V2.Z (in final clearance)

Criteria for Assessing FIPS 201 Compliance of PIV Applicant Registration & Card Issuance Services

the Zygma partnership LLC

Digitally signed by Richard G. WILSHER
DN: cn=Richard G. WILSHER, c=US,
o=the Zygma partnership LLC, ou=CEO
Reason: Approved for public release
Date: 2006.10.11 20:46:17 Z

Abstract

This document specifies **the full set** of "Criteria for Assessing FIPS 201 Compliance of PIV Applicant Registration and Card Issuance Services" as developed by the Federal Identity Credentialing Committee (FICC – see http://www.cio.gov/ficc/). The document should be used by Federal executive departments and agencies in determining their compliance with the requirements of HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" and NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors" for offering and performing such services. This document is intended to be used in conjunction with NIST FIPS 201, NIST SP 800-79 "Guidelines for the Certification and Accreditation of Personal Identity Verification Card Issuing Organizations" and NIST SP 800-37 "Guide for the Certification and Accreditation [Authorization] of Federal Information Systems." The latter two documents provide a high level approach to evaluating the reliability of an organization and the security status of an information system, respectively. NIST intends to publish a subset of these criteria – this document provides the full set of system-wide criteria originally developed by the FICC.

This document provides very specific criteria for assessing an organization's compliance to FIPS 201. It provides a two-way mapping between the criteria set out herein and the specific clauses within FIPS 201 which those criteria respond to (special versions of the applicable HSPD-12 and FIPS 201 texts are provided in Annex A).

Agencies should use these criteria to assure themselves and others that the requirements of FIPS 201 are properly understood, implemented, and utilized. The fourth column of the tables in Sections 4, 5 and 6 should be used by Agencies and service providers wishing to comply with FIPS 201 to reference evidence of their PIV Applicant Registration and Card Issuance Service implementations such that an impartial third party can use this as input to an independent assessment (or more formally, an audit) of the organization so as to determine whether or not the organization is in compliance with the FIPS 201 standard.

The FICC is able to provide points of reference for additional guidance in the application of these criteria.

Table of Contents

1. Introduction & Scope

This document is provided to assist Federal Executive Departments and Agencies (Agencies) in establishing, assessing, and demonstrating compliance with requirements for Personal Identity Verification enrollment & issuance systems as set out by HSPD-12 and subsequently expanded by NIST FIPS 201 and SP 800-79.

OMB has determined that in order to demonstrate compliance with the control objectives for Part 1 of FIPS 201, agencies may 'self assert' that their enrollment processes meet the requirements of FIPS 201. The criteria described in this document provide Agencies with a tool for developing consistent interpretations and applications of the FIPS 201 enrollment process and thereby fostering consistency among similar components of the Federal Government. These criteria are informative.

The criteria address the core technical functions of enrollment and issuance in the context of Personal Identity Verification systems – these core functions may be applicable to Federal entities and/or to External Service Providers (who may perform aspects of identity proofing, vetting and verification, and credential issuing on behalf of Agencies). In addition, the criteria address operational and management criteria inherent in enrollment and issuance of credentials.

Each of the criteria is mapped to FIPS 201 (and, more broadly, to HSPD-12): Agencies' compliance with these criteria will therefore provide them with a mapping back to the FIPS 201 standard, and therefore support their demonstration of compliance.

Certain criteria (or sub-clauses of them) are placarded with 'NOTICE's which indicate either that the clause is not acceptable under PIV-II or that the clause is not required under PIV-I but is mandatory under PIV-II. Agencies are encouraged to comply as fully and as soon as possible with PIV-II requirements since this will minimize any changes they are required to make during the transition from PIV-I to PIV-II. Agencies adopting the PIV-II compliant solutions can confidently expect not to conflict with any criteria herein during the PIV-I period.

This document consists of the following parts:

§1 - Introduction
Includes the scope, structure and contents of this document.

§2 - Glossary
Those terms which have a particular meaning within this document and the terms are not already defined in FIPS 201 or NIST SP 800-79.

§3 - Overview of criteria and their usage
An explanation of how to interpret the criteria, and how to apply them.

§4 - Management and Operational compliance – agencies
Criteria with which an Agency's management and operations should comply.

§5 - Functional compliance
Core Technical functions that either Agencies or External Service Providers should comply with, where they provide enrollment and issuance functions.

§6 - External Service Provider Management and Operational compliance
Compliance criteria for Personal Identity Verification enrollment and issuance Service Provider management and operations.

Appendix A - HSPD-12 and FIPS 201 Requirements
Essential parts of these documents which have been used to derive the criteria in the present document, with specific references inserted to provide a greater level of discrete, reference-able, granularity.

Appendix B – References
A set of documents which provide essential guidance to Agencies seeking compliance with FIPS 201.

2. Glossary

This Section defines the terms which have a particular meaning within this document and where such **Terms** are not already defined in either FIPS 201 or NIST SP 800-79.

Term	Definition
Affiliate	a person who has an established working relationship and status with an **Agency** (e.g. visiting academic/researcher, exchange visitor, …) and has been Sponsored by an Agency for the issuance to them of a credential.
Contractor	a non-governmental enterprise to which an **Agency** contracts for services and whose staff may be present at **Agency** establishments and whose employees have been **Sponsored** by an **Agency** for the issuance to them of a credential.
Contractor's Employee	a person employed by a **Contractor**.
Federal Employee	a person employed directly by an **Agency**.
Applicant	Note – although the NIST SP 800-79 definition applies, where, in the subsequent criteria, it is the intention to refer explicitly to any such parties the terms **Federal Employee, Contractors' Employee,** or **Affiliate** will be used).
External Service Provider	an entity beyond the direct management responsibility of the **Agency**, possibly within another **Agency** or an non-Federal commercial enterprise, which fulfils some of the functional aspects of the **Registration** and/or **Issuance** processes. Frequently abbreviated to '**ESP**'.
Identity vetting	the process of establishing beyond reasonable doubt that the person who presents themselves for the purposes of being given possession of a credential is the person to whom the identity vouched-for by the credential is actually the individual to whom it relates. ***CAVEAT*** *– this definition is* ***not*** *intended to be equivalent to that given in NIST SP 800-79 for 'Identity verification' – the SP 800-79 definition should be more accurately defined as 'Identity authentication' (ref. FIPS 201 §1 "Introduction" on this subject).*

Enrollment	the combination of **Identity proofing, Identity vetting** and **Registration**.
PIV participants	Any person or entity which participates in a PIV enrolment and issuance system (refer to SP 800-79, Appendix B, for definitions of roles which participants may take).
Policy	used to include by inference all derived processes and procedures, etc.
Proofed Applicant	an **Applicant** who's identity has been established by being subjected to an **Identity proofing** process.

Terms such as 'document', 'write', 'record' and other similar terms apply equally to paper, electronic, optical storage and any other media or representation unless specifically qualified.

3. Overview of criteria and their usage

The criteria set out in this document are the basis against which Agencies shall demonstrate their compliance with FIPS 201 and HSPD-12. The criteria are structured in three classes.

