from our users or customers any specific request for merging towards the ISO standard.
Even though we see the great interest of adopting a new standard, we would like the adoption being smooth enough and adopting a smooth transaction.
We are also concerned on having internationally recognized standards for assessing our security, which both of them provide.

*3- Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?*
*5- Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?*

We consider that the ISO standard provides less precise requirements for tests and evidence of conformance than the FIPS 140-2.
There is no implementation guidance defined for the ISO standard.
Annexes E and F are not completed and are very important.
The description of the low-level testing is not precise enough and could lead to different interpretation.
The notion that the module shall be designed to allow testing of all provided security related services is not precised. Do we have to consider the internal mechanism?

*4- Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?*

The ISO standard contains much concepts than the FIPS 140-2. It represents for us an update on the security which is very important.
We strongly believe that our product will benefits from this update.
Except from the risks that using an ISO standard would allow countries to participate in the standard, or emit certificates.
We think that the risks would be easily mitigated by a FIPS 140-3 NIST validation.

*6- Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?*

Our usage of the ISO standard won't be inhibited by the price, as we already buy many ISO standards for the compliance of our products.
But, we think that for an international certification, which aimed to be public, a buyable standard is not deserving our interest of transparency.
We believe that the end-customer has the right to know the certification process, and that brings confidence.
We therefore suggest to use the ISO standard as the Common Criteria standard.

*7- Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?*

So far to our analysis, we didn't find any gap area.
We think that a trial use could be of interest such as to identify any potential gap area or black area.
Actually, a standard reveals his real nature by usage.

*Additional comments*

As part as our additional comments, we have identified some questions.

- How will be managed any update of the document? The NIST will take over the update? Or we will align with the regular updates from the ISO?
- The FIPS logo for certification will still be maintained? (there is a very big identification of that)
- How would be defined the certification scheme?

Regards,
Thales e-Security

**Subject:** NIST RFI on use of ISO/IEC 19790:2012
**Date:** Sunday, September 27, 2015 at 7:43:11 AM Eastern Daylight Time
**From:** Thomas, Ryan
**To:** UseOfISO
**CC:** Boire, Marc, Thomas, Ryan
**Attachments:** image001.jpg

Hello,

Thank-you for the opportunity to provide feedback and comments on the proposed transition to an ISO/IEC 19790:2012-based version of FIPS 140. The CGI ITSETF is an NVLAP accredited Cryptographic Security Testing Laboratory (CSTL) responsible for performing FIPS 140-2 validations on cryptographic modules. Please find our feedback on the NIST proposal in addition to comments and questions below:

**CGI ITSETF COMMENT #1 - Paragraph 80 FR 48295**: *"NIST is also interested in comments on the possible uses of ISO/IEC 19790:2014 that range from use of only selected sections, continuing with a FIPS requirement that cites a baseline version of the ISO/IEC 19790:2014, and/or full use of the ISO/IEC standard."*

We welcome the switch to an ISO-based FIPS 140 standard as it is an internationally reviewed and accepted publication. As NIST is likely aware, ISO/IEC JTC 1 sub-committee 27 was responsible for the development of both 19790:2006 and 19790:2012. Editors and experts from the US, France and Japan led an international group contributed to its development. Japan (IPA) and South Korea (KCMVP) both already use ISO/IEC 19790 as a basis for their cryptographic module validation programs. In the interest of mutual recognition, alignment with other international security standards and testing programs such as Common Criteria, the CGI ITSETF would like to express a strong desire for the next version of FIPS 140 to remain as close as possible to the current version of ISO 19790:2012.

While we respect that NIST will be selecting Approved Algorithms for use, developing the Annexes, IGs and testing tools for labs we respectfully request that NIST publicly identify areas they feel it necessary to deviate from the requirements of ISO/IEC 19790:2012 or ISO /IEC 24759 and issue a formal public comment period for the changes. A rationale for the deviation and the proposed change/update to the requirement should also be provided for review. This review would be in alignment with the principles outlined in the recent "Report and Recommendations of the Visiting Committee on Advanced Technology (VCAT) of the NIST" from July 2014.

