FIPS 140, Quo Vadis?

Apostol Vassilev, Ph.D.
Technical Director - CMVP
NIST

(ICMC15, Rockville, MD, November 6, 2015)

Acknowledgments

- **Many of the ideas in this presentation are the result of numerous conversations with my NIST colleagues**

  - **Michael Cooper**
  - **Murugiah Souppaya**
  - **Matthew Scholl**
  - **Donna Dodson**

- **Thanks for their thoughtful input and support!**

Some facts about FIPS 140

- FIPS 140-1 was issued on January 11, 1994
  - developed by a government and industry working group

- FIPS 140-2 was issued on May 25, 2001
  - only very modest changes compared to predecessor

Observation

It is hard for an essentially unchanged security standard to capture well the incredibly fast evolving domains of cybersecurity and cryptography.

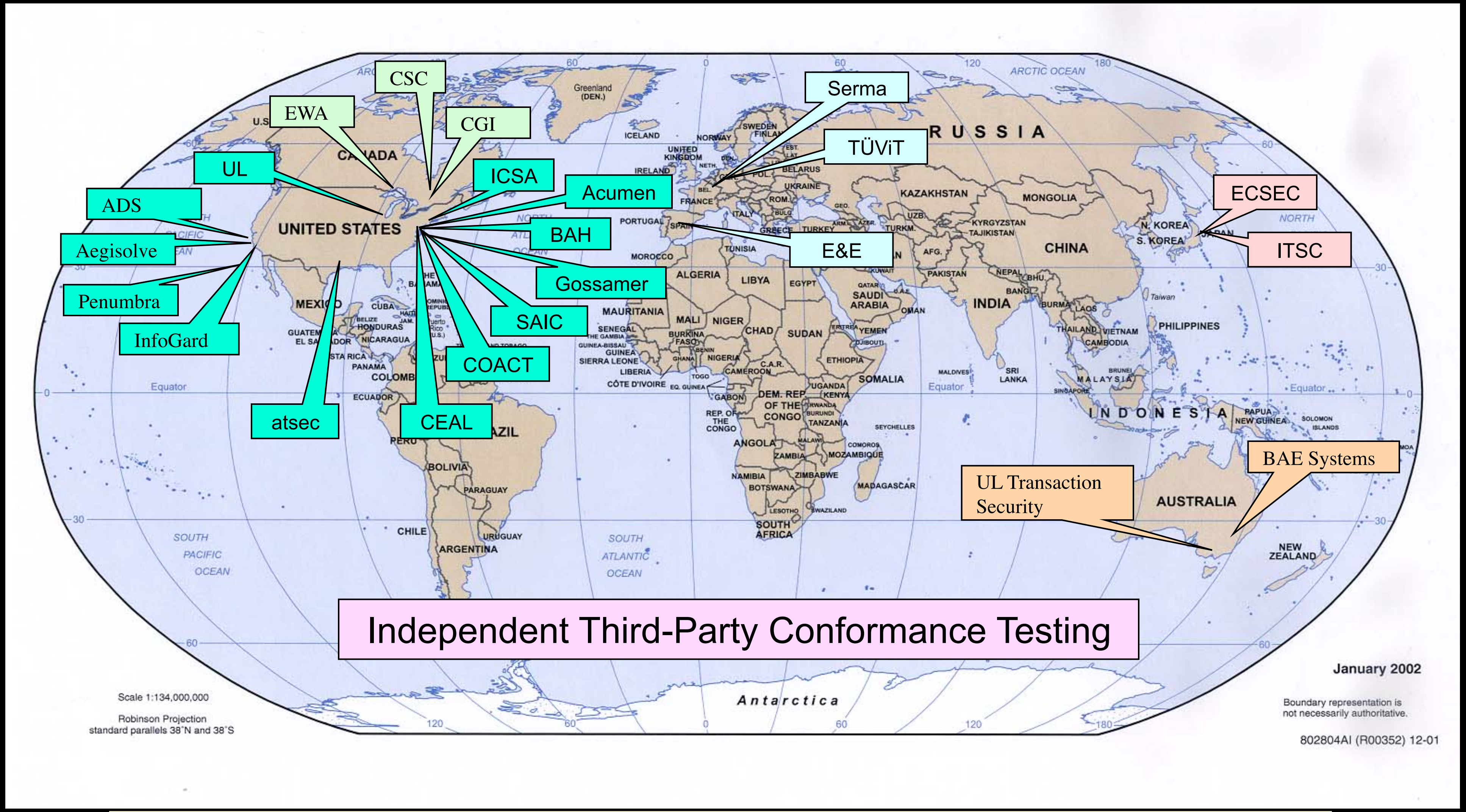
Some background on the CMVP

MISSION:

Improve the security and technical quality of cryptographic modules employed by Federal agencies (U.S. and Canada) and industry by

- developing standards;
- researching and developing test methods & validation criteria;
- leveraging accredited independent third-party testing laboratories

International footprint of CMVP



Independent Third-Party Conformance Testing

Development of standards, test artifacts, proficiency exams and training

NVLAP HB 150-17: Cryptographic and Security Testing

CMVP Testing and Validation

Vendor	CST Lab	CMVP NIST and CSEC	User
Designs and Produces Hardware • Software • Firmware	*Tests for Conformance* Derived Test Requirements	*Validates*	*Specifies and Purchases*
Define Boundary Define Approved Mode of Operation Security Policy	CAVP Algorithm Testing Documentation Review Source Code Review Operational and Physical Testing	Review Test Results Ongoing NVLAP Assessment Issue Certificates NIST Cost Recovery Fee	Security and Assurance Applications or products with embedded modules