3.1. Classes of criteria

Criteria are in three classes:

- Those which deal with the Agency's overall PIV system management and operations (Section 4, Management and Operational compliance – agencies);
- Those which deal with the technical PIV system enrolment and issuance functions (Section 0, Functional compliance);
- Those which deal with how External Service Providers must exercise their own management and operations responsibilities when providing PIV system services to Agencies (Section 6, Management and Operational compliance – external service providers).

3.2. Groups of criteria

Within each class of criteria there are groups of criteria which have a common focus, e.g. establishing policy, or identity proofing, identity vetting, etc. These are grouped simply as an aid to Agencies trying to establish their compliance as much as to assessors who might be assessing or auditing that compliance. Notwithstanding that general intention, users will find instances of overlap between some of these groups simply because of the complex interactions between components of PIV systems.

3.3. Specification of criteria

With each group one or more criteria are stated, according to the following form:

3.3.1. Criteria tags

A 'tag', used as a convenient, if somewhat cryptic, unique reference to each of the criteria– column 1 in the criteria tables which follow. This facilitates reference when determining compliance. Each has the prefix "201C"(FIPS 201 Compliance). A three-letter acronym is then used to refer to the general name applied to the group within which the criteria are declared: a discrete numeric value is then assigned

3.3.2. *Criteria expressions*

Each of the criteria is stated, with a brief title and then a normative statement defining an action or condition which the subject (typically the Agency) should comply with – column 2 in the criteria tables which follow. Each of the criteria is intended to be 'atomic' in its expression, i.e. any discrete clause requiring compliance is capable of being discretely referenced, either by the tag alone or by a subscripted label, (a), (b), etc. Should users of the present document find instances where this is not achieved they are encouraged to submit a comment to Fixer@Zygma.biz.

3.3.3. *Criteria source references*

A criteria source reference is contained in column 3 in the tables which follow. There are three levels of compliance references:

- To HSPD-12 – provided as a form of completeness, but owing to the very abstract level at which the Directive's requirements are expressed, often not able to be usefully assigned to a specific clause of the Directive;
- To FIPS 201 – by far the most useful compliance mapping, since that standard determines much of the detail which HSPD-12 required;
- To SP 800-79 – giving guidance in the implementation of information systems which should comply with FIPS 201;
- To GSA's Federal Identity Management Handbook – a number of valuable best practices are cited in this document and have been considered worthy of inclusion as explicit requirements for Agencies wishing to ensure they meet the requirements of HSPD-12 / FIPS 201.

With the exception of references to the Handbook and SP 800-79, the source references are hyper-linked to Appendix A which includes the relevant clauses from HSPD-12 and FIPS 201 such that users can view the original text from which the criteria have been derived. Further, for references to FIPS 201, a reverse link is provided back to each criterion which refers to that clause.

In addition, some criteria have been 'Introduced' as representing established or accepted good practices in the information security management field.

3.4. Compliance with criteria

A fourth column is provided in the criteria tables. This is so that Agencies may indicate, alongside each of the criteria, the evidence they have to demonstrate their compliance. This evidence should be either a reference, as specific as possible, to their relevant documented policy, procedure, etc., or a quotation of the compliant text itself. When completed, these tables can be the basis of a self-declaration or formal certification of the Agency's PIV system. Should an Agency consider any criteria not be applicable then their justification should be placed in this column.

Finally, an Assessor may, during the course of an assessment or audit of an Agency's PIV system, also use this column to add their own comments as to the sufficiency of evidence offered.

4. Management and Operational compliance – agencies

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.1. Policy The **Agency** must show that it applies relevant policies and procedures and that it retains appropriate records of identity proofing activities and evidence.			
201C_POL#010	**Scope of PIV System**: The **Agency** shall set out the scope and purpose of its PIV System and in particular demonstrate that it has applied the provisions of NIST SP 800-59 to establish that the System is not, nor supports, nor is related to a “national security system” as defined by 44 U.S.C. 3542(b)(2).	**§6.1**	
201C_POL#020	**Credential issuing policy**: The **Agency** shall: a) document its policy relating to the issuing of identity credentials to **Applicants**. This policy shall ensure that the criteria set out in this Guidance are complied with or that the **Agency** has in place alternative mechanisms which demonstrably achieve at least the same degree of rigor for all areas addressed in this Guidance; b) maintain an auditable record of the mapping between its internal policy and each discrete clause of these criteria.	*(3)(d)*, **§2.2.1(a)**	
201C20OL#030	**Identify key roles**: The **Agency** shall set out in its policy those roles which have direct oversight responsibilities and accountability for the identity vetting and credential issuing processes.	*3(b)*, Hbk:2.2.11	
201C_POL#040	**Separation of roles**: The **Agency** shall specify key roles required for the correct operation of its PIV system and	*3(b)*, **§2.1.2(i)**,	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	implement policy such that no single individual can be assigned to more than one of the following roles: System Owner/Authority, Senior Agency Official for Privacy (in accordance with *OMB Memorandum M-05-08 "Designation of Senior Agency Officials for Privacy"*); Sponsor/Requestor of an application; Issuer.	**§2.2.1(e)**, **§2.4.3(a)**	
201C_POL#050	**Rights and Privileges**: The **Agency** shall limit access to all parts of the PIV system, including personal information in identifiable form, such that: a) only those persons with a legitimate need are authorized to access such information; b) a strict 'need to know' access policy is used to limit the extent of access, even when authorized; c) areas where dual control is required shall be identified and appropriate controls applied.	*3(b)(ii)*, **§2.4.3(f)**	
201C_POL#060	**Published Privacy Policy**: The **Agency** shall document, publish and maintain in a form and medium accessible to all **Applicants** its policy for performing the vetting of **Applicants**' identities in order that they may be issued with an identity credential. This policy shall define the Agency's requirements for and practice in handling **Applicants**' personal information in identifiable form, in terms of: a) which personal identity information and documentary evidence the employee is required to make available; b) which information shall be recorded and retained by the **Agency**, including detailing for how long it shall be retained;	*(3)(a)*, **§2.2.1(a)**, **§2.4.3(c)**, **§2.4.3(c)(i)**, **§2.4.3(c)(i,iii)**, **§5.3.2.4.2(e)**, **§2.4.3(c)(ii,iii, v)**,	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	c) uses to which such information shall be put and with whom it shall be shared (and for which purposes), including information held in **Agency** records and included within the credential to be issued; d) the privacy protection measures which are applied to information in all media and usage; e) the procedural steps and ways in which the **Applicant** must participate in order that the **Agency** can fulfill its obligations for the secure vetting of employees' identities (such steps being some but not all of those defined in the Agency's full PIV System Policy document. The **Agency** is not required to reveal parts of their process not relevant to and not requiring the direct participation of **Applicants**.)	§2.4.3(c)(iv,vi)	
201C_POL#070	**Privacy Impact Assessment**: The **Agency** shall determine its Privacy Policy and other affected operational policy only after conducting a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form.	*(3)(a)*, §2.4.3(b)	