One of the main concerns our vendors have is the various testing/certification requirements for different schemes around the world. In some cases this results in a lot of redundancy – in other cases it can result in a separate code bases to address one schemes requirements vs. another's. Where possible and where it makes sense it would be appreciated if cryptographic module security requirements could be tested under a mutually accepted and recognized standard such as the ISO. We recognize that schemes/agencies outside of Canada and United States will have different Annexes and the validation procedures might differ - but overall the module requirements would adhere to the same standard. This harmonization would hopefully encourage a recognition of the CMVP as the defacto validation program in the world.

**CGI ITSETF COMMENT #2 - Paragraph 80 FR 48295:** *" NIST is also interested in feedback on the impacts of a potential U.S. Government requirement for use and conformance using a standard with a fee-based model where organizations must purchase copies of the ISO/IEC 19790:2014 "*

The fee based model is not ideal and it may limit the initial distribution of the standard amongst security

vendors and the community at large. However, we believe that this cost is not prohibitive and nearly all vendors we spoke with would be willing to absorb the fee as a "cost of doing business" provided it is a one-time cost.

***(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?***

Yes. CGI ITSETF is an accredited CST laboratory, as such, our primary business is to perform FIPS 140-2 validations. There is a strong interest in both FIPS 140-2 and ISO 19790-based validations of cryptographic products. There is also a strong desire in industry for a testing program that demonstrates conformance to an international standard which is mutually accepted by different certification schemes and programs. We hope that the ISO-based version of FIPS can achieve this objective.

***(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?***

As a CST laboratory, many of the comments we receive from security product vendors or the industry (as the markets we serve) are requesting an updated version of FIPS 140-2. Many of the current FIPS 140-2 requirements do not add significant value to a product from a security perspective (in the case of the pre-operational self-tests - they may even hinder performance without any demonstrable increase in security). Technology has changed significantly since the standard was introduced - it is time to move to a new standard for cryptographic security requirements that can better account for these changes.

***(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?***

Overall, we believe the ISO-based requirements are better positioned to address today's technology. In ISO 19790 the requirements for pre-operational self-tests have been reduced to the module integrity test and critical function tests. While the algorithm tests would become conditional. We believe the current pre-operational algorithm tests in FIPS 140-2 serve no real value and actually and hinder product/module performance in some circumstances.

FIPS 140-2 is not always explicitly clear on the requirements for sensitive security parameters vs. public security parameters. This leads to misinterpretation and confusions from vendors. The ISO explicitly define the two and specify requirements for each.

FIPS 140-2 permits hardware/firmware modules to only perform a 16-bit EDC such as a CRC. We believe most hardware and firmware today should meet stronger integrity test requirements specified in ISO 19790.

Currently, FIPS 140-2 Annex B references a sunset version of a NIAP Common Criteria Operating System Protection Profile (OSPP). As of today's date a level 2 software validation is practically not possible as the platforms and OSes specified in the CC OSPP are almost 8 years old. This is a real sore spot for many software vendors. In ISO 19790, the dependency on Common Criteria for the Operating Environment (OSPP listed in FIPS 140-2 Annex B) for software modules aiming for a Validation Level 2 or higher is removed.

ISO 19790 introduces requirements for developer testing on the module to complement the lab's testing Software/firmware components in the cryptographic boundary must undergo automated security testing (such as static code analysis etc.). Developers of cryptographic modules also need to document the internal security testing practices. In our opinion this provides real-world tangibles security value and aligns with industry best practices for software development - something that is lacking in FIPS 140-2.

In addition to the points above, ISO 19790 no longer permits password complexity requirements to be enforced procedurally. All default passwords used to initially set up and initialize the module must be changed by the Cryptographic officer before use. These, in our opinion provide more robust security than FIPS 140-2.