The party of four

Govt. Agencies

CMVP

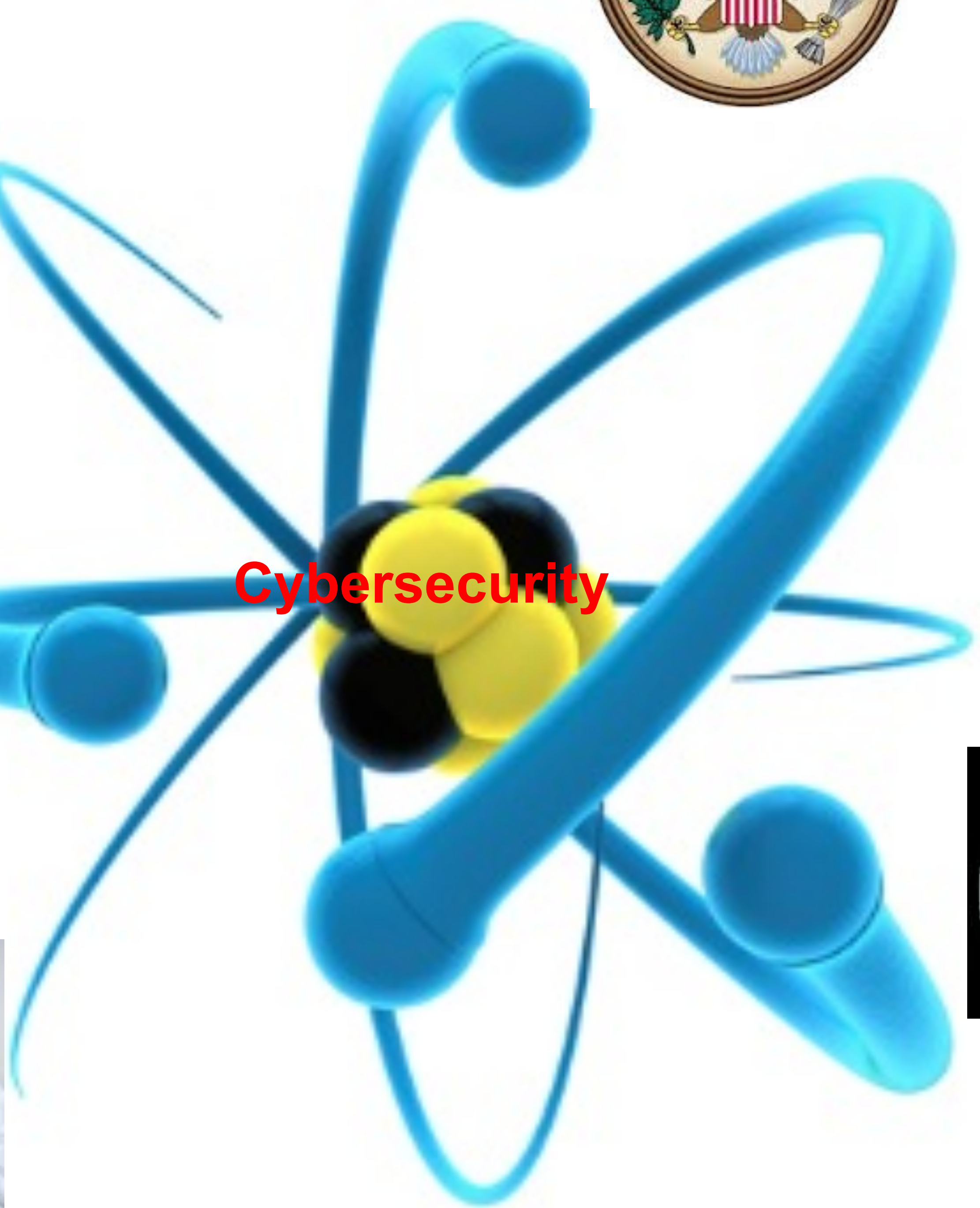
FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Certificate No. xxx