201C_POL#080	**PIA Scope**: The **Agency** shall conduct its PIA such that the assessment is cognizant of and consistent with controls and obligations specified in:
	i) the E-Government Act of 2002;
	ii) Office of Management and Budget (OMB) Memorandum M-03-22;
	iii) the Privacy Act of 1974's fair information practices;
	iv) NIST SP 800-53, Recommended Security Controls for Federal Information Systems;
		(3)(a),
		§2.4.3(b),
		§2.4.3(d),
		§2.4.1	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	v) all other applicable Federal privacy laws and policies; vi) privacy issues identified by appropriate **Agency** personnel responsible for privacy issues (e.g., Chief Information Officer); plus vii) any other applicable Agency-specific controls and obligations, which shall be cited.		
201C_POL#090	**No negative impact**: The **Agency** shall ensure that there is no negative impact upon its privacy controls and obligations arising from: a) technologies used within its systems and communications infrastructure; b) identity credentials which it issues.	**§2.4.3(j)**,	
201C_POL#100	**Policy Violations**: The **Agency** shall establish rules for handling breaches and violations of its policies, specifically for but not limited to privacy breaches and violations, which: a) take into consideration department or agency officials' viewpoints; b) define measures which may be taken against offending **PIV participants** where blame is apportioned; c) are documented, published and maintained in a form and medium accessible to all **PIV participants**.	*3(b)*, **§2.4.3(g)**	
201C_POL#110	**Credential usage**: The **Agency** shall document, publish and maintain in a form and medium accessible to all **Applicants** a description of the uses to which the credential may be put in gaining access to **Agency** facilities, services and systems.	*3(b)*, **§2.4.3(c)(v,vi)**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
201C_POL#120	**Use of PIV System**: The **Agency** shall ensure that its policy prohibits the use of its PIV system and credentials issued under its Authority for any purpose which conflicts with the HSPD-12 control objectives, namely "*to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy*".	*(3)(d)*, **§2.4.2**, **§2,4,3(i)**	
201C_POL#130	**Overseas Applicants**: If the Agency is responsible for the vetting of **Applicants** which are foreign nationals working for the Federal government overseas at a location(s) which does not fall under the command of a U.S. area military commander it shall, for each specific country/location in which it performs this function: a) indicate in its policy those parts of its registration and approval method which apply in the country/location concerned; b) include within the policy a requirement to seek and maintain the approval the U.S. Department of State's Bureau of Diplomatic Security for the defined registration and approval method; c) retain a record of such approval which shows the reference of the approval and the period of its validity.	*(3)(a)*, **§2.2.3**	
201C_POL#140	**Special-risk security provision:** If the **Agency** has determined a need to issue special-risk security credentials it shall define and justify within its policy and derived processes and procedures (or if security requirements dictate, another document(s) referenced from the policy): a) the conditions under and extent to which any compliance	*(3)(a)*, **Preamble §6.2**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	security provisions are granted; b) the specific guidance criteria to which compliance security provisions are granted and the extent to which it applies. The **Agency** is not required to disclose the risk/threat analysis which leads it to determine the need to establish special-risk security provisions. Furthermore, where security considerations may be considered threatened by disclosure of justifications for such security provisions these also need not be cited.		
201C_POL#150	**Enhanced PIV system**: Although **Agencies** may enhance their identity vetting and credential issuance processes beyond the requirements of FIPS 201 no enhancement shall compromise adherence to the criteria set out in this Guidance nor to FIPS 201.	**§5.3.1.4**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.2. Approved PIV Process The Agency must have its identity vetting and credential issuance processes audited and approved for operation.			
201C_APP#010	**PIV-I Approval**: Under PIV-I, the **Agency** shall issue a self-declaration of conformity (to these criteria) that shall be underwritten by the Head of the Agency and reviewed at least annually. (Refer to NIST SP 800-79)	*(3)(d)*, **§2.2.2**, **§2.3.1(a)**, **§2.3.1(d)** **§5.3.1.1** Hbk:2.2.11	
201C_APP#020	**PIV-II Approval**: Under PIV-II, the **Agency** shall have its PIV system independently audited and certified, as defined in NIST SP 800-79.	*(3)(d)*, **§2.2.2**, **§2.3.1(a)**, **§2.3.1(d)** **§5.3.1.1** Hbk:2.2.11	
201C_APP#030	**Assignment to roles**: **Agencies** shall maintain a register which identifies those individuals who fulfill those policy roles which have direct oversight responsibilities and accountability for the identity vetting and credential issuing processes.	*(3)(d)*, **§2.2.2**, **§2.3.1(a)**, Hbk:2.2.11	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding

4.3. Identity Proofing

The Agency shall show that it applies relevant identity proofing policies, processes and procedures.

201C_PRF#010	**Request to issue credential**: The **Agency** shall only commence the processing of an Applicant when an application to issue them with a credential has been received from a recognized authority, with a valid reason for the issuance[1].	*(3)(a)*, **§5.3.2.2.1**, **§5.3.2.2.2**, Hbk:2.2.5.4(a)	
201C_PRF#020	**Required Information**: The **Agency** shall collect, as a minimum, the following personal information concerning each **Applicant**: a) First, any Middle, and LAST name(s) of the **Applicant**; b) where applicable, the **Applicant**’s maiden name or any prior names or aliases; c) gender; d) Date and place of birth; e) Social Security Number and date of issuance; f) driver’s license number and State and dates of issuance and expiry; g) residential address; (Form SF-85 is the recommended basis for collating this textual information.)	*(3)(a)*, **§2.2.1(b)**, Hbk:2.2.5.4(b) re item (f): §4.4(b), §4.4.1.4,§2.2.3 re item (g): §4.1.5.1(d), §4.4(a), ’(c), §4.4.1.1]	

[1] First-time and re-issuance require the full verification process to be applied: renewal, wherein a credential is replaced prior to its natural expiry, permits some procedural steps to be omitted where the applicant is still in good standing with the **Agency** and previous verification records remain accurate and valid.

Criteria tag	**Criteria**	***HSPD-12*** **/ FIPS 201 /** ***SP800-79*** **/ Handbook ref.**	**Compliance source / Assessment finding**
	h) an electronic facial image obtained in a manner which conforms to NIST SP 800-76; i) a full set of ten biometric fingerprints obtained in a manner which conforms to NIST SP 800-76; In addition, where the **Applicant** is a **Contractor's Employee**: j) written confirmation of employment by the **Contractor**, stating: i) original date of hiring; ii) Contractor's employee-specific reference number; In addition, where the **Applicant** is a foreign-national working for the Federal government overseas at a location which does not fall under the command of a U.S. area military commander: k) approval for employment determined through a registration and approval method which has itself been approved by the U.S. Department of State's Bureau of Diplomatic Security, for the specific country/location in question. Those documents on which identity proofing may be based are set out in §0 Functional Compliance, sub-section Proofing Practice.	*(3)(a)*, **§2.2.3**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
201C_PRF#030	**Initial proofing of id:** The **Agency** shall, as policy: a) perform proofing of sufficient basic information pertaining to the **Applicant** to provide reliable input to a further investigation; b) if proofing fails, challenge the **Applicant** as to the accuracy of the supplied information; c) in the event that changes (if any) do not render the proofing positive, deny the request for issuance of a credential and find the application to have failed.[2]	*(3)(a)*, **§2.2.1(b)**, *79:§5.2*	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.4. Identity Vetting The Agency shall show that it applies appropriate identity vetting policies, processes and procedures.			
201C_VET#010	**Initiating investigation:** The **Agency** shall: a) establish whether the **Applicant** has been previously **Sponsored** and if so reject the application if the **Agency**'s conditions for re-application have not been	**§2.2.1(b)** (item b), otherwise Introduced	

[2] It is not within the scope of this guidance to determine what actions an Agency should take in the event of failure of the identity verification measures it applies, but Agencies must remain alert to the possible need to take immediate action to apprehend and possibly alert law enforcement authorities as to the circumstances pertaining with regard to the Applicant. Whether such action is required will depend upon the nature of the cause of the failure, and Agencies must remain alert also to the need to ensure no breach of civil liberties where restraining or legal action may not be justified (e.g. past misdemeanours for which the Applicant has served any sentence/fines applied need not require action).