***(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?***

We believe there are challenges with the current version of the standard (FIPS 140-2) due to its age which reduce its overall effectiveness and the "real world security" value a FIPS 140-2 certificate provides to federal users that are looking to procure validated crypto modules. The risk is the program is becoming less important to some vendors - as in their eyes some requirements are no longer relevant or provide very little in the way of security value. Requirements for module pre-operational cryptographic algorithm tests (such as known answer tests) are not really beneficial to modern software/hardware modules. Another example is a hardware must meet rigorous requirements for entropy but can implement a CRC-16 for a module integrity test. As a result many vendors are just trying do the minimum required to obtain a validation certificate.

The above integrity test example demonstrates how as the years have passed many new requirements have been introduced in the FIPS 104-2 Implementation Guidance (IG) document - while older and less relevant requirements still remain in the standard. We see a lot of vendors that design or develop their products to the requirements in the FIPS 140-2 Standard and the Derived Testing Requirements - thinking that these are the only important documents prior to engaging a lab. These vendors do not realize that that the IG document actually contains several standalone new requirements and the re-interpretation of others.

We believe this is a significant concern and problem with the program as a product developed to meet the FIPS 140-2 Standard and DTR (along with the Annexes) on their own (without the IG) will in our experience have significant gaps that will require product redesign/re-engineering. We strongly believe it is time to move forward to an updated set of requirements that better accommodates for modern technology types and the IG should be harmonized to provide clarification/interpretive assistance on new standard. The IG should not be used to implement new requirements which do not exist in the Standard or Derived Testing Requirements.

***(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?***

No, as it stands today, the Annexes (A-F) in ISO 19790:2012 still need to be addressed by NIST/CSE. We also believe a new/updated version of the Implementation Guidance will be required before vendors can develop cryptographic modules to ISO 19790:2012.

Before CST labs can test a product for conformance validation program guidance documents such as the Laboratory Managers Manual, FAQ and other associated policies/procedures will also need to be updated and distributed to CST laboratories.

***(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?***

No, we do not believe the fee for the standard will not be a problem provided it is clearly communicated and understood that this is a one-time purchase.

***(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?***

Please see Answer to Question 5 above. We believe the current gap for implementation is the development of Annexes, Implementation Guidance and validation program material. We request that NIST adhere to the public comments process for the development of the Implementation Guidance for the ISO-based version of FIPS.

**CGI ITSETF Questions:**

1. Does NIST currently plan to publish proposed changes/additions/deletions to ISO/IEC 19790:2012 for public comment period similar to this request? We would also request that NIST provide a rationale for their change and provide a change log of the delta.

2. Will NIST disclose their strategy for the FIPS 140-2 Implementation Guidance (IG) document as it relates to the new ISO-based version of the Standard? Will a list of proposed IGs for ISO 19790 from FIPS 140-2 or new IGs be open for public comment? The IGs selected could have a major impact on the interpretation of the new DTR (ISO 24759). Some examples are IG 9.10 (default point of entry) and IG 7.14/IG 7.15 (entropy requirements).

3. Will the FIPS 140-2 Implementation Guidance for the ISO/IEC 19790-based standard become a NIST Internal Report (NISTIR) document? Whereby any change or update would need to go through a public comment period?

Please don't hesitate to contact me if you would like to discuss any of the comments/feedback provided in this email. Thank-you once again for the opportunity to provide this feedback.