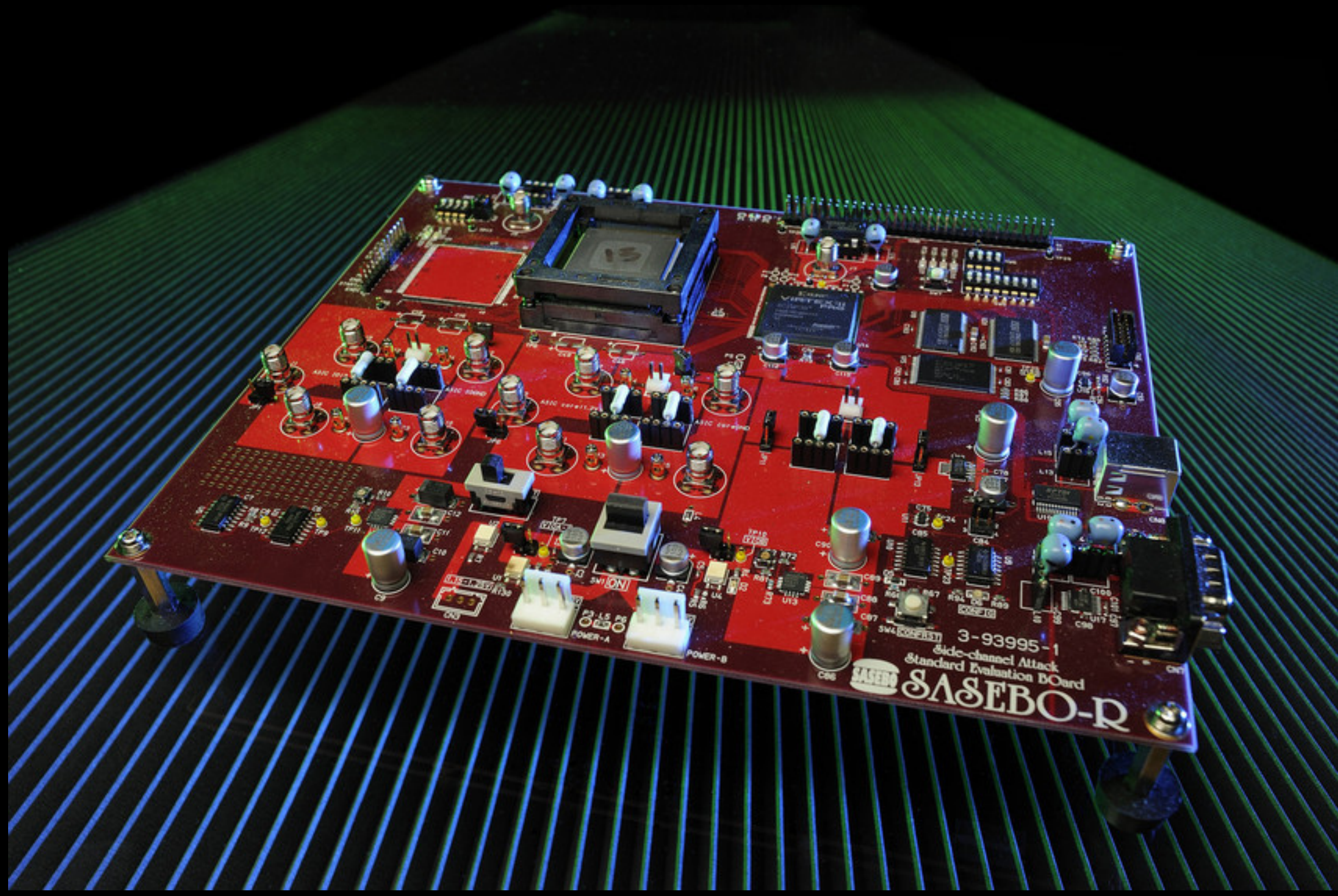
Hi-Tech Industries

CST Labs

Industry perspectives on CMVP

- long review cycles
  - well beyond product cycles

- security test requirements
  - software is not covered well
  - physical security testing has not kept up with state-of-the-art e.g., low-cost fault injection



- relationship w/ other Government Programs
  - e.g., NIAP and CC

CMVP and CST Labs

- **Labs concerned with fast-changing Implementation Guidance**
    - **the tire between crypto standards and industry**
    - **CMVP-NIST started applying interpretation of the standard, instead of strict constructionism**

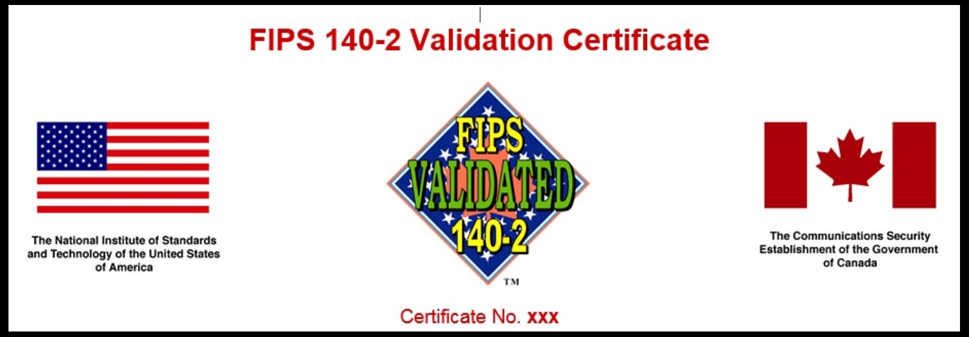
- **CMVP concerned with Labs' competency in challenging technical areas, e.g.,**
    - **entropy & physical security testing**

      competency <u>unevenly</u> distributed among labs

- **CMVP concerned with Labs' ability to avoid conflicts of interest**

The metamorphosis effect

Module validated <u>without</u> a single implementation change



FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS
VALIDATED
140-2
TM

The Communications Security Establishment of the Government of Canada

Certificate No. xxx

Test report review uncovers <u>significant</u> discrepancies

documentation-only metamorphosis

A systemic problem casting doubts on security assurances due to lack in trust in laboratory testing

Agencies and CMVP

- long review cycles
  - slowing down adoption of latest technology

- difficult-to-use validation results
  - difficult-to-read validation certificates
    - caveats, operational environment versioning, etc;
  - confusing configuration instructions in Security Policies

- inability to get real-time FIPS-mode compliance data
  - no SCAP hooks for module configuration

