Enter Date: **Enter NVLAP Lab Code:**

NIST HANDBOOK 150-17 Annex D CHECKLIST

General Services Administration Precursor (GSAP) Testing

Instructions to the Assessor: This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-17, *Cryptographic and Security Testing*, for the General Services Administration Precursor test methods. It is used in conjunction with the NIST Handbook 150-17 Checklist, which covers the requirements in clauses 4 and 5 of the program handbook.

Place an “X” beside any of the following items that represent a nonconformity. Place a “C” beside each item on which you are commenting for other reasons. Record the item number and your nonconformity explanation and/or comments on the appropriate comment sheet(s). Write "OK" beside all other items you observed or verified as compliant at the laboratory.

Note: The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-17, Annex D, Section D.5.

D.5 Additional technical requirements for accreditation

D.5.2 Additional personnel requirements

___ D.5.2.1 The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel has basic knolwedge of cryptographic and security practice for information systems and that the laboratory is aware of the govering standards and publications, especially the ones listed in this handbook.

___ D.5.2.2 The laboratory’s personnel shall have experience, training, or familiarity in the areas of:

___ a) cryptography – symmetric versus asummetric algorithms and uses;

___ b) cryptography – encryption protocols and implementations;

___ c) key management techniques and concepts;

___ d) cryptographic self-test techniques;

___ e) the families of cryptographic algorithms;

___ f) FIPS-approved and NIST-recommended security functions (FIPS 140-2 or successors);

___ g) cryptography – Public Key Infrastructure (PKI);

___ h) access control security models;

___ i) smart cards;

___ j) smart card readers (contact and contactless);

___ k) Application Protocol Data Unit (APDU);

___ l) Basic Encoding Rules (BER);

___ m) biometric authentication techniques;

___ n) concepts of the operational PIV systems;

___ o) contact and contactless interface standards; and

___ p) Server-based Certificate Validation Protocol (SCVP).

D.5.3 Additional accomodation and environmental conditions

___ The laboratory shall have appropriate areas, including ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus**.**

D.5.5 Additional equipment requirements for 17GSAP testing

___ The laboratory shall also meet the following minimum hardware, software, and operating system requirements for any platform on which the *PIV Data Model Tester* (SP800-85B) and *Test Fixture Software* tools required for GSAP testing will run:

a) Hardware:

___ 1) at least 1 USB and 1 serial port available on the Windows XP test computer;

___ 2) Golden contact PIV Card Reader – Gemalto GemPC twin USB HW111459A[1];

___ 3) Breakout Box;

___ 4) 22 AWG Wire – category 5 or similar Ethernet; and

___ 5) tools needed for the breakout box:

- Drill;
- Screwdriver; and
- Glue.

b) Software:

___ 1) BouncyCastle crypto provider, version 1.32 (bcprov-jdk15-132.jar);

___ 2) BouncyCastle mail utilities, version 1.32 (bcmail-jdk15-132.jar);

___ 3) Crypto++ DLL version 5.2.3;

___ 4) *PIV Test Data Software* (which includes the *JPIV Test Data Generator* jar file and the *PIV Data Loader* executable);

___ 5) a *Gemplus GemPIV applet* v1.01 on Gemplus GemCombi Xpresso R4 E72K Smart Card;

___ 6) a *PIV EP v.108 Java Card Applet* on Oberthur ID-One Cosmo v5 64K Smart Card;

___ 7) card reader driver provided by the manufacturer;

___ 8) SP 800-85B Data Conformance Test Tool v6.2.0;

___ 9) Cardholder Facial Image Test Tool v1.0.1;

___ 10) SCVP Client Test Tool v2.0.0; and

___ 11) Data Populator Tool v2.3.0.

D.5.6 Additional measurement traceability

___ D.5.6.3 Laboratories shall use the test methods listed at the website http://fips201ep.cio.gov/contact.php under the “Test Procedures.”

Prior to testing the IUT, the laboratory shall create an inventory list with all the equipment received and tag all systems.

During the conformance testing, the laboratory shall use and complete the following documentation:

- Approval Procedure;
- Test Procedure; and
- Evaluation Report.

DATE: NVLAP LAB CODE:

NIST HANDBOOK 150-17 Annex D CHECKLIST
General Services Administration Precursor (GSAP) Testing

COMMENTS AND NONCONFORMITIES

Instructions to the Assessor: Use this sheet to document comments and nonconformities. For each, identify the appropriate item number from the checklist. Identify each comment with a "C" and each nonconformity with an "X." If additional space is needed, make copies of this page or use additional blank sheets.

Item No.	*C or X*	*Comments and/or Nonconformities*