Regards
Ryan

**Ryan Thomas** CISA, CISSP
FIPS 140-2 Program Manager
CGI Global IT Security Labs - Canada
1410 Blair Place, 7th floor
Ottawa, ON K1J 9B9
T: 613-234-2155
C: 613-314-7579

CGI

# Microsoft's Response to NIST for Seven Questions about ISO/IEC 19790:2012 vs. FIPS 140-2

September 25, 2015
Compiled by Tim Myers, Security Program Manager, Microsoft Corporation

*NIST requests comments on the following questions regarding the use of ISO/IEC 19790:2012, but comments on other cryptographic test and conformance issues will also be considered.*

1. *Have your customers or users asked for either ISO/IEC 19790:2012 or FIPS 140-2 validations in cryptographic products?*

**Yes, Microsoft has US as well as international customers who have asked for FIPS 140-2 validations in cryptographic products. Microsoft also has non-US customers who have asked for cryptographic validation either as a crypto evaluation or as part of a larger evaluation such as ISO 15408.**

2. *Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?*

**Yes, the US Federal government market that Microsoft serves has asked for FIPS 140-2 validation. There has also been increased interest from international customers seeking independent evaluation of cryptography, security functionality, and cloud services. The latter two items include aspects of cryptographic validation. We received a requirement from a large international customer to use international standard algorithms and evaluation processes in addition to US standards.**

3. *Do you think the ISO/IEC 19790:2012 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?*

**At Microsoft, we think the ISO/IEC 19790:2012 standard appears to specify tests and provide evidence of conformance for cryptographic algorithms and modules equally compared to FIPS 140-2 in the following areas:**

1. **Cryptographic Module Specification**
2. **Cryptographic Module Interfaces**
3. **Roles, Services, and Authentication**
4. **Operational Environment**
5. **Mitigation of Other Attacks**

**The ISO/IEC standard appears to do better than FIPS 140-2 in the following areas:**

1. **Non-Invasive Security**
   **FIPS 140-2 does not cover this area.**
2. **Sensitive Security Parameter Management**
   **Procedural zeroization is not allowed for Security Level 2 and higher.**

3. **Self-Tests**
   **Crypto algorithm self-tests do not have to be run at power-up; they can be run conditionally, thereby improving performance.**
4. **Life-Cycle Assurance**
   **Finite State Model (FSM) requirements include more security states.**

4. *Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?*

**At Microsoft, we do not perceive a difference in technical security risks that would be mitigated or accepted in use of one standard versus the other. However, as a company with a global customer base, there is a current business risk. We have ongoing requests from customers for national crypto validation which adds cost and consumes engineering resources.**

5. *Are the requirements in ISO/IEC 19790:2012 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?*

**Yes, the requirements in ISO/IEC 19790:2012 appear to be specific enough for Microsoft to develop a cryptographic module that can demonstrate conformance to this standard.**

6. *Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?*

**No, the U.S. Government citation of an ISO standard that has a fee for access to the standard would not inhibit the use or implementation of this standard at Microsoft.**

7. *Do either FIPS 140-2 or ISO/IEC 19790:2012 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?*

**Currently, neither standard appears to have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules.**

**Other comments:**
**Microsoft has increased its cadence with more frequent product releases / updates. We would need timely guidance for using ISO/IEC 19790:2012 through the migration process. An improved process for the review and publication of Implementation Guidance as well as Test Requirements (e.g. ISO/IEC 24759:2014) would be valuable.**

*The responses to this request for information will be used to plan possible changes to the FIPS or in a decision to use all or part of ISO/IEC 19790:2012 for testing, conformance and validation of cryptographic algorithms and modules.*

**Subject:** Comments on ISO/IEC 19790:2012
**Date:** Friday, September 25, 2015 at 6:01:54 PM Eastern Daylight Time
**From:** Mark D. Baushke
**To:** UseOfISO

I am pleased to respond to the National Institute of Standards and Technology (NIST) request for public comments on using the ISO/IEC 19790:2012 standard as the U.S. Federal Standard for cryptographic modules http://csrc.nist.gov/groups/STM/cmvp/notices.html dated August 12, 2015 with comment period closure on September 28, 2015.

First, the need to go through a paywall and purchase this standard (19790:2012) is an extremely undesirable barrier to entry.