- relationship w/ other government programs
  - e.g., NIAP and CC

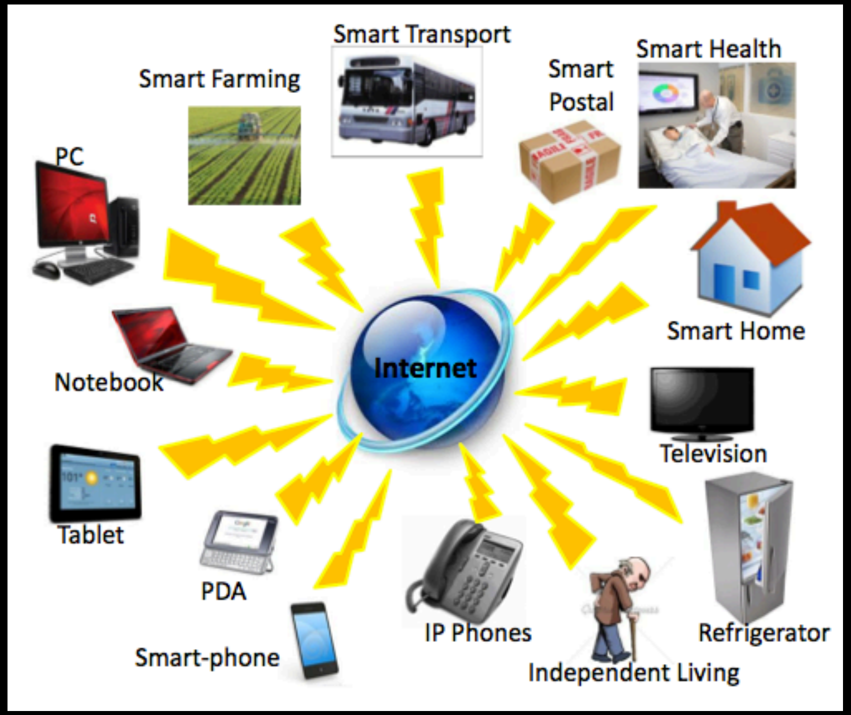
A look at the challenges ahead

- The Internet of Things

  - likely to bring unprecedented cybersecurity challenges

  - new crypto technologies/standards
    - lightweight crypto

  - focus on
    - physical security
    - crypto leaks via side channels



More challenges ahead

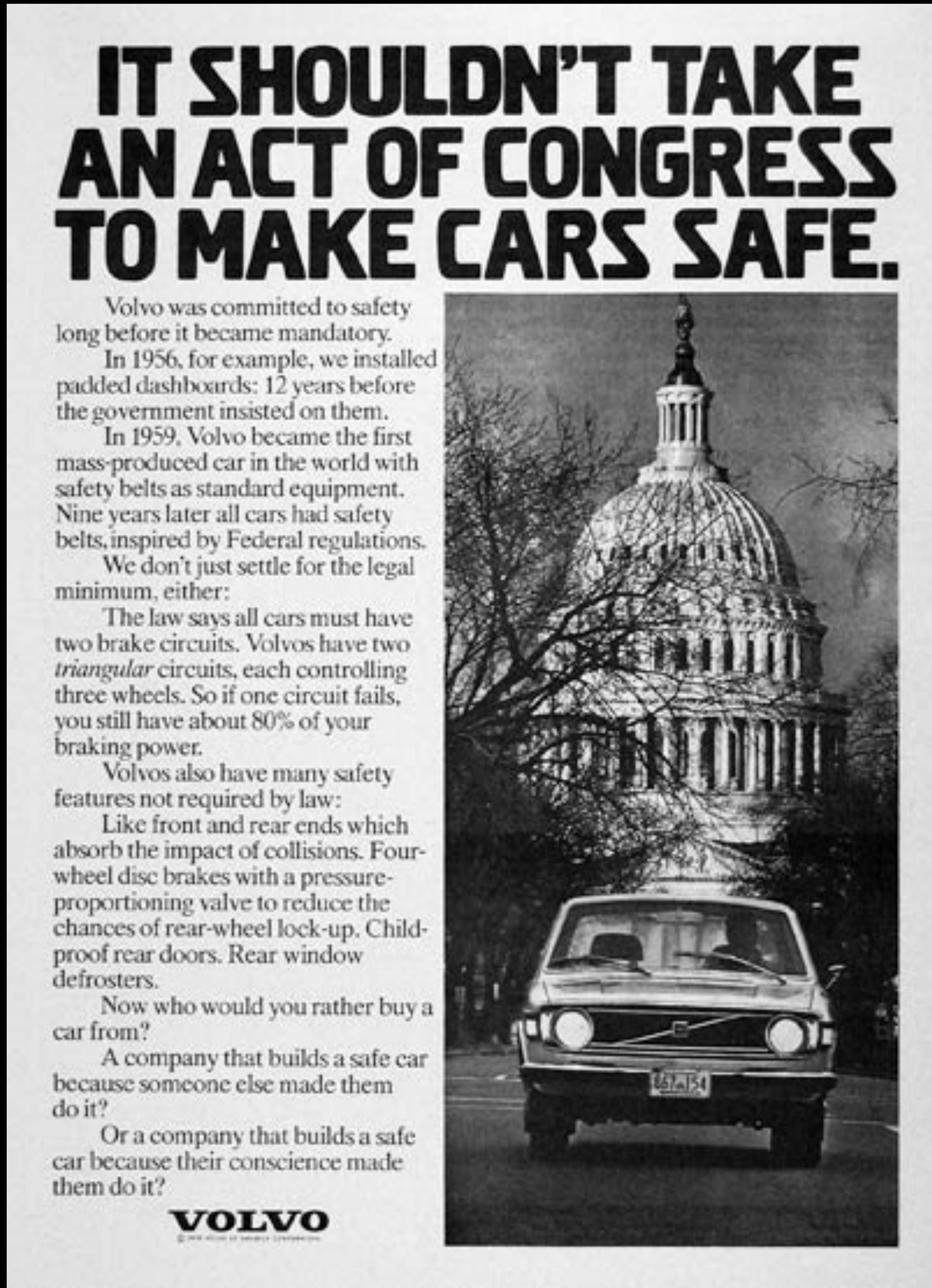
- The economy of cybersecurity - slow to emerge

- The Economist in 2014 declared a market failure in cybersecurity

- main reason - the way computer code is produced

- automotive industry experience – a useful guide
  - turning car safety into a competitive advantage

the Volvo effect



IT SHOULDN'T TAKE AN ACT OF CONGRESS TO MAKE CARS SAFE.

Volvo was committed to safety long before it became mandatory.

In 1956, for example, we installed padded dashboards: 12 years before the government insisted on them.

In 1959, Volvo became the first mass-produced car in the world with safety belts as standard equipment. Nine years later all cars had safety belts, inspired by Federal regulations.

