NIST and NIAP: Working Together

Mary Baish
Deputy Director, NIAP
Matt Scholl
Chief, Computer Security Division

ICMC May 19, 2016

NIST and NIAP: Working Together

- Collaboration Goals
- International Standards
- International Agreements
- Automation

NIST and NIAP: Working Together

Collaboration Goals:

- Partnership is Re-invigorated
- Eliminate duplicative testing
  - *NIAP recognizes CST lab test activities conducted as part of a CAVP/CMVP validation to meet NIAP assurance activities (NIAP Policy #5 and FAQ)*
  - *NIST recognizes CCTL test activities conducted as part of a NIAP evaluation to meet CAVP/CMVP requirements*
- CMVP points to NIAP Protection Profiles for necessary assurances outside the scope of the module
- Alignment between NIAP PPs and CMVP DTRs/IGs

International Standards

- **International Standards Organization**
  - **ISO/IEC 19790** *Security Requirements for Cryptographic Modules*
    - *Published August 2012*
  - **ISO/IEC 24759** *Test requirements for cryptographic modules*
    - *Published January 2014*
- **NIST recognition and use of ISO/IEC 19790**
  - Federal Register Notice published Aug 12, 2015 and closed end of Sep
  - Most Comments were on ISO pay model
  - Negotiating a contract with ANSI/INCITS on bulk purchase of 2000 licenses
  - Also asking for permission to post the standards during NIST open comment period
- US Standards necessary to support the ISO
  - FIPS 140-3 wrapper to point to ISO
  - FIPS140-3 appedixes A-F point to ISO appendixes and to SP 800-140 A-F
  - SP 800-140 – points to ISO 24759

International Standards

ISO/IEC 15408

- **CCRA Goal is international Mutual Recognition, tied to national procurement**
- **“Evaluate once, sell to many”**
- **Industry, government, end users develop collaborative Protection Profiles in international Technical Communities**

International Agreements

- NIST/CSE Agreement
  - Working to change language that prohibits the sharing of test data to allow if authorized by the vendor.
- Agreements with other validating authorities
  - After public announcement on ISO 19790 decision
  - Requires the same intellectual property protections
- Agreements will be based on the sharing of the test data
  - Based on the same standards and validation processes
  - Does not imply Common Criteria mutual recognition

International Agreements

Support WTO – (minimizing Technical Barriers to Trade)

- Benefits government and industry
- International Technical Communities- allow all stakeholders to have input into test requirements
- Minimize duplicative evaluation regimes
- Internationally accepted evaluation norms for all member nations
- Use of international standards/protocols

CCRA International Crypto Working Group –

- Coalesce on widely accepted crypto requirements
- Allows nations to include their preferred crypto as options in cPPs
- Coordination with industry

Automation

- CMVP Automation – aka Resolve
  - Internal system in use by CMVP now.
  - Fine tuning and bug fixes still ongoing.
  - Still working on adding new infrastructure
- Next Phase – externally focused
  - First task – automate validation lists
  - Add ability to enter/upload test data and files

Automation

- Secure, online document, data upload
- Process Efficiencies
  - Assurance Maintenance
  - ECR tool – improvements underway
- Technical Rapid Response Team tool – coming soon

For More Information

NIAP website: www.niap-ccevs.org
email: niap@niap-ccevs.org
phone: 410.854.4458

CCRA: www.commoncriteriaportal.org

CSD website: csrc.nist.gov

CAVP email: cavpask@nist.gov

CMVP email: cmvp@nist.gov

Questions/Suggestions