A large number of the cryptographic implementations that would need to be informed by this standard are Free and Open Source Software packages maintained by individuals who really have no strong incentives to pay for this standard in order to modify their software to comply with any changes mandated by it.

The ISO documents listed as approved security functions in Annex C are likewise behind a paywall and are an undesirable barrier to entry.

I will note that I would expect NIST to provide a replacement for Annex C. I expect this because even the first listed ISO standard in Annex C "18033-3:2010 - block ciphers" provides for many block ciphers (e.g., MISTY1, CAST-128, HIGHT, Camellia, SEED) which I would find unlikely to be added to the NIST approved security functions. I would also expect that FIPS PUB 202 for SHA-3 standards will also be added to the Annex C list.

While I suspect that NIST will be providing its own set of algorithms as a replacement to Annex C of the document, if they are also ISO documents, then those documents should be free of charge as well.

The definition 3.20 cryptographic algorithm as a 'well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces and output' seems poorly defined. By this definition, the sort algorithm and/or a tree-walk algorithm to find a particular cryptographic public/private key pair qualifies as a cryptographic algorithm. This definition is in need of refinement and suffers from the current problem of not being able to explicitly define the nature of a cryptographic algorithm other than by exhaustive enumeration. Given that an 'approved security function' is defined by reference in Annex C, this would leave a large number of 'cryptographic algorithms' in a 'cryptographic module' that are 'non-security relevant' ... which seems perverse.

The definition 3.21 cryptographic boundary of 'explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware,

software, and/or firmware components of a cryptographic module' does not easily allow for nested cryptographic boundaries such as a 'Trusted Platform Module' (TPM) which should be excluded from issues such as zeroization during a transition to an error state of the external cryptographic boundary that contains the TPM.

The definition 3.38 entropy of 'measure of the disorder, randomness or variability in a closed system' seems to be the thermodynamic definition. However, in any system that has a cryptographic module, the system is NOT closed, but is an open system. A closed system would be very secure in that it would not allow any incoming or outgoing control, status, or data, but would also be useless. I respectfully suggest that this is not an appropriate definition for use in a cryptographic module. Especially as documents such as NIST Special Publication 800-90A/B/C seem to wish for additional entropy to be introduced into the system which is not possible in a closed system.

Section 7, 'Table 1 -- Summary of security requirements' on the first row (Cryptographic Module Specification) contains this phrase:

> All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function or process in an approved manner.

Would seem to require the modification/instrumentation of software that utilizes an approved cryptographic algorithm. It is not clear to me how the status information should be stored or saved. Clearly, logging the information could lead to excessive amounts of logging material. See also sections '7.2.4.2 Normal operation' and '7.4.3 Services' ...

Section 7.5, has the following text:

> "* For a software or firmware module, if the loaded software or firmware image is a complete replacement or overlay of the validated module image, the software/firmware load test is not applicable (NA) as the replacement or overlay constitutes a new module.
>
> If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated module but is not a complete replacement or overlay of the validated module, then the software/firmware load test is applicable and shall [05.11] be performed by the validated module."

If I am able to do a replacement of an individual piece of the software, I should be able to replace each component in turn which effectively provides me with a complete replacement of the software/firmware. In this case, there appears to be no need to do a zeroization step even though the sum of the replacement elements would show as being a complete replacement. It seems as though there should be a way to provide a successor image which has been properly validated by the predecessor image without constituting a new module.

However, I suspect that this part of the standard is making an assumption or set of assumptions on an implementation rather than providing guiding principles to be followed which determine if a particular set of SSPs need to be zeroized or not.

Section A.2.3 'Cryptographic module interfaces' does not seem to specify any kind of optional 'status request' interface, just a 'status output' is specified. This would seems to mean that an operator command to show the status of the crypto module must glean such information from remembering previous 'status output' information. This seems to be inconsistent with the 'show status' mandate of section 7.4.3.1. I am not entirely in favor of the 'current status' as I suspect it could be used in a side channel attack, but I am also not sure I understand how to implement what is mandated in a cryptographic module when an operator requests the current status of a module which may be concurrently handling many different parallel simultaneous cryptographic primitive operations.