We don't just settle for the legal minimum, either:

The law says all cars must have two brake circuits. Volvos have two *triangular* circuits, each controlling three wheels. So if one circuit fails, you still have about 80% of your braking power.

Volvos also have many safety features not required by law:

Like front and rear ends which absorb the impact of collisions. Four-wheel disc brakes with a pressure-proportioning valve to reduce the chances of rear-wheel lock-up. Child-proof rear doors. Rear window defrosters.

Now who would you rather buy a car from?

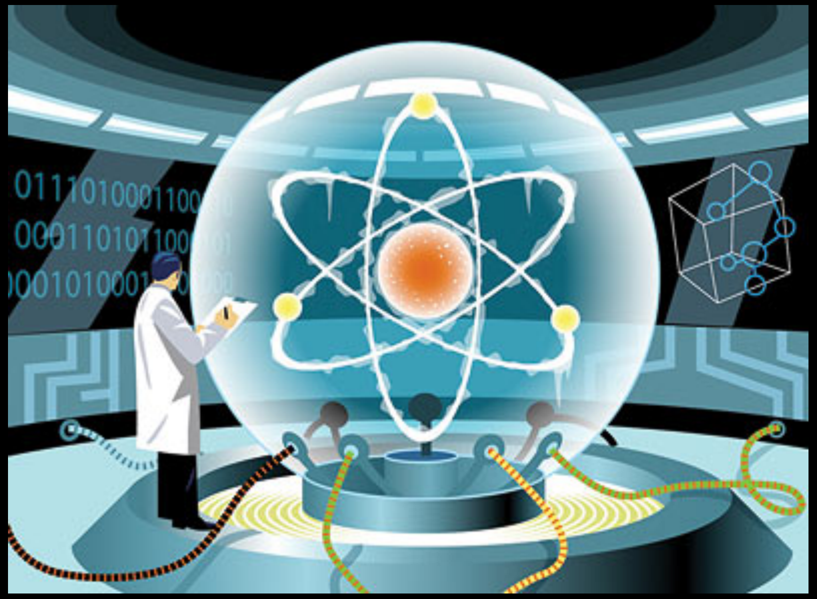
A company that builds a safe car because someone else made them do it?

Or a company that builds a safe car because their conscience made them do it?

VOLVO

And more challenges…

- The evolution of cryptographic technology



  - quantum computing
  - post-quantum cryptography

- The evolution of hacker capabilities

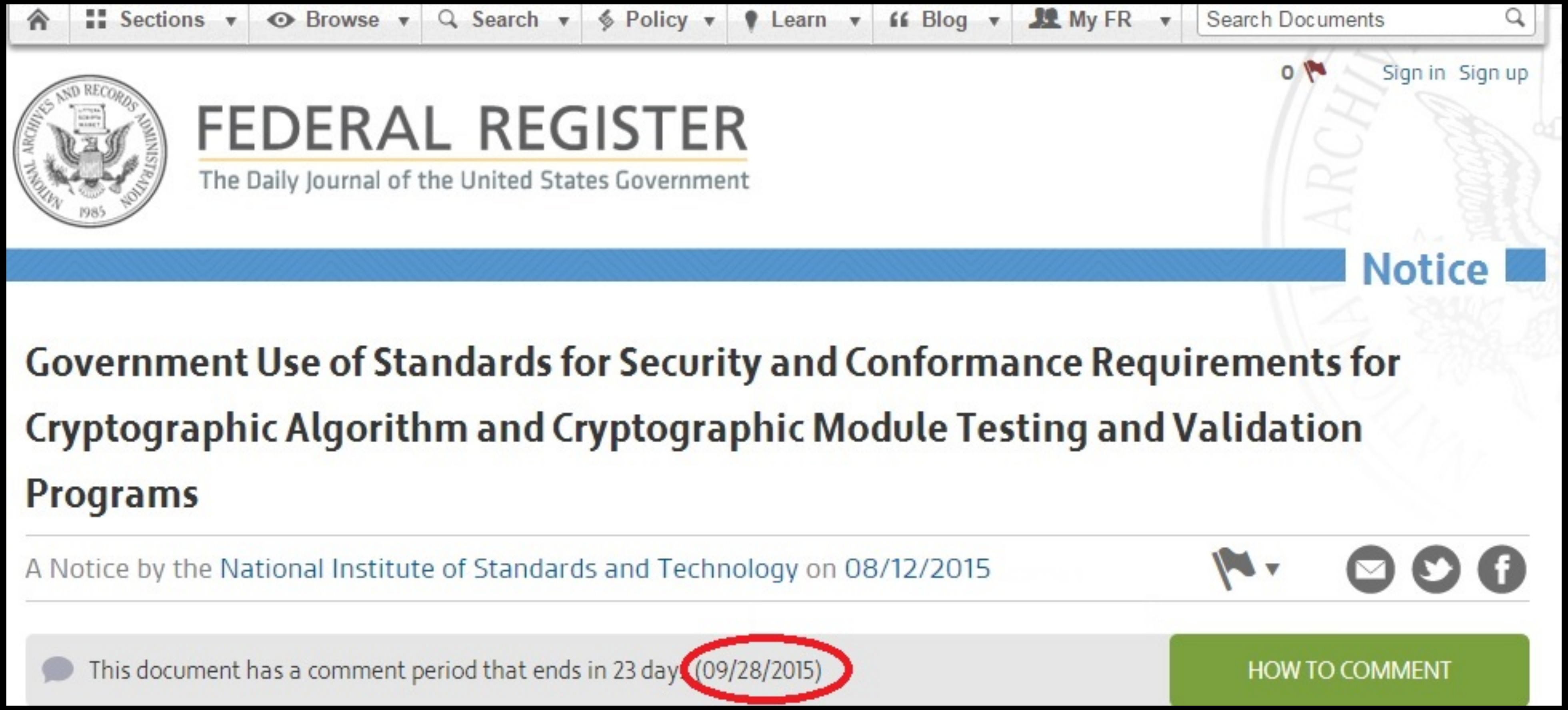
  - increases of crypto complexity come with increased brittleness
  - advances in factoring allow breaking low entropy keys
  - the combination of low-cost fault injection w/ IoT could be painful

