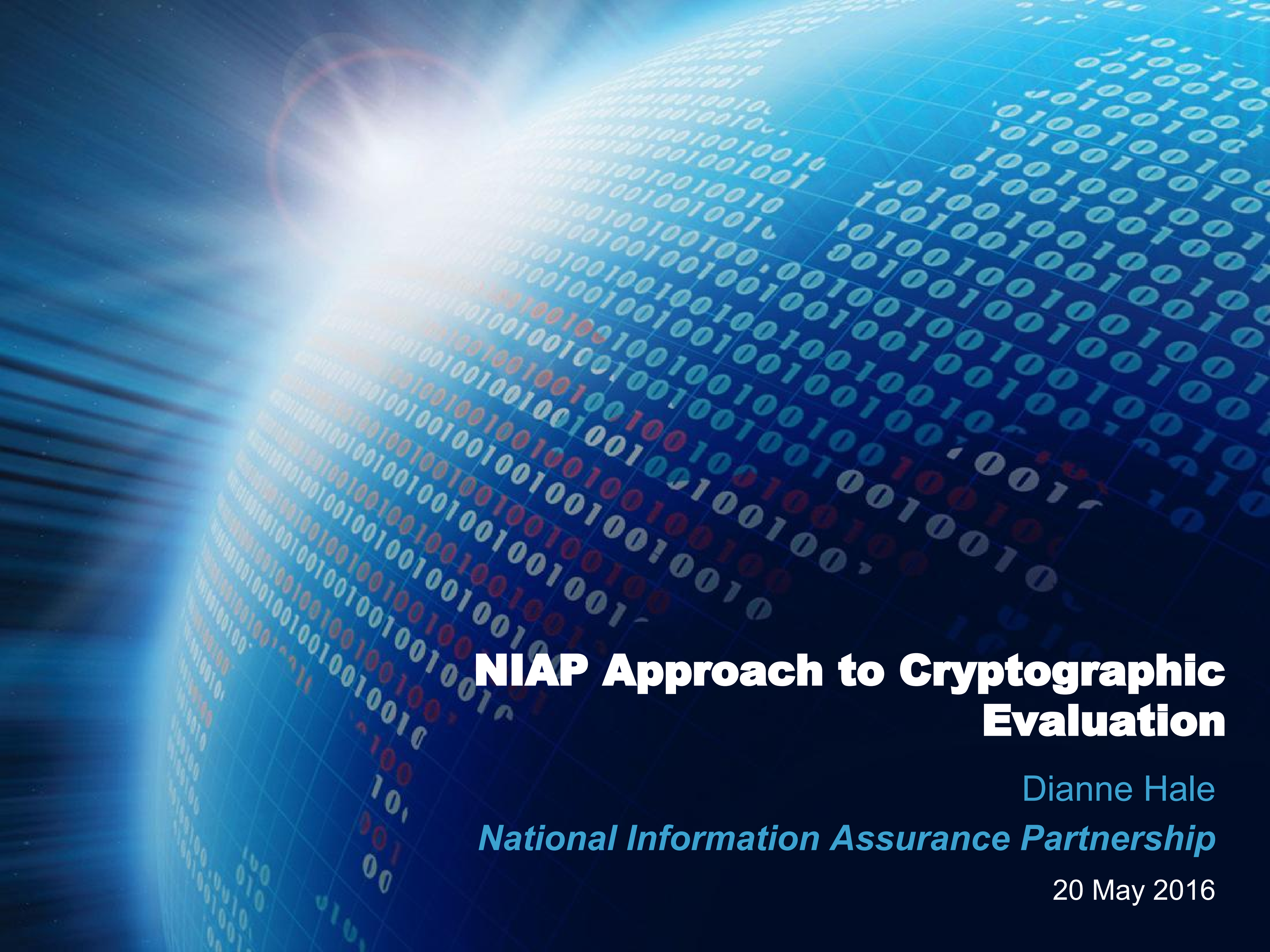

NIAP Approach to Cryptographic Evaluation

Dianne Hale

National Information Assurance Partnership

20 May 2016

NIAP Policy #5

“All cryptography in the TOE which is a NIST approved security function (as specified in FIPS 140-2 Annex A) must be NIST CAVP and/or CMVP validated. At minimum an appropriate NIST CAVP certificate is required before a NIAP CC Certificate will be awarded.”