In the general case, in a high performance system, I would expect that hardware acceleration will be in place that will not be able to easily provide the 'current status' of any particular services, operations, or functions at a human time scale that is meaningful. Determining if a particular service is 'not currently in an error state' or it is 'currently in an error state' is easy. Anything else is non-trivial and will add a lot of complexity to the algorithms.

Section B.2.7 The text 'Specify the operator role responsible for securing and having control at all times of any unused seals, and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.' references a 'FIPS Approved state' which does not exist in the rest of the document. I suspect that 'operational state' of 'normal operation' was the one intended.

Annex D contains references to ISO/IEC standards behind a paywall. This is not desirable.

Annex E 'Approved authentication mechanisms' does not currently specify any approved mechanisms. This leads me to wonder how to properly implement section 7.4.4 Authentication if no methods are approved.

Best Regards,

Mark

Mark D. Baushke
Distinguished Engineer, Junos Security
Juniper Networks, Inc.

mdb@juniper.net
www.juniper.net
+1 408-745-2952


# atsec Feedback on Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs

**Last Updated:** 2015-09-22

## Overview

This document serves as atsec's response to the NIST request for information on the Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs (released on 08/12/2015) .

Note that the Federal Regiser website references ISO/IEC 19790:2014 but provides a link to ISO/IEC 24759:2014. NIST released a notice (dated 09/28/2015) stating that the correct ISO site was for ISO/IEC 19790:2012. Due to this, we will respond to the questions in regards to ISO/IEC 19790:2012. atsec's response to the request for information is outlined below.

## Response

(1) *Have your customers or users asked for either ISO/IEC 19790:2012 or FIPS 140-2 validations in cryptographic products?*

Our clients are interested in having their product validated under ISO/IEC 19790:2012 and would like to know if the ISO will be the successor to FIPS 140-2 and, if not, the standard that will be.

(2) *Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?*

The markets that we serve (banking, mobile, healthcare, and supercomputing) are all interested in getting validated under ISO/IEC 19790:2012.

(3) *Do you think the ISO/IEC 19790:2012 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?*

There are many benefits to ISO/IEC 19790:2012 in regards to test flexibility. Known answer tests and power-on self-tests are conditional. Self-tests would only have to be run for modes and algorithms that are being used. Cryptographic operations can begin while pre-operational tests are running as long as output cannot be provided until the tests have completed. The standard also allows for degraded modes of operation (if an algorithm stops working others may still be used).

(4) *Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?*

The risks associated with the FIPS 140-2 standard are that it is outdated and adds unnecessary complexity. The standard was established more than a decade ago and was based heavily on securing hardware cryptographic modules. This is not sufficient to meet the needs of the cryptographic modules today which are not only implemented as hardware but also as software, firmware, and hybrid modules. The Implementation Guidance (IG) document was developed to patch the standard and is now longer than the standard itself

(IG is 195 pages and FIPS 140-2 is ~70 pages). This poses a risk by adding increased complexity, making it harder for users to interpret the standards. Having all of the information in one well written document is necessary to reduce this risk. Another risk associated with the FIPS standard is that it doesn't have the necessary guidance to address new modules. This can prevent vendors from getting their certificate on time.

The main risk associated with the ISO standard will be the transition time necessary to move to the standard. The transition may be chaotic but it will improve over time and reduce risks in the long term.

(5) *Are the requirements in ISO/IEC 19790:2012 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?*

As a lab, atsec does not develop cryptographic modules; however, we believe the requirements of ISO/IEC 19790:2012 in conjunction with ISO/IEC 24759:2014 to be specific enough for organizations to develop a cryptographic module that is in conformance with the standard.