Putting it all together

- Monty Python:
  The Royal Society for putting things on top of other things

Changing standards

- NIST is considering adopting ISO 19790 as FIPS 140-3
  - comment period closed on September 28, 2015



FEDERAL REGISTER

The Daily Journal of the United States Government

Notice

Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs

A Notice by the National Institute of Standards and Technology on 08/12/2015

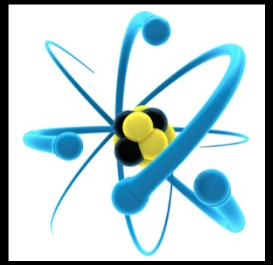
This document has a comment period that ends in 23 days (09/28/2015)

  - currently analyzing the received feedback

- Provides a <u>rare</u> opportunity to reorganize the CMVP

Changing the CMVP

- NIST intends to continue to specify the cryptographic modules, modes and key management schemes that are acceptable for use by the U.S. Government



- A big job spanning the interests of the four constituents
  - create a working group with representatives from government, industry, laboratories and academia
    - leading experts affiliated with entities with deep knowledge and understanding of security, standards and the program
    - Interested? Send email to Apostol.Vassilev@nist.gov

Ideas for changing the CMVP

- **Tackle the problem of depth and scope of testing**
  - **leverage mature industrial security development processes like**

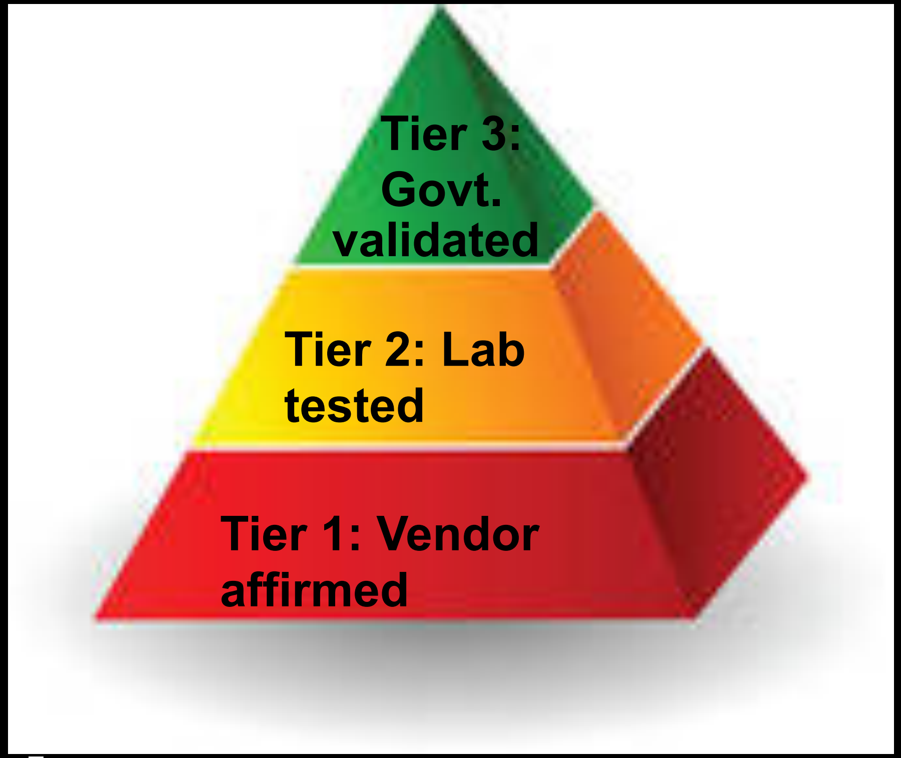
    ISO/IEC 27034 Information technology — Security techniques — Application security

  - **reuse vendor test evidence in government validations**
    - **require laboratories to verify evidence, <u>not</u> recreate it 100% independently**
    - **refocus laboratories on testing beyond what is already tested by vendors**

  - **develop a <u>measurement criteria</u> for reusing test evidence**

Ideas for changing the CMVP

- Tackle the problem of length of validation testing
  - introduce a three-tier assurance model



  - allow companies with mature security development process to participate in Tier 1
    - if not in Tier 1, a company must work with Labs for Tier 2
    - the Volvo effect?
  - allows the industry to enter early markets that require Tier 1 or 2
  - focused lab testing would help shorten Tier 2 timespan
    - without sacrificing depth and scope of testing

Ideas for changing the CMVP

- Tackle the problem of length of validation testing
  - automate internal validation processes
    - first stage to be deployed this month

  - increase program capacity by employing contractors to help with report reviews
    - already in progress
  - streamline access to algorithm validation test data via Web services
    - high on the industry wish list

