CAVP Overview

ICMC 2020

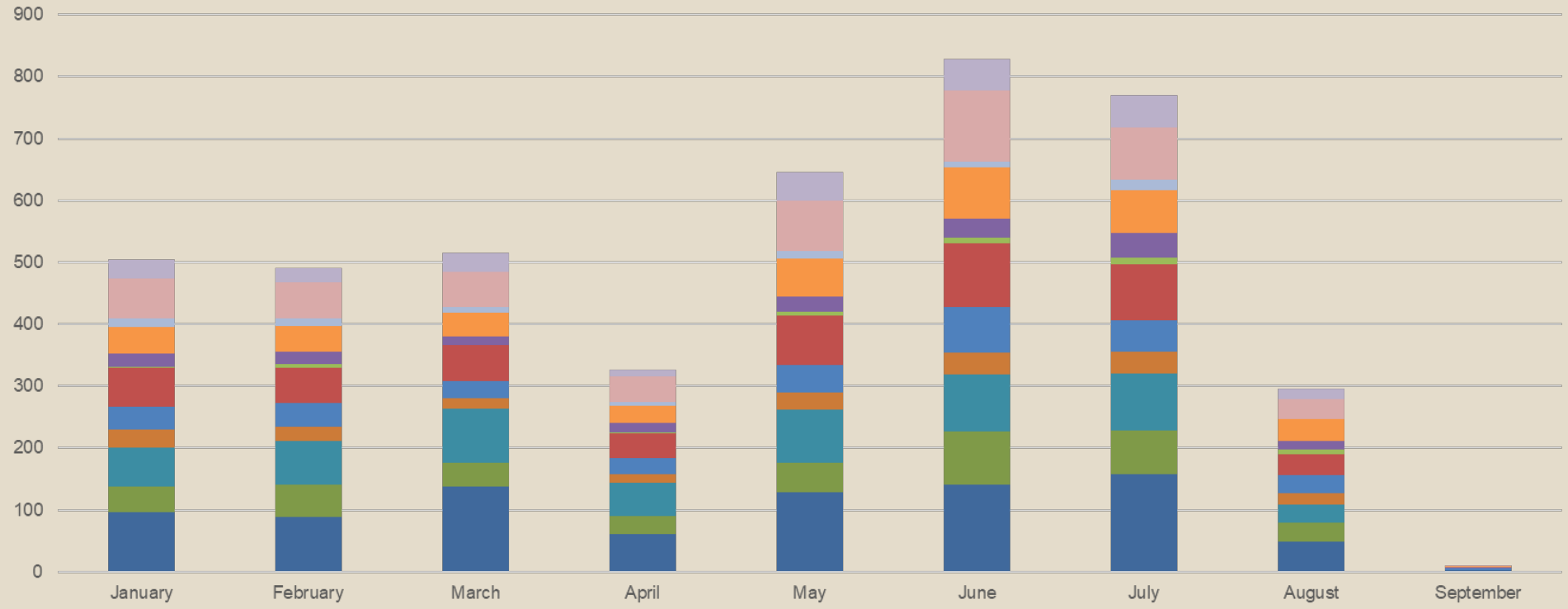
Tim Hall

Chris Celi

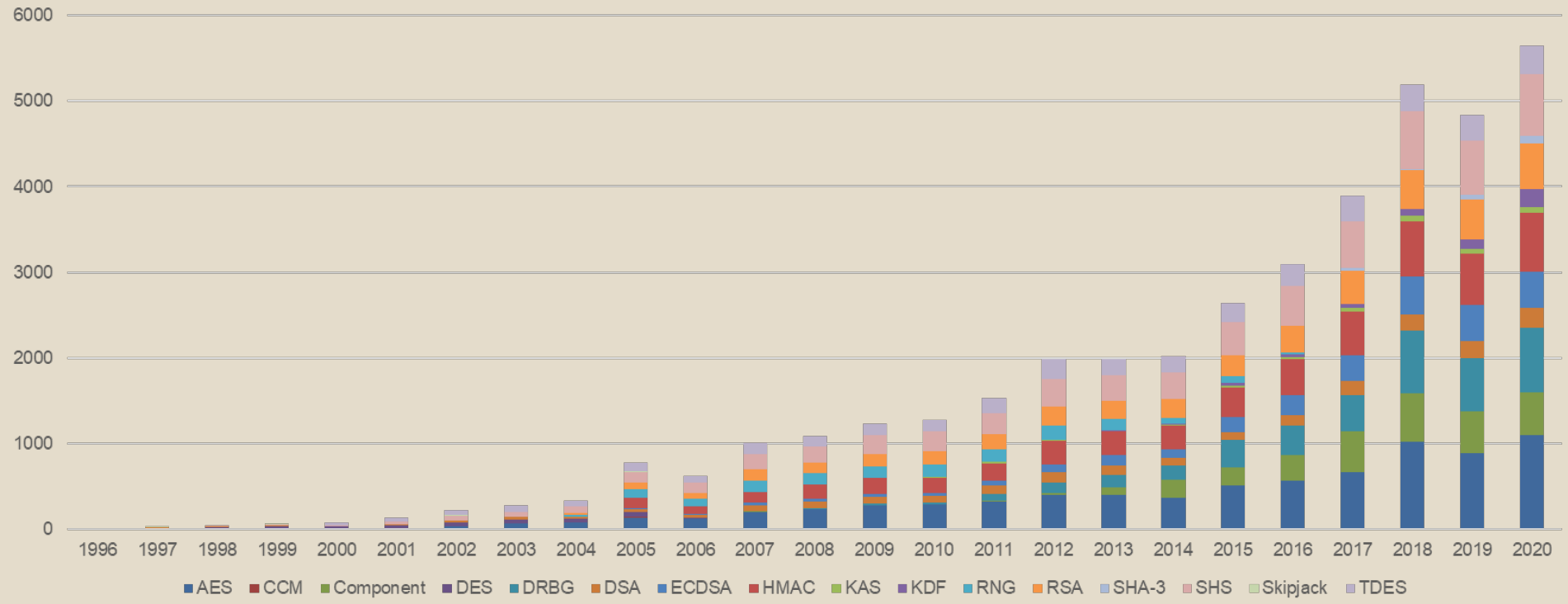
Topics

- FY 2020 Highlights
  - Number of Validations
  - CAVS Retirement on 30 June 2020
  - Extensions and Waivers
  - Testing of SP 800-56Ar3/-56Br2/-56Cr1,2
- FY 2021 Plans
  - Documentation and Guidance
  - Support for Prerequisites, Billing and ITAR
  - Better Testing and Integration
  - Staff updates

Algorithm Validations by Month for FY 2020



Algorithm Validations over 25 Years



CAVS Retirement on 30 June 2020

- Retirement date announced in October 2019
  - CAVS (semi-)retired on 30 June 2020
  - ACVTS preferred for algorithm testing
  - No billing for ACVP vector sets for remainder of FY 2020
- Extensions and Waivers for CAVS
  - ITAR using CAVS until 30 September 2020
  - In support of module validation reports, e.g., in coordination
  - General waiver until 30 September 2020

SP 800-56A Rev 3, 56B Rev 2 and 56C rev 2 on ACVTS Prod

- Testing for latest versions of key establishment schemes by 30 September
- SP 800-56A Rev 3: Key establishment using DLC, i.e., FFC and ECC
  - full key agreement scheme (KAS) testing, including KDF and optional KC
  - KAS-SSC only
- SP 800-56B Rev 2: Key establishment using IFC, i.e., RSA
  - full key agreement scheme (KAS) testing, including KDF and optional KC
  - KAS-SSC only