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	met; b) initiate a National Agency Check with Inquiries (NACI) or other appropriate check; c) based on the results of an FBI national criminal fingerprint database check, if the check yields a negative result, deny the request for issuance of a credential and find the application to have failed;[2] d) otherwise, find the initial application to have been successful and initiate the issuance of a credential.		
201C_VET#020	**Notification of application result**: The **Agency** shall provide the **Applicant's Sponsor** with written confirmation of the outcome of the application, stating reasons where it has been denied.	*79:§5.2*	
201C_VET#030	**Completing the investigation:** The **Agency** shall, through its policy and derived processes and procedures, and in parallel with proceeding with the issuance of an identity credential, initiate a background investigation based upon the results of a positive initial vetting. That investigation shall be one of the following: a) a National Agency Check with Inquiries (NACI); b) an investigation approved by the Office of Personnel Management (OPM) required for Federal employment; c) a National Security Community investigation required for Federal employment. Where the **Agency** has on file and can verify the successful results of one of the above background investigations	*(3)(a)*, **§2.1.2(b)**, **§2.1.2(e)**, **§2.2.1(b)**, **§2.3.1(b)**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	concerning the Applicant then those results may be used.		
201C_VET#040	**Negative investigation outcome:** If this investigation (see Completing the investigation) fails the **Agency** shall, in fulfillment of its policy, revoke any credential which has been already issued.	*(3)(a)*, **§2.1.2(b)**[3], **§2.2.1(b)**, **§5.3.1.2**	
201C_VET#050	**Timed-out investigation:** If the **Agency** cannot verify successful completion and adjudication of this investigation (see Completing the investigation) within six months of PIV card issuance it shall, in fulfillment of its policy, revoke any credential which has been already issued. ***[NOTICE – mandatory for PIV-II]***	**§5.3.1.2**	
201C_VET#060	**Vetting on renewal**: When undertaking vetting for renewal purposes the **Agency** shall state which of the above vetting steps may be omitted, and under what qualifying conditions (e.g. status of individual, OPM Guidance with regard to NACI checks, nature of reason for issuance, …)	**§5.3.2.1.1**	
201C_VET#070	**Monitor vetting responses**: The Agency shall monitor OPM notifications concerning vetting outcomes of any Applicants to whom a credential remains issued and shall act on any negative findings and revoke the credential when required.	Introduced	
201C_VET#080	**Appeal of denial/revocation**: The **Agency** shall provide and notify **Sponsors**, **Applicants** and **Holders** of an appeals process which shall be available under the following circumstances: a) rejection of an application for a credential; b) revocation of a credential **not** arising from one of: i) change in the **Holder**'s employment or other relationship with the **Agency**;	*(3)(a)*, **§2.4.3(e)**	

[3] Note - In FIPS 201, §2.2.1(b) is contradicted by both its footnote and §5.3.1.2 – this criterion follows the footnote and §5.3.1.2.»

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	ii) termination of the **Holder**'s employment or other relationship with the **Agency**; iii) an instruction from the Head of the Agency; iv) the **Holder**'s request for revocation; v) a determination that the claimed identity is fraudulent; vi) the natural expiry of the credential where no application for renewal has been received vii) the death of the **Holder**.		
201C_VET#090	**Exception plans**: The **Agency** shall have in place plans to handle exceptions which may occur during identity proofing & vetting, stating the circumstances under which they may be invoked (e.g. recent change of address not yet stabilized within formal records, inability to provide required documents, physical loss or disfiguring which prevents the collection of biometric information).	Introduced	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.5. Credential Issuance and Delivery The **Agency** must ensure that issued credentials are unique and are delivered securely to the intended **Proofed Applicant**.			
201C_CID#010	**Authorized Issuance**: The **Agency** shall ensure that a designated official has authorized the issuance of a credential once the Applicant's identity has been proven, and shall only issue the credential once authorization has been received. This designated authorizing official must not be the same individual that requested issuance at the beginning of the process.	*(3)(a)*, **§2.1.2(a)(ii)**	
201C_CID#020	**Unique PIV system identity**: Prior to issuing a credential the **Agency** shall: a) check for any duplication of personal information with other verified identities; b) ensure that an identity that is unique within its PIV system name-space is created and linked to the verified identity.	*(3)(a)*, **§2.1.2(j)**	
201C_CID#030	**Compliant identity credential**: The **Agency** shall ensure that all identity credentials issued on its behalf (either by the **Agency** itself or by its appointed **ESP**) are provided by a manufacturer whose products have been shown to be fully FIPS 201-compliant.	*3(b)*, **§2.1.2(j)**, **§2.4.3(j)**	
201C_CID#040	**Compliant credential personalization**: The **Agency** shall ensure that systems used to personalize identity credentials have been and remain proven to be fully compliant with all FIPS 201 PIV II requirements. ***[NOTICE – mandatory for PIV-II]***	**§2.1.2(j)**	
201C_CID#050	**Verified credential delivery**: The **Agency** shall ensure that	*3(b)*,	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	once a credential has been issued it is delivered securely by its physical hand-over to the **Applicant** only after a successful 1:1 biometric match of the **Applicant** against the biometric included in the credential (required if renewal) or in the PIV enrollment record, and the receipt signature of the **Applicant** received; ***[NOTICE – mandatory for PIV-II]***.	**§2.1.2(f)**, **§5.3.1.3**, **§5.3.2.1.2**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.6. Credential life-cycle management The **Agency** must the validity of all credentials which it issues, ensuring that expired or revoked credentials are notified as such and are put beyond use..			
201C_LCM#010	**Credential validity limit**: The **Agency** shall state within each credential it issues the expiration date/time at which the validity of the credential shall 'naturally' expire, and retain independent record of such details.	*3(b)*,	
201C_LCM#020	**Credential status management**: The **Agency** shall maintain and make publicly available[4] information as to the status of each credential which it issues.	*3(b)*,	
201C_LCM#030	**Credential renewal**: The **Agency** shall, within the six week period prior to a credential's natural expiry, accept a request for its renewal and only issue the new credential to the holder after authenticating them against biometric data held on the expiring credential..	**§5.3.2.1.2**	
201C_LCM#040	**Credential information update**: The **Agency** shall provide the means by which and state the conditions under which Applicants/Credential Holders may correct errors in their personal information or request updates where there are changes which do not require the re-issue of or re-application for a credential.	*79:§5.2*	
201C_LCM#050	**Credential expiration**: On the passing of the validity date/time, or on the renewal of the credential (see **Credential renewal**) the **Agency** shall determine the credential to have been revoked .	*3(b)*, **§2.1.2(h)**	
201C_LCM#060	**Credential revocation**: The **Agency** shall provide a means by	*3(b)*, **§2.1.2(h)**,	

[4] Agencies may, with reasonable justification, interpret 'Publicly available' as referring to a community of interest, rather than as meaning to the public at large.