(6) *Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?*

Having a fee associated with the standard will make developing and testing cryptographic modules more expensive for vendors. If a fee must be associated with the standard it must be a reasonable one. The fee will have a direct impact on the accessibility of the standard within the community.

Many developers and testing laboratories are small companies. Licenses for several perople or even a site license would need to be considered and may be prohibitive when project teams have several personnel. This issue is likely to be less onerous for large companies that already have favorable mechanisms in place for licensing standards.

Currently the standard price from ANSI for the cryptograpohic module document set is $878 for single user licenses. It is likely to rise as more documents are added to the set of documents relevant to cryptographic module specification and testing.

- ISO/IEC 19790:2012 from ANSI is currently advertised at $240

The ISO/IEC supporting documents are also not free:

- IS 24759:2014 Test Requirements for Cryptographic Modules. $265.00
- IS 29128:2011 Verification of cryptographic protocols $200
- TR 30104: Physical Security Attacks, Mitigation Techniques and Security Requirements $173

And other documents, currently drafts, must be considered as potentially being needed by cryptographic module developers:

- IS 18367: Cryptographic algorithms and security mechanisms conformance testing. (draft)

- IS 17825: Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. (draft)

It would be beneficial if NIST could support industry by supporting a mechanism for reducing the overall price of the standard and associated documets to cryptographic module developers and laboratories.

(7) *Do either FIPS 140-2 or ISO/IEC 19790:2012 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?*

The primary gap area we see is that Level 2 software modules cannot be tested with the current FIPS standard due to the expired U.S. Government General Purpose Operating System Protection Profile (GPOSPP). ISO eliminates this gap by removing the dependency on Common Criteria (CC) for evaluation. In addition to this, ISO also provides more economical self-test guidance and allows for degraded modes of operation.

## Conclusion

atsec fully supports the transition from FIPS 140-2 to ISO/IEC 19790:2012 Security Requirements for Cryptographic Modules Standard as the U.S. Federal Standard for Cryptographic Modules. We believe that ISO/IEC 19790:2012 is better suited for the diversity of today's cryptographic modules and provides an increased level of adaptability and flexibility that will allow the standard to continue evolving.

**Subject:** Public comment on the potential use of certain ISO standards
**Date:** Tuesday, August 18, 2015 at 2:11:00 PM Eastern Daylight Time
**From:** Meagher, Kevin
**To:** UseOfISO

I am NOT in favor of using ISO standards in place of FIPS 140-2 or -3.

(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?
[kmeagher] FIPS 140-2 only

(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?
[kmeagher] More customers are asking for common criteria and FIPS 140-2

(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?
[kmeagher] Have not reviewed 19790:2014

(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?
[kmeagher] From a US DoD standpoint, it seems risky to leave cryptography in the hands of an international organization. ISO may not be able to move quickly to adjust to new threats. ISO may not be willing to remove compromised cryptography in an effort to maintain compatibility. ISO politicking may drive crypto in the wrong direction.

(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?
[kmeagher] Have not reviewed 19790:2014

(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?
[kmeagher] Yes, the high fee ISO charges for its documentation is a barrier. The fee for 19790:2014 is $182 as of today. Standardizing products among many vendors requires free and easy access to standards. Internet appliances are low cost, low margin and are the target of attacks. Ease of access to security standards is the only hope of securing such devices.

(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?
[kmeagher] Have not reviewed 19790:2014

**Kevin S. Meagher** | Technical Certification Project Manager
kmeagher@ciena.com | 7035 Ridge Road | Hanover, MD 21076 USA
Direct +1.410.865.8936 | Mobile +1.301.512.1742 | Fax +1.410.865.8547

**Subject:** cost
**Date:** Monday, August 17, 2015 at 8:25:05 AM Eastern Daylight Time
**From:** Challener, David C.
**To:** UseOfISO

The one thing I don't like about this proposal is that there appears to be no way to get copies of the standards for free.
I thought that for the legal system that was mandatory – you can't have laws /rules that cost money to read. Is there any
way to have copies of the rules that a normal citizen can read without paying money?