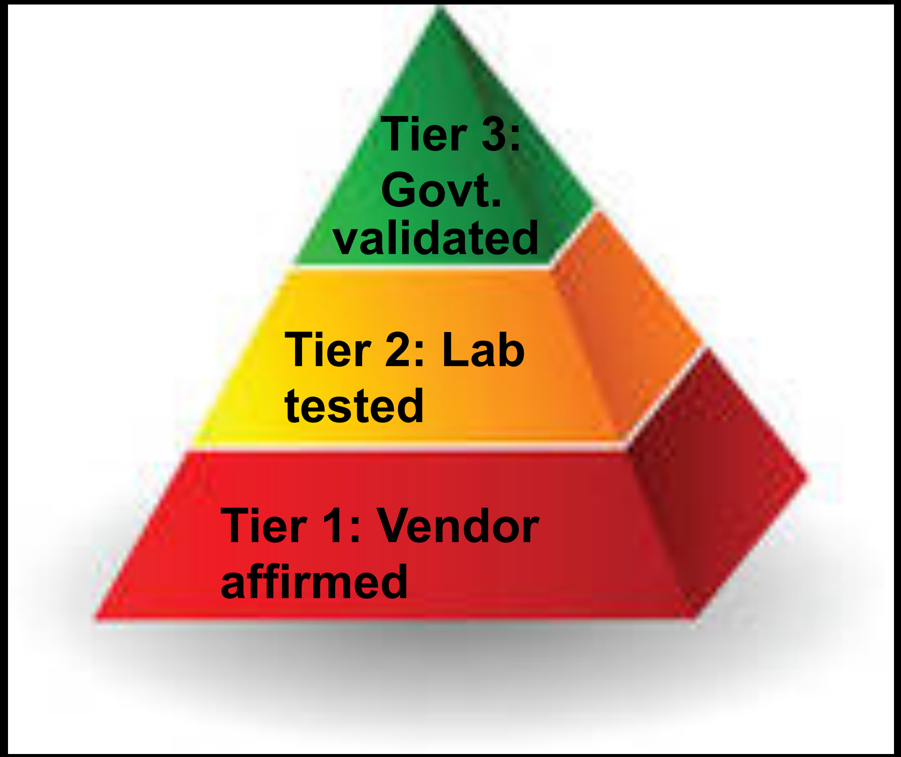
Ideas for changing the CMVP

- **Help US industry access to international markets**

  - **Leverage adoption of the ISO standard to establish bilateral partnerships with other validation programs from Asia & Europe**
    - **allow companies to choose the validation authorities they want to target**
    - **not like the mutual recognition in Common Criteria**
    - **retain independence of US program**
  - **Align cryptographic module testing w/ NIAP PP’s**

Ideas for changing the CMVP

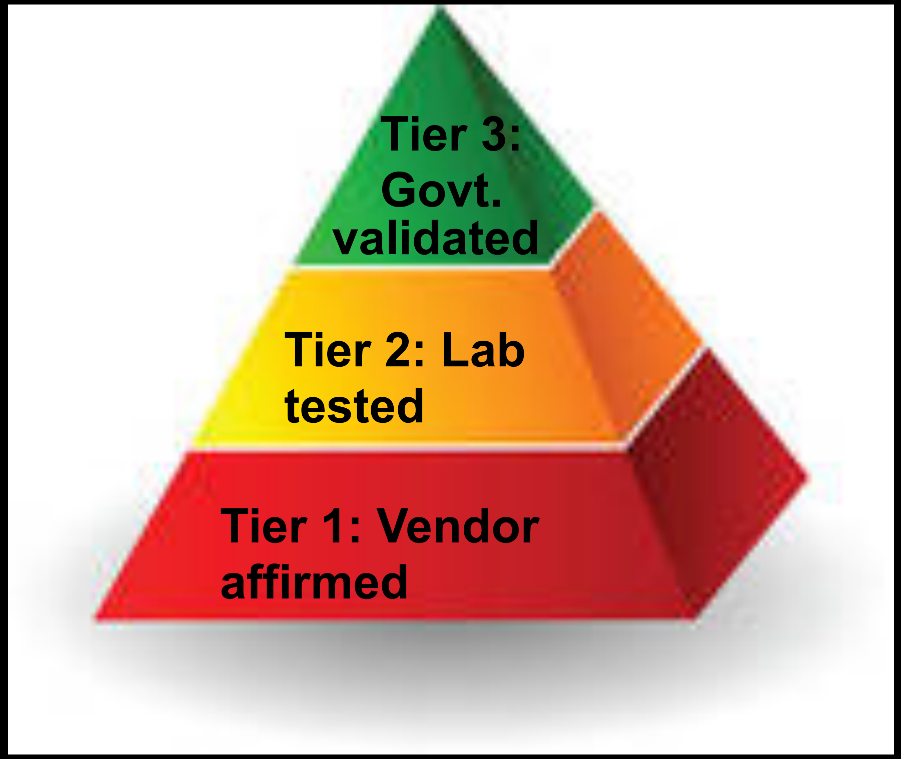
- Three-tier assurance benefits for Govt. Agencies
  - allows for risk management in timely adoption of new technology



  - allows for much shorter cycles of patching validated modules
  - promotes proper differentiation of government and national security priorities vs. commercial applications
    - Tier 3 intended for U.S. govt. & national security systems
    - Tier 1 and 2 could be used in other markers where FIPS 140-2 validations are <u>voluntarily</u> used today