DoD mandates a CMVP (FIPS 140-2) certificate for products procured for use in DoD

NIAP and NIST CAVP/CMVP Relationship

- *CAVP/CMVP integral to NIAP certification - almost all COTS products in the market incorporate cryptographic functionality.*

- *NIST crypto standards are applicable to and used by private and public sectors.*

- *NIAP works with NIST to ensure CAVP/CMVP activities are incorporated into NIAP evaluations.*

- *Ensures all crypto functionality is evaluated to a consistent level of rigor.*

NIAP Recognition of CAVP/CMVP

- *Streamlines the NIAP evaluation process,*
- *Reduces cost, and*
- *Eliminates redundant activities – certain NIAP Assurance Activities are met by the CC Test Lab if that testing is conducted as part of a NIST CAVP or CMVP validation.*

NIAP Verification of CAVP/CMVP Certificates

- Product Name
- Operational Environment (CAVP); HW/SW defined in Security Policy (CMVP)
  - Not always easy comparing what's in the ST to the CAVP Operational Environment
- CAVP/CMVP Certificate numbers
- SFRs for which certificates apply
- All public facing documentation (ST, AAR, VR, PCL listing, Admin Guide)

Documentation Review

- *Historical CAVP/CMVP lists are not valid (example, RNG transition).*
- *TSS must match SFR claims.*
- *The DRBG claimed in the ST must match the DRBG described in the Entropy Analysis Report.*
- *Misleading terms - If there are no CMVP claims they may not claim FIPS 140-2.*
- *Claiming both CMVP and CAVP - the CAVP certificates must be included in the CMVP Security Policy.*

How do you know what to look for?

- *Some algorithms have different test methods, only some of which apply to the requirement.*
  - *RSA Key Generation*
  - *RSA Signature Generation*
  - *RSA Signature Checking*
- *Older certificates may be for older standards (186-2 vs. 186-4 for DSS).*
- *Multiple lists may seem to apply.*
  - *KAS, CVL for 800-56A*
- *Some requirements (for crypto) not obvious.*
  - *Algorithms used in Cryptographic Protocols*

CAVP Mapping Document – Coming Soon

- *Addresses all Crypto Requirements.*
  - *Details what CAVP validation lists to look at*
  - *Details what to look for on each list*

- *Requirements not addressed must be performed by CCTL.*

CAVP Mapping Document - Example

SFR: FCS_COP.1.1(1) *The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [selection: CBC, GCM] mode and cryptographic key sizes [selection: 128 bits, 192 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [selection: CBC as specified in ISO 10116, GCM as specified in ISO 19772].*

CAVP Mapping:

- *AES Validation List*
- *Look for "CBC" and/or "GCM" as selected in the ST*
  - *Key sizes (in parentheses for CBC, following "KS:" for GCM) should include all sizes selected in the ST.*
  - *If GCM listing specifies: "IV Generated: (Internally)", the GCM implementation must use the same DRBG that is referenced in FCS_RBG_EXT.1*

Current Efforts and Future Direction

- *NIAP supports the charter of the CMVP WG.*
- *Drafting CAVP mapping document for evaluators/validators to verify certificates are valid for requirements/assurance activities.*
- *US support to the CC International Crypto WG to develop internationally-accepted cryptographic evaluation requirements and assurance activities.*

End Goals

- *Lab test results that pertain to both CMVP and NIAP can be performed and recorded once and used as inputs to both programs.*
- *NIST recognition and use of ISO/IEC 19790 - supports CCRA*
  - FIPS 140-3 wrapper to point to ISO

Questions, Comments, Suggestions?

niap@niap-ccevs.org