- SP 800-56C Rev 1, 2: KDFs for use in approved key establishment schemes
  - One-step KDF
  - Two-step KDF, including HKDF
  - Testing for above as part of KAS and standalone
- TLS v1.3 KDF testing on ACVTS Demo
  - maps to SP 800-133 Rev 2, SP 800-56C Rev 2 and SP 800-108

FY 2021 Plans and Priorities

- More user documentation
  - "How-tos" both text and video
- Updates to programmatic guidance
  - CAVP FAQ last updated in May 2016
- ITAR using ACVTS
  - Initially a partially manual process, using nfiles
  - Move to fully automated

FY 2021 Plans and Priorities (2)

- CSRC (csrc.nist.gov) updates
  - Updated validation listing format
  - Endpoint returning JSON for a validation
- Billing
  - 100 vector set and 500 vector set bundles
  - Unlimited annual subscription
- Prerequisites
  - Update and clarify
  - Move from registration to certify

FY 2021 Plans and Priorities (3)

- New testing
  - Large message SHA test
  - Research into tests with known (and better) coverage metrics
- Integration with Web Cryptik and Resolve
  - Automate matching and checking algorithm validations on certificates
- Staff updates
  - Tim Hall, acting STVM group manager, will remain as CAVP PM
  - Chris Celi to ESVTS and research topics
  - Ben Livelsberger taking on Tech Lead role

Questions

Tim Hall – tim.hall@nist.gov

Chris Celi – christopher.celi@nist.gov