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	which revocation requests may be received, processed and acted upon after they have been validated. Credentials shall be suspended until validation of the revocation request has been accomplished.	**§5.3.2.0.2**, **§5.3.2.4.1**, **§5.3.2.4.2(b)**	
201C_LCM#070	**Revocation validation**: Other than upon the natural expiration of a credential (and its possible renewal), the **Agency** shall only accept a revocation request if it comes from one of the following with an acceptable reason: a) the Holder; b) the Head of Department or Agency; c) the authorized **Agency** official responsible for the management of identity vetting (e.g. should a NACI with written investigation fail); d) any lawful entity with authority so to direct;	*3(b)*, **§2.1.2(h)**, **§5.3.2.0.2**, **§5.3.2.4.1**, **§5.3.2.4.2(b)**	
201C_LCM#080	**Interim Suspension**: On receipt of a revocation request the Agency shall first suspend the credential while it validates the source of the revocation request. If the validation fails the suspension on a credential shall be removed.		
201C_LCM#090	**Revocation reason**: The **Agency** shall accept a revocation request arising from any of the following circumstances: a) an **Employee** separates (voluntarily or involuntarily) from Federal service; b) an **Employee** has revised needs for access to Federal buildings or systems changes. c) a **Contractor** employee separates (voluntarily or involuntarily) from a Federal **Contractor**; d) a Federal **Contractor** has revised needs for the **Contractor**'s employees to access Federal buildings	**§5.3.2.4.1**, **§5.3.2.4.2(b)**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	or systems changes; e) a credential holder is determined to have a fraudulent identity; f) a credential holder fails a NACI assessment; g) the death of a credential holder; h) the compromise of a credential; i) the loss or theft of, or damage to, a credential; j) the return of a 'lost' credential not already reported as lost.		
201C_LCM#100	**Credential destruction**: The **Agency** shall, following revocation, collect and destroy all expired credentials, and retain a record of their destruction. In the case that a credential has been lost that fact shall be recorded. Procedures shall be in place to ensure the permanent destruction or invalidation of the use of the card.	§5.3.2.1.2, §5.3.2.4.1, §5.3.2.4.2(a)	
201C_LCM#110	**Revocation notification**: The **Agency** shall, within a period of 18 hrs under normal operations, make public the revocation of credential.	§5.3.2.2.4, §5.3.2.4.2(b), (c), (d)	
201C_LCM#120	**Emergency revocation**: The **Agency** shall define parameters to determine whether a revocation should be treated as an emergency and shall have in place procedures to issue emergency publication	§5.3.2.2.4	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
4.7. Record & Archive Keeping The **Agency** must retain appropriate records of identity proofing activities and evidence.			
201C_RAK#010	**Required records**: The **Agency** shall, taking account of all applicable legislative and policy obligations, record the facts of the identity enrollment and issuance processes. As a minimum, records of the applicable processes must include: a) the **Sponsor**'s/**Requestor**'s identity and authority; b) all textual information captured for the purposes of identity proofing and vetting; c) type, issuing authority and reference number(s) of both primary and secondary documents checked in the identity vetting proces**s**, with electronic (scanned) copy of the documents in question; d) a facial photograph of the **Applicant**; e) a set of ten fingerprints belonging to the **Applicant**; f) record of the applied investigation results (including any written enquiries made); g) date and time of vetting outcome, issued by a trusted time-source; h) the hand-written signature of the **Applicant** at all required stages of the enrollment and issuance process; i) the identity of the **Registrar**; j) identity of the **ESP** providing any parts of the enrollment and issuance process or the location at which the (in-house)	*(3)(a)*, *3(b)*	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	vetting was performed; k) the identity and authority of the Authorizer for credential issuance; l) the PIV system identity assigned to the **Proofed applicant**; m) the index number of the issued identity credential. Other information required by the Agency's policies may also be retained.		
201C_RAK#020	**Security-event audit**: The **Agency** shall maintain a log of all security-relevant events concerning the operation of the service (especially the collection, use, distribution and storage of personal information in identifiable form), together with a precise record of the time at which the event occurred (time-stamped by reference to a trusted time-source, e.g. NIST, DoD, …) and such records must be retained with appropriate protection, accounting for service definition, risk management requirements and applicable legislation.	*3(b)*, **§2.4.3(h)**	
201C_RAK#030	**Record Retention**: The **Agency** shall retain securely its audit data and the record of the vetting/revocation process for at least the duration of the credential, plus whatever further period its particular requirements may dictate in accordance with National Archives and Records Administration (NARA) requirements (refer to Federal PKI Common Policy). If the documents are maintained as hard copy, they should be stored in a secure facility. If the documents are maintained electronically, they should be stored in a secure database.	*3(b)*, **§2.4.3(h)**, Hbk:2.2.5.5	
201C_RAK#040	**Record Destruction**: The **Agency** shall have in place procedures to dispose of sensitive information (particularly **Applicant** information in identifiable form - IIF) in accordance	**§5.3.2.4.2(e)**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	with its stated privacy and data retention policies (cf. *Published Privacy Policy*).		
201C_RAK#050	**Information protection**: The **Agency** shall define its policy and derived encryption algorithms and cryptographic key types and sizes used for the protection of personal identifiable and other system-critical information when in storage.	*79:§6.1/1.1*	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding

4.8. Technical compliance & management

An **Agency** may operate 'in-house' all or some of the required **identity proofing, Identity vetting**, **enrollment**, **credential issuance** and **Identity vetting** functions or it may choose to outsource the performance of some or all functions to **External Service Providers** (**ESP**s). In either case the **Agency** must show compliance with all the preceding criteria in order to adequately manage the outsourced services and additionally fulfill the following criteria in the management of their **ESP**s.

