Cryptographic Algorithm Validation Program (CAVP)

http://csrc.nist.gov/groups/STM/cavp/index.html

Sharon S. Keller, Director	skeller@nist.gov	301.975.2190
Timothy A. Hall	tim.hall@nist.gov	301.975.8077
Janet Jing	jjing@nist.gov	301.975.4293

Cryptographic Algorithm Validation Program (CAVP)

- **Uniform testing criteria across all vendors and implementations**
- **Validates implementations against NIST cryptography standards**
- **<u>All</u> cryptography used by US Federal Government to protect non-classified data goes through NIST CAVP validation**
- **A suite of automated tests for each cryptographic algorithm**
- **Implementations tested for correctness, completeness of functionality, proper handling of inputs, and stable behavior**

Cryptographic Algorithm Validation Program (CAVP)

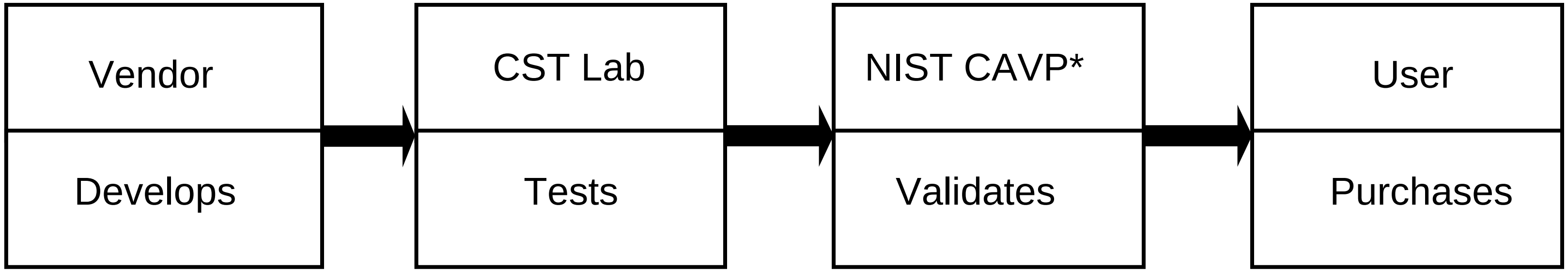
- **Joint program between the United States Federal Government and the Government of Canada**

- **Accredited private laboratories conduct the testing**
  - **NIST CAVP develops the automated tests and acts as final validation authority**

- **Works jointly with the NIST Cryptographic Module Validation Program (CMVP)**
  - **CAVP validation is a prerequisite for CMVP validation**

- **List of validated implementations posted publicly on CAVP website**
  - **http://csrc.nist.gov/groups/STM/cavp/validation.html**

Validation Process for Cryptographic Algorithm Implementations



Vendor

Develops

CST Lab

Tests

NIST CAVP*

Validates

User

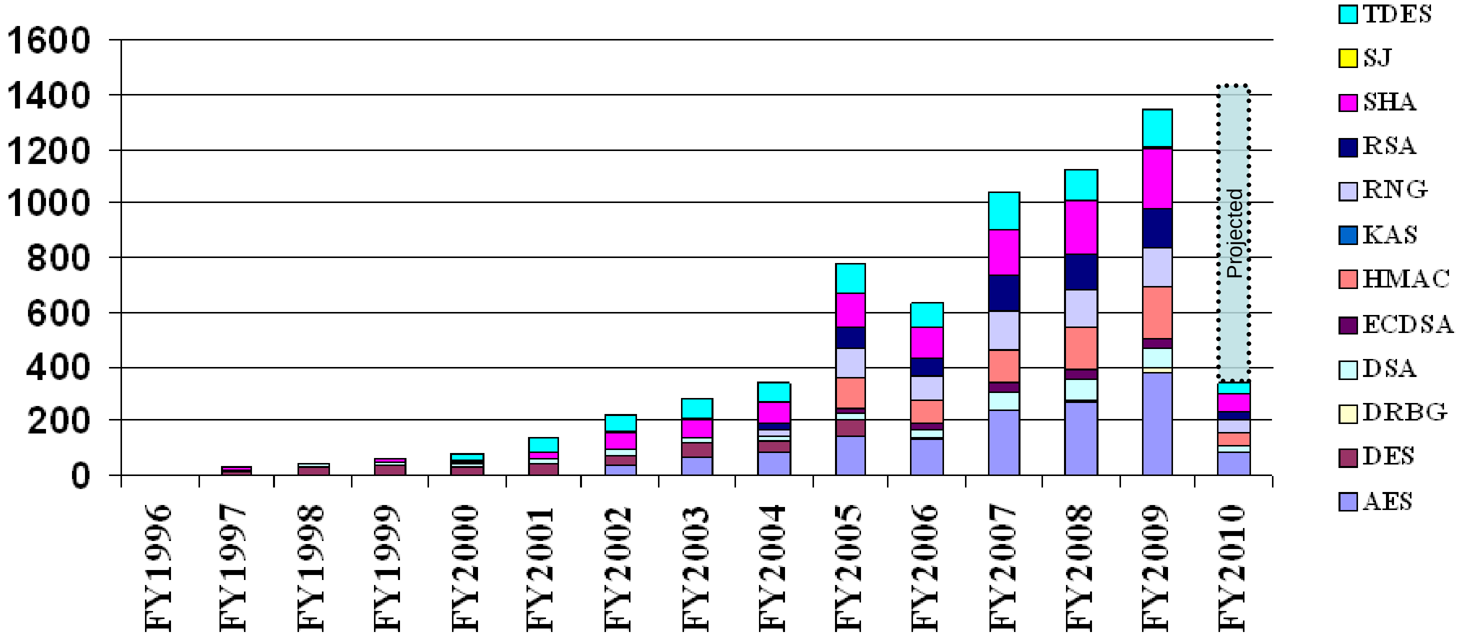
Purchases

186 CAVP validations from Maryland vendors since 1996

3 of the 9 US CST Labs reside in Maryland

*** NIST CMVP must also validate module prior to its use in US Federal Government**

CAVP Validations By FY



CAVP Validated Implementation Actual Numbers

Updated As Tuesday, December 29, 2009

FiscalYear	AES	DES	DSA	DRBG	ECDSA	HMAC	KAS	RNG	RSA	SHA	SJ	TDES	Total
FY1996	0	2	0	0	0	0	0	0	0	0	0	0	**2**
FY1997	0	11	6	0	0	0	0	0	0	7	2	0	**26**
FY1998	0	27	9	0	0	0	0	0	0	6	0	0	**42**
FY1999	0	30	14	0	0	0	0	0	0	12	1	0	**57**
FY2000	0	29	7	0	0	0	0	0	0	12	1	28	**77**
FY2001	0	41	15	0	0	0	0	0	0	28	0	51	**135**
FY2002	30	44	21	0	0	0	0	0	0	59	6	58	**218**
FY2003	66	49	24	0	0	0	0	0	0	63	3	73	**278**
FY2004	82	41	17	0	0	0	0	28	22	77	0	70	**337**
FY2005	145	54	31	0	14	115	0	108	80	122	2	102	**773**
FY2006	131	3	33	0	19	87	0	91	63	120	1	83	**631**
FY2007	240	0	63	0	35	127	0	137	130	171	1	136	**1040**
FY2008	269	0	77	4	41	158	0	137	129	191	0	122	**1128**
FY2009	374	0	71	23	33	193	3	142	143	224	1	138	**1345**
Total	**1337**	**331**	**388**	**27**	**142**	**680**	**3**	**643**	**567**	**1092**	**18**	**861**	**6089**