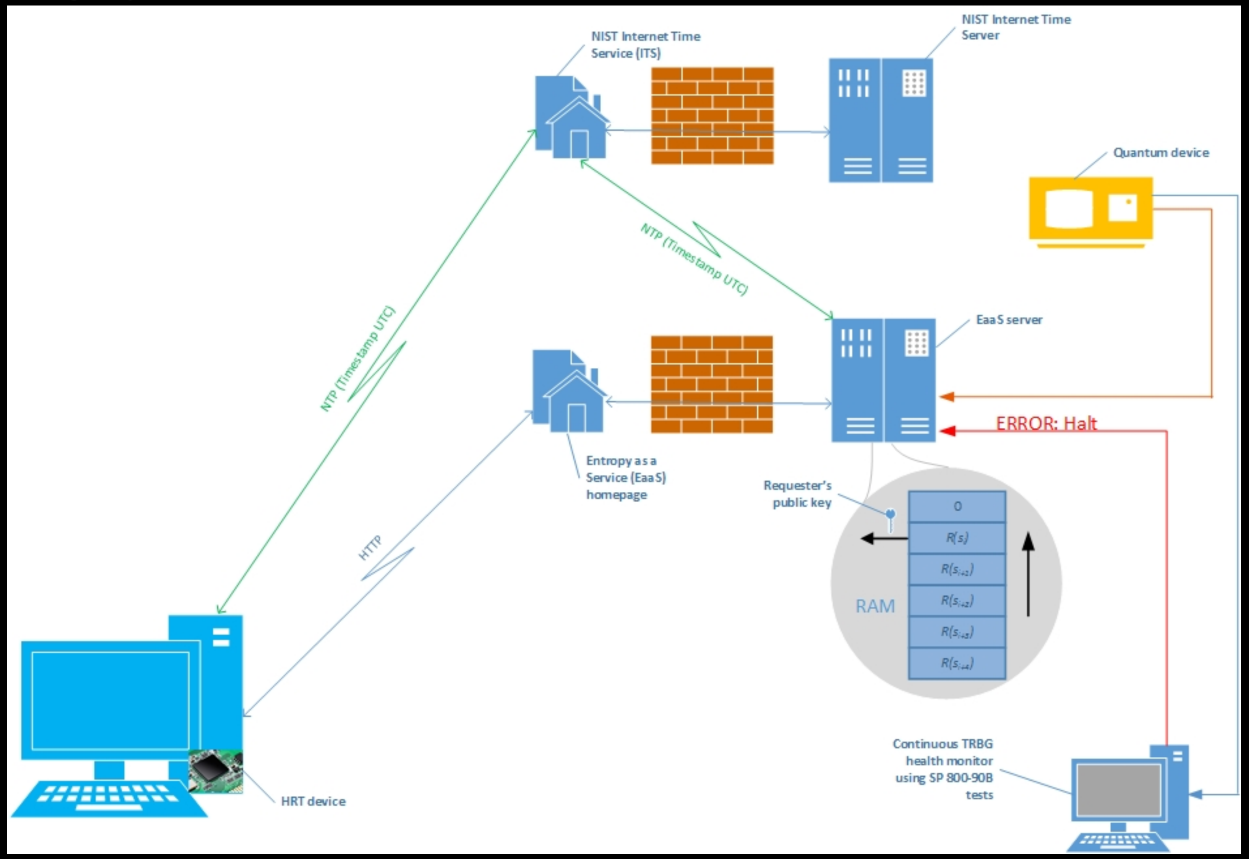
Ideas for changing the CMVP

- Tackle the problems of lab competency and conflict of interest
  - introduce <u>dual</u> lab reviews for Tier 2
    - one lab validates the work of another
    - eliminates the metamorphosis problem
    - accounts properly for lab competency and capability
  - tighten lab accreditation requirements
    - already implemented with NVLAP
    - rigorous competency exams and stringent quality measures starting this fall



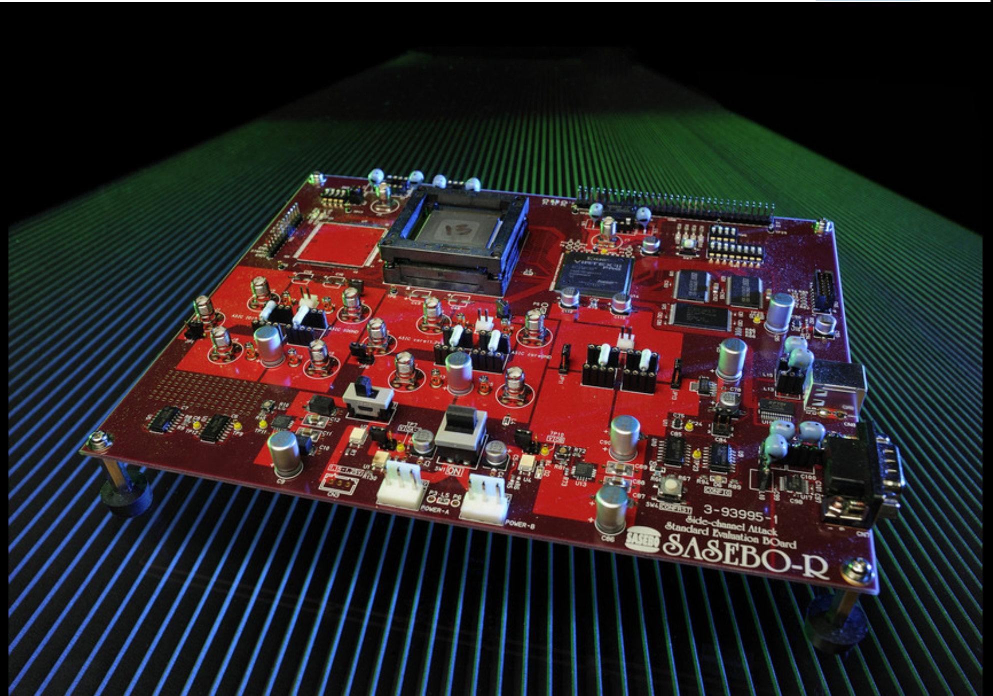
Ideas for changing the CMVP

- Help the industry and the labs meet difficult security requirements by introducing technology innovations
  - Entropy as a Service
    - leverages known good sources
    - eliminates complex estimation
    - see <u>demo on Thursday, 11:25 am</u>



  - Working w/ leading academic institutions (Univ. Maryland, KU Leuven Belgium) on leakage-resistant crypto

  - Advanced physical security testing
    - developing artifacts for rigorous lab competency exams



Questions?