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
201C_TCM#010	**Externally provided services**: For each part of its overall PIV enrollment and issuance system, if any, which is fulfilled by an **ESP** the **Agency** shall state: a) which are, or the boundaries of, the part(s) of the system fulfilled by the **ESP** in question; b) the registered business name and any trading name of the **ESP** in question; c) the specific name or reference of the service(s) of the **ESP**	*(3)(a)*, *3(b)* **§2.3.1(d)**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	which is/are used; d) how the **Agency** applies ongoing oversight of the **ESP** so as to ensure that the **Agency**'s policies are applied and enforced on its behalf;		
201C_TCM#020	**Approved external services**: For each part of its overall PIV enrollment and issuance system, if any, which is fulfilled by an **ESP** the **Agency** shall either: a) provide the reference of the individual PIV system approval granted to the **ESP** for the function fulfilled, OR b) demonstrate itself the **ESP**'s compliance with the further criteria in §6 (External Service Provider Management and Operational compliance)of this document.	*(3)(a)*, *3(b)* **§2.3.1(d)**	
201C_TCM#030	**External service oversight**: For each part of its overall PIV enrollment and issuance system, if any, which is fulfilled by an individually approved **ESP** the **Agency** shall have a documented procedure for ensuring that each **ESP** retains its approval for the whole time over which they fulfill a part of the **Agency**'s PIV system functionality.	*(3)(a)*, *3(b)* **§2.3.1(d)**	
201C_TCM#040	**In-house functional compliance**: For each part of its overall PIV enrollment and issuance system, if any, which the **Agency** fulfils itself it shall demonstrate it's compliance with the further criteria in §0 (Functional compliance) of this document.	*(3)(a)*, *3(b)*	

5. Functional compliance

The criteria in this section relate to functional aspects of the Agency's PIV system. These functions may be provided by the Agency itself or outsourced to an ESP (see §4 above). In these criteria phrases such as 'The **Agency** shall … " are to be interpreted as meaning "The **Agency**, or a contracted **ESP** on behalf of the **Agency**, shall …", as applicable to the operational circumstances.

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
5.1. Proofing Practice The **Agency** shall show that it applies relevant identity proofing policies and procedures.			
201C_PRF#010	**Primary proofing document:** The **Agency** shall require the **Applicant** to submit one of the following documents as primary proof of id. The primary document must: a) be Federal or State government issued; a. be the original document or a certified copy of the original; b) be unexpired; and c) bear a photographic record of the applicant. *Note – The following listed document references are taken from OMB 1115-1036 Form I-9 which was prepared for the purposes*	*(3)(a)*, *3(b)* **§2.1.2(c)**, **§2.2.1(d)(i,ii,iii)**[5]	

[5] Prior identity verification on the basis of Form I-9 alone is not acceptable – FIPS 201 requirements are more stringent than OMB 1115-0136: FIPS 201 requires *TWO* documents of which one *MUST* be a photo id (I-9 requires only *one* document from List A (photo id) **or** *two* from List B plus *one* from List C, hence it may be possible to satisfy OMB 1115-0136 without presenting picture id).

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	of establishing eligibility for employment. Although these criteria refer to the same documents their use in the context of a PIV System is purely to establish identity and hence the eligibility of certain documents differs in this context List of acceptable documents (references to Form I-9 (Rev. 11-21-91) are given for comparative purposes, in italics): 1) United States Passport (*A.1*); 2) Certificate of US Citizenship (*A.2* - *CIS Form N-560 or N-561*); 3) Alien Registration Receipt Card (*A.5* - *CIS Form I-551 only*); 4) Temporary Resident Card (*A.6* - *CIS Form I-688*); 5) Employment Authorization Card (*A.7 & A.10* - *CIS Form I-688A/B*); 6) Re-entry Permit (*A.8* - *CIS Form I-327*); 7) Refugee Travel Document (*A.9* - *CIS Form I-571*); 8) Driver's license or ID card issued by a State or Outlying Possession of the United States (*B.1*); 9) ID card issued by a Federal or State Government agency or entity (*B.2*);		
201C_PRF#020	**Secondary proofing document:** The **Agency** shall require the	(3)(a), 3(b)	

Criteria tag	**Criteria**	***HSPD-12*** **/ FIPS 201 /** ***SP800-79*** **/ Handbook ref.**	**Compliance source / Assessment finding**
	Applicant to submit secondary proof of id which may be either a second document from the list of acceptable primary id documents or one of the following listed documents: The secondary document must: a) be the original document or a certified copy of the original; b) be unexpired; and c) not have been issued by the same **Agency** or organizational entity. List of acceptable documents (references to Form I-9 (Rev. 11-21-91) are given for comparative purposes, in italics): 1) Certificate of Naturalization (*CIS Form N-550 or N-570*); 2) Foreign passport (*A.4*); 3) Alien Registration Receipt Card (*CIS Form I-151*); 4) ID card issued by a school[, university or other Federally- or State-accredited educational establishment] (*B.3*); 5) Voter's registration card (*B.4*); 6) U.S. Military card or draft record (*B.5*);	§2.1.2(c),§2.2.1(d)(i,ii,iii)	

Criteria tag	**Criteria**	***HSPD-12*** **/** **FIPS 201 /** ***SP800-79*** **/** **Handbook ref.**	**Compliance source / Assessment finding**
	7) Military dependent's ID card (*B.6*); 8) U.S. Coast Guard Merchant Mariner card (B.7); 9) Native American tribal document (*B.8 & C.4*); 10) Driver's license issued by a Canadian government authority (*B.9*); 11) U.S. Social Security card issued by the Social Security Administration (*C.1*); 12) Certificate of Birth Abroad issued by the Department of State (*C.2 – Form FS-545 or Form DS-1350*); 13) Original or certified copy of a birth certificate issued by a State, County, Municipal Authority or Outlying Possession of the United States and which bears an official seal (*C.3*); 14) U.S. Citizen ID card (*C.5 – CIS Form I-197*); 15) ID card for the use of a Resident Citizen in the United States (*C.6 – CIS Form I-179*); 16) Unexpired employment authorization document issued by the INS (*C.7*); For persons under the age of 18 who are unable to present a document from the above list (a document from the primary list is still mandatory): 17) School record or report card (*B.10*);		