**Subject:** ATTN Use of ISO/IEC 19790
**Date:** Monday, August 17, 2015 at 5:33:38 AM Eastern Daylight Time
**From:** Alan Gornall
**To:** UseOfISO

(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?
No one has yet asked me for ISO 19790 evaluation, but users are becoming confused and are asking about the standard. They are still only asking for FIPS 140 though.

(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?
See (1) above.

(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?
I do not have access to the ISO standard.

(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?
I think that the ISO standard would require modification to serve the US federal market, such as providing a FIPS 140 wrapper that would allow for a US-specific version with annexes specifying acceptable algorithms, key generation methods, etc, as per the current standard.

(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?
See (3) above.

(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?
Yes it would.

(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?
I feel that FIPS 140-2 does need to be updated. There are areas of the standard where it is no longer practical to meet the specific requirements, such as in the higher levels for O/S requirements and also, there are standard attacks such as side-channel analysis that some modules are increasingly vulnerable to that vendors are not specifically required to address. But I do feel that the standard still works in the majority of cases and that it only needs tweaking and not wholesale change. The community understands the standard. Any major change to it or the evaluation process could have a dramatically negative effect in the short to medium term, as vendors may struggle to deliver compliant modules.

Regards,

Alan Gornall
Rycombe Consulting Limited

Office: +44 (0) 1273 476366
Email: alan.gornall@rycombe.com
Skype: alangornall
Web: www.rycombe.com
LinkedIn: http://tinyurl.com/rycombe

**Subject:** ISO/IEC 19790:2014 feedback
**Date:** Thursday, August 13, 2015 at 9:13:30 AM Eastern Daylight Time
**From:** Held, Douglas
**To:** UseOfISO

(1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?

(2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?

(3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?

I believe that ISO/IEC 19790:2014 is "better" than FIPS-140-2 because it does not include the Dual Elliptic Curve Deterministic Random Bit Generator, commonly known as "DUAL_EC_DRBG" from NIST SP 800-90A. This algorithm in its FIPS-140-2 compliant state, is widely observed to fail the "Nothing Up My Sleeve" requirement.

(4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?

I believe that adoption of FIPS-140-2 is "riskier" than SO/IEC 19790:2014 because FIPS-140-2 includes the Dual Elliptic Curve Deterministic Random Bit Generator, commonly known as "DUAL_EC_DRBG" from NIST SP 800-90A. This algorithm in its FIPS-140-2 compliant state, is widely observed to fail the "Nothing Up My Sleeve" requirement.

(5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?

(6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?

Yes.

(7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of cryptographic modules?

**Douglas Held** | Principal Security Consultant | **Security Consulting**
+44 7876 831393 | dheld@netsuite.com
NetSuite: Where Business is Going | **London Office**

**Subject:** Comment on using ISO/IEC 19790:2012 as the U.S. Federal Standard for cryptographic modules
**Date:** Wednesday, August 12, 2015 at 2:45:21 PM Eastern Daylight Time
**From:** Peter Alterman
**To:** UseOfISO
**CC:** Mollie Shields-Uehling

SAFE-BioPharma Association thanks CSRC/NIST for the opportunity to support this idea enthusiastically. CAs that provide X.509-based services to the global business community need to have common standards for as many of the services supporting digital certificate issuance and management as possible.

SAFE-BioPharma pharmaceutical members include AbbVie, Astellas, AstraZeneca, Bayer Healthcare, Bristol-Myers Squibb, GlaxoSmithKline, Eli Lilly, Merck, Pfizer, and Sanofi, among others. For more information about SAFE-BioPharma, visit: www.safe-biopharma.org.

/s/

---

Peter Alterman, Ph.D.
Chief Operating Officer
SAFE-BioPharma Association
cell: 301-943-7452