CMVP Programmatic Status

Where security starts ….

Mike Cooper and Carolyn French
CMVP

November 5, 2015

Outline

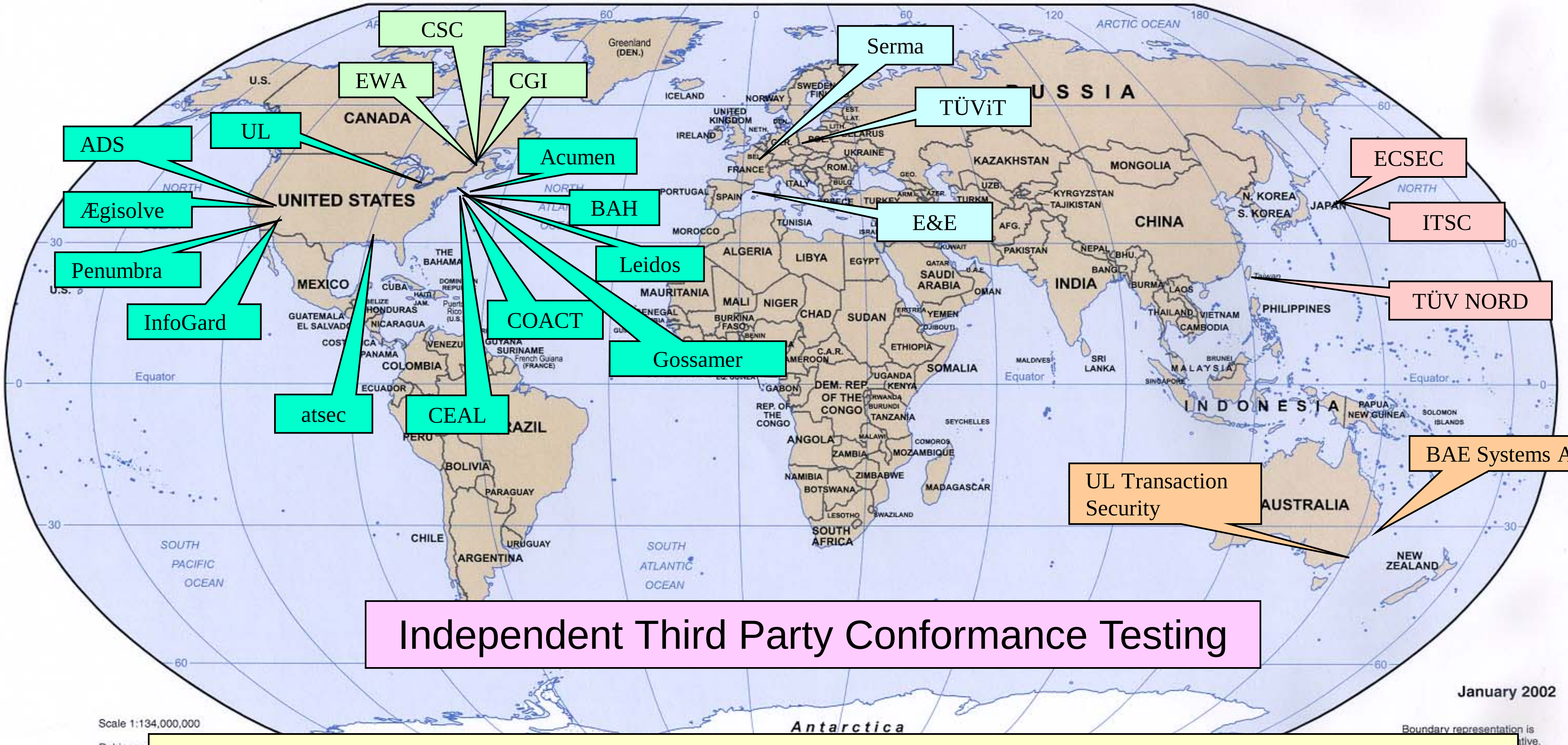
- CMVP Status
- NIST Cost Recovery – One Year Later
- What’s Next?

Mission

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

- the development of Cryptographic Module standards;
- research and development of test methods & validation criteria; and
- accreditation of independent third party laboratories.

23 NVLAP Accredited CST Laboratories



CSC

EWA

CGI

UL

ADS

Acumen

Ægisolve

BAH

Penumbra

Leidos

InfoGard

COACT

Gossamer

atsec

CEAL

Serma

TÜViT

E&E

ECSEC

ITSC

TÜV NORD

BAE Systems AI

UL Transaction Security

Independent Third Party Conformance Testing

Development of standards, test artifacts, proficiency exams and training

NVLAP HB 150-17: Cryptographic and Security Testing

Status

September 30, 2015

- Continued growth in the number of cryptographic modules validated for conformance to FIPS 140-2
  - **2454** Validations representing all four security levels
  - 500+ vendors
- Average time for modules at Review Pending stage
  - Generally less than 3 months
  - NIST Cost Recovery must be paid before review can begin

NIST Security Testing, Validation and Measurement Group

- 4 Testing programs
  - CAVP, CMVP, SCAP and PV + the NVD
  - Supported by contractors for CMVP report review and tool development

CSE COTS Assurance Programs:

- CMVP: 5 Staff
  - 3 Reviewers, 1 Admin, 1 Program Manager
- Common Criteria: 5 Staff
- Tailored Assurance Program (in house)

NIST Cost Recovery

- **FY15**
  - IG G.8 Scenario's 1, 2 and 4: CR fee N/A, ECR fee: $1000
  - IG G.8 Scenario 3: CR fee $2000, ECR fee: $1000
  - IG G.8 Scenario's 1A, 1B and 5:
    - Security Level 1: CR fee: $4250, ECR fee: $2000
    - Security Level 2: CR fee: $5750, ECR fee: $3000
    - Security Level 3: CR fee: $8000, ECR fee: $4000
    - Security Level 4: CR fee: $11000, ECR fee: $5000

- **FY16 – No change from above**

NIST Cost Recovery – One year later

- **Funding of contractors used for:**
  - **Assist in CMVP report review**
  - **Internal CAVP and CMVP Automation development**
    - **On October 7, NIST went live with its automated report processing tool; this tool frees up CMVP resources for report review and guidance development.**

What’s Next: ISO?

- **August 12, 2015:**
  - NIST published a Federal Registry Notice seeking public comment on the potential use of certain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by Federal Information Processing Standard (FIPS) 140-2.

- **September 28, 2015:**
  - Close of FRN comment period
  - Feedback currently being adjudicated

Points of Contact

NIST

- **Jennifer Cawthra** – Program Manager, CMVP
  jennifer.cawthra@nist.gov
- **Apostol Vassilev** – NIST CMVP Technical Director
  apostol.vassilev@nist.gov
- **Mike Cooper** – Manager, Security Management & Assurance Group
  michael.cooper@nist.gov

CSE

- **Carolyn French** – Program Manager, CMVP
  carolyn.french@CSE-CST.GC.CA
- **Dan McCarthy** –Manager, COTS Assurance Programs
  daniel.mccarthy@CSE-CST.GC.CA