Criteria tag	**Criteria**	***HSPD-12*** **/ FIPS 201 /** ***SP800-79*** **/ Handbook ref.**	**Compliance source / Assessment finding**
	18) Clinic, doctor or hospital record (*B.11*); 19) Day-care or nursery-school record (*B.12*);		
201C_PFR#030	**Document & information checks:** The **Agency** shall ensure the presented primary (photographic) identity document: a) appears to be a genuine document properly issued by the claimed issuing authority and acceptable at the time of application; b) bears a photographic image of the holder which matches that of the **Applicant** who, for the purposes of this check, shall be physically present before the agency's Registrar; c) corroborates information provided by the applicant (e.g. DOB, current address of record and other personal information)	*(3)(a)*, *3(b)* **§2.1.2(a)(i)**, **§2.1.2(d)** **§2.2.1(c)**	
201C_VPR#040	**Approved foreign national method:** If the **Agency** employs foreign nationals at locations not established on US territory and which do not fall under the command of a U.S. area military commander, the agency must show, for each such country/location, that the documented registration and approval method has been approved by the U.S. Department of State's Bureau of Diplomatic Security and is being applied in practice.	*(3)(a)*, *3(b)* **§2.2.3**	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
5.2. Biometric capture The **Agency** shall show that it has appropriate technology, systems and sufficient numbers of staff which it trains to the level of skills necessary for the effective prosecution of their responsibilities.			
201C_BIO#010	**Bio-capture**: The **Agency** shall ensure, through appropriate recruitment and training programs, that staff responsible for capturing biometric information are fully-versed in the proper techniques and use of related materials and equipment	*(3)(a)*, 3(b)	
201C_BIO#020	**Bio-capture**: The **Agency** shall capture biometric information from Applicants in a manner consistent with NIST SP 800-76.	*(3)(a)*, 3(b)	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
5.3. Resources and competencies The **Agency** shall show that it has sufficient numbers of staff which it trains to the level of skills necessary for the effective prosecution of their responsibilities.			
201C_RCO#010	**Defined security roles**: The **Agency** shall define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures and other job descriptions. Where the role is security critical, related to privacy or where special privileges or shared duties exist these must be specifically highlighted, including access privileges	*(3)(a)*, 3(b)	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	relating to logical and physical parts of the services operations.		
201C_RCO#020	**Personnel recruitment**: The **Agency** shall demonstrate that it has defined practices for the selection, vetting and contracting of all personnel, both direct employees and those whose services are provided by **Contractors**. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the service policy.	*(3)(a)*, *3(b)*	
201C_RCO#030	**Personnel skills**: The **Agency** shall establish a training program, including recurrent training, which ensures that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished by recruitment practices, through a specific training program or a combination of both. Where employees are undergoing 'on the job' training they must only do so under the guidance of a mentor with established leadership skills and experience of the job in question.	*(3)(a)*, Hbk:2.2.4.1(a)	
201C_RCO#040	**Adequacy of Personnel resources**: The **Agency** shall have sufficient staff to operate the PIV system according to its policies and procedures**.**	*(3)(a)*	

Criteria tag	**Criteria**	***HSPD-12*** **/** **FIPS 201 /** ***SP800-79*** **/** **Handbook ref.**	**Compliance source / Assessment finding**
5.4. Secure communications The **Agency** shall show that it applies adequate protection to sensitive information, especially personal identity information, when such information is transmitted over telecommunication networks.			
201C_SEC#010	**Secure communications**: The **Agency** shall define its policy and derived communication and authentication protocols, encryption algorithms and cryptographic key types and sizes used for the protection of personal identifiable and other system-critical information when being sent over networks and other communication channels between components of its PIV System.	*79:§6.1/1.1*	

6. External Service Provider Management and Operational compliance

Criteria tag	**Criteria**	***HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.**	**Compliance source / Assessment finding**
6.1. Enterprise and Service Maturity Criteria in this section address the establishment of the ESP offering the service and its basic standing as a legal and operational business entity, ready to deliver its services.			
201C_ESM#010	**Established enterprise**: The **ESP** shall be a legally registered trading enterprise and a person with legal authority to commit the enterprise must submit the Assessment Package.	Introduced	
201C_ESM#020	**Established service**: The **ESP** shall be described in the Assessment Package as it stands at the time of submission for assessment and shall be assessed strictly against that description.	Introduced	
201C_ESM#030	**Legal compliance**: The **ESP** shall set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for specific needs of the executive departments/agencies to which its services may be offered.	Introduced	
201C_ESM#040	**Financial Provisions**: The **ESP** shall demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.	Introduced	
201C_ESM#050	**Ownership**: If the enterprise named as the **ESP** is a part of a larger entity, the **ESP** shall disclose to the assessors, and to	Introduced	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	executive departments and agencies should they so request, the nature of the relationship with its parent organization.		
201C_ESM#060	**Independent management and operations**: The **ESP** shall demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability and function according to separate policies, procedures and controls	Introduced	

<table>
<tr><th>Criteria tag</th><th>Criteria</th><th><i>HSPD-12</i> / FIPS 201 / <i>SP800-79</i> / Handbook ref.</th><th>Compliance source / Assessment finding</th></tr>
<tr><td colspan="4"><b>6.2. Information Security Management</b>
Criteria in this section address the way in which the enterprise manages the security of its business, the specified service and information it holds relating to its user community. This focuses on the key components which make up a well-established Information Security Management System (ISMS)..</td></tr>
<tr><td>201C_ISM#010</td><td><b>Documented policies and procedures</b>: The <b>ESP</b> shall have documented all security-relevant administrative, management and technical policies and procedures. The enterprise shall ensure that these are based upon recognized standards or published references which fulfill the needs of executive departments and agencies, are adequate for the specified service and are applied in the manner intended.</td><td>Introduced</td><td></td></tr>
<tr><td>201C_ISM#020</td><td><b>Policy Management and Responsibility</b>: The <b>ESP</b> shall have a clearly defined managerial role, at a senior level, where full</td><td>Introduced</td><td></td></tr>
</table>

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	responsibility for the business' security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place shall be properly maintained so as to be effective at all times.		
201C_ISM#030	**Agency Contact**: The **ESP** shall have a clearly identified liaison officer, responsible for dealing with any issues executive departments and agencies may have with the **ESP**'s service(s).	Introduced	
201C_ISM#040	**Risk Management**: The **ESP** shall demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and shall show that on-going risk assessment review is conducted as a part of the business' procedures	Introduced	
201C_ISM#050	**Continuity of Operations Plan**: The **ESP** shall have and shall keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified service and shall show that on-going review of this plan is conducted as a part of the business' procedures	Introduced	
201C_ISM#060	**Configuration Management**: The **ESP** shall demonstrate a Configuration Management system that at least includes: a) version control for software system components; b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service; c) version control and managed distribution for all documentation associated with the specification, management and operation of the system, covering both internal and publicly available materials.	Introduced	
201C_ISM#070	**Quality Management**: The **ESP** shall demonstrate a Quality	Introduced	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
	Management system that is appropriate for the service it is contracted to provide.		
201C_ISM#080	**System Installation and Operation Controls**: The **ESP** shall apply controls during system development, procurement installation and operation which protect the security and integrity of the system environment, hardware, software and communications having particular regard to: a) the software and hardware development environments, for customized components; b) the procurement process for COTS components; c) contracted consultancy/support services; d) shipment of system components; e) storage of system components; f) installation environment security; g) system configuration; h) transfer to operational status.	Introduced	
201C_ISM#090	**Internal Service Audit**: Unless it can show that by reason of its size or for other arguable operational reason it is unreasonable so to perform, the **ESP** shall be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the Specified Service.	Introduced	
201C_ISM#100	**Independent Audit**: The **ESP** shall be audited by an independent auditor at least every 12 months, against a recognized industry reference model for information security management, to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor shall have appropriate accreditation or other acceptable experience and qualifications for the performance of the audit.	Introduced	

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
201C_ISM#110	**Audit Records**: The **ESP** shall retain full records of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber. Such records shall be held securely and protected against loss, alteration or destruction.	Introduced	
201C_ISM#120	**Termination provisions**: The **ESP** shall have in place a clear plan for the protection of executive departments' and agencies' subscribers' private and secret information related to their use of the service which shall ensure the ongoing secure preservation and protection of legally-required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be provided to Federal entities.	Introduced	
201C_ISM#130	**Best Practice Security Management**: The **ESP** shall have in place **a certified** Information Security Management System (ISMS) which is based upon the [draft] information security management standard ISO/IEC 27001:2005, which implements the code of practice set out in ISO/IEC 17799:2005, follows best practice as accepted by the information security industry and which applies and is appropriate to the ETPS in question. All requirements expressed in preceding criteria in this 'ISM' section must fall wholly within the scope of this ISMS.	Introduced	

