

# **NIST and NIAP: Working Together**

**Janine Pedersen**  
*Director, NIAP*

**Michael Cooper**  
*Manager, Security Testing Validation and Measurement Group*

**ICMC Nov 6, 2015**

# **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

# NIST and NIAP: Working Together

- **Technology stack**
  - *NIST focus is on lower layers, ie. algorithm and module*
  - *NIAP tests layers above the module*
  - *Programs are complementary*
- **NIST/CSE working toward adoption of OS, mobile device, and network device Protection Profiles**
- **Lab test results that pertain to both CMVP and NIAP can be performed and recorded once and used as inputs to both programs**

# 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
  - Will respond to comments received by the end of Nov
  - Will submit recommendation to the Commerce secretary by end of year
  - Transition period of 1 year from approval date
- **US Standards necessary to support the ISO**
  - FIPS 140-3 wrapper to point to ISO and to SP
  - SP 800-175D Management Manual
  - NISTIR 8019 Implementation Guidance

# 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
  - CCRA defining international cryptographic requirements for inclusion in cPPs, coordinating w/industry:
    - *Coalesce on widely accepted crypto requirements*
    - *Allows nations to include their preferred crypto as options in cPPs*

# International Agreements

- NIST/CSE Agreement
  - Working with NIST Legal 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

## NIAP/NIST 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



# 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
- Work with NIAP/Mitre to determine viability of integration between systems.

# Automation

- NIAP evaluation support tool
- Secure, online document, data upload
- Process Efficiencies
- Technical Rapid Response Team tool - coming soon

# For More Information

NIAP website: [www.niap-ccevs.org](http://www.niap-ccevs.org)  
email: [niap@niap-ccevs.org](mailto:niap@niap-ccevs.org)  
phone: 410.854.4458

CCRA: [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

CSD website: [csrc.nist.gov](http://csrc.nist.gov)

CAVP email: [cavpask@nist.gov](mailto:cavpask@nist.gov)

CMVP email: [cmvp@nist.gov](mailto:cmvp@nist.gov)

# Questions/Suggestions