<table>
<tr><th>Criteria tag</th><th>Criteria</th><th><i>HSPD-12</i> / FIPS 201 / <i>SP800-79</i> / Handbook ref.</th><th>Compliance source / Assessment finding</th></tr>
<tr><td colspan="4"><b>6.3. External services and components</b>
This section addresses the relationships and obligations upon sub-contracted parties both to apply the policies and procedures of the ESP and also to be available for assessment as critical parts of the overall service provision.</td></tr>
<tr><td>201C_ESC#010</td><td><b>Contracted policies and procedures</b>: Where the <b>ESP</b> uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, it shall ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the sub-contractor is required to fulfill and shall gain approval of these arrangements from either the Agency or from another approval source recognized by the Agency (e.g. a formalized Federal government scheme established to provide such approvals).</td><td>Introduced</td><td></td></tr>
<tr><td>201C_ESC#020</td><td><b>Visibility of contracted parties</b>: Where the <b>ESP</b> uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its control, it shall ensure that those contractors’ compliance with contractually stipulated policies and procedures, and thus with Guidance criteria, can be proven and subsequently monitored.</td><td>Introduced</td><td></td></tr>
</table>

Criteria tag	Criteria	*HSPD-12* / FIPS 201 / *SP800-79* / Handbook ref.	Compliance source / Assessment finding
6.4. Required Records The Agency must retain records of the identity enrollment and issuance services that it provides.			
201C_RQR#010	**Required records**: The ESP shall capture and either securely retain itself or pass to the contracting Agency information related to the enrollment and issuance process in accordance with the criteria set out in Required records and any other requirements stipulated by applicable law or the Agency/ies concerned.	Introduced	
201C_RQR#020	**Long-term Archiving**: The ESP shall ensure that its contract with any Agency to which it provides service shall include provisions for the long-term secure storage of required records and other sensitive material which provides for the security of these records in the case the ESP ceases its service or business.	Introduced	

Appendix A: HSPD-12 and FIPS 201 Requirements

The following requirements specified in HSPD-12 and FIPS 201 have been re-structured to enable the discrete referencing of specific clauses in the assessment criteria set out in preceding Sections. No semantic changes to the requirements have been made. New sections have been added for clarity along with section numbering, the alphabetic labeling of bullet lists and additional levels of referencing where necessary. Those references which are changed from the original text are shown in blue highlighting, thus. Cross-referencing hyper-links point to the criteria in the main sections. They are shown in brackets [*like this*].

From HSPD-12, paragraph (3):

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that

(a) is issued based on sound criteria for verifying an individual employee's identity;
(b) is strongly resistant to
 (i) identity fraud,
 (ii) tampering,
 (iii) counterfeiting, and
 (iv) terrorist exploitation;
(c) can be rapidly authenticated electronically; and
(d) is issued only by providers whose reliability has been established by an official accreditation process.

From the FIPS 201 Preamble, "Announcing the Standard …":

6. Applicability.

6.1 This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2).[*Scope of PIV System*] Except as provided in HSPD 12, nothing in this standard alters the ability of government entities to use the standard for additional applications.

6.2 Special-risk security provision – The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For those agencies with particularly sensitive OCONUS threats, the issuance, holding, and/or use of PIV credentials with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV credentials, the head of a Department or independent agency may issue a select number of maximum security credentials that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, heads of Departments and independent agencies should minimize the issuance of such special-risk security credentials so as to support inter-agency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, this need for this provision will be re-assessed as the standard undergoes the normal review and update process. [*Special-risk security provision*]

From the FIPS 201 §2, “Common Identification, Security, and Privacy Requirements”:

2.1 Control Objectives

2.1.1 [HSPD-12] established control objectives for secure and reliable identification of Federal employees and contractors. These control objectives, provided in paragraph 3 of the directive, are quoted here: (3) “Secure and reliable forms of identification” for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee’s identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. [*See separate indications of compliance with HSPD-12 in specific criteria*]

2.1.2 Each agency’s PIV implementation shall meet the four control objectives (a) through (d) listed above such that –

a) Credentials are issued:

i) to individuals whose true identity has been verified and; [*Document & information checks (a)*]

ii) after a proper authority has authorized issuance of the credential; [*Authorized Issuance*]

b) Only an individual with a background investigation on record is issued a credential;[*Completing the investigation*, *Negative investigation outcome*, *Positive investigation outcome*]

c) An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture ID; [*Primary proofing document*, *Secondary proofing document*]

d) Fraudulent identity source documents are not accepted as genuine and unaltered; [*Document & information checks(a)*]

e) A person suspected or known to the government as being a terrorist is not issued a credential; [*Completing the investigation*]

f) No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued;[*Verified credential delivery*]

g) No credential is issued unless requested by proper authority; [*Request to issue credential*]

h) A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked; [*Credential expiration*, *Credential* *Credential revocation* , *Revocation validation*]

i) A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential;[*Separation of roles*]

j) An issued credential is not: [*Compliant credential personalization*]
i) modified; [*Compliant identity credential*]
ii) duplicated, or; [*Unique PIV system identity*]
iii) forged; [*Compliant identity credential*]

2.2 PIV Identity Proofing and Registration Requirements

2.2.1 For compliance with the PIV-I control objectives, departments and agencies shall follow an identity proofing and registration process that meets the requirements defined below when issuing identity credentials.

a) The organization shall adopt and use an approved identity proofing and registration process.[*Credential issuing policy*, *Published Privacy Policy*]

b) The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. At a minimum, the National Agency Check (NAC) or other recognized investigation shall be completed before credential issuance.[6] Appendix C, Background Check Descriptions, provides further details on NAC and NACI. [*Required Information*, *Initial proofing of id*, *Initiating investigation*, *Completing the investigation*, *Negative investigation outcome*]

c) The applicant must appear in-person at least once before the issuance of a PIV credential.[*Document & information checks (b)*]

d) During identity proofing: [*Primary proofing document*, *Secondary proofing document*]

i) the applicant shall be required to provide two forms of identity source documents in original form

ii) the identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*

iii) at least one document shall be a valid State or Federal government-issued picture identification (ID).

e) The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.[*Separation of roles*]

2.2.2 The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency Designated Accreditation Authority as satisfying the requirements above and approved in writing by the head of the Federal department or agency. [*PIV-I Approval*, *PIV-II Approval*, *Assignment to roles*] [Two examples of processes that meet these requirements are provided in Appendix A, PIV Processes. *Informative note only – Agencies are not required to implement these provisions*]

2.2.3 These requirements also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for registration and approval must be established using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander. These procedures may vary depending on the country.[*Overseas Applicants*, *Approved foreign national method*, *Required Information*]

2.3 PIV Issuance and Maintenance Requirements

2.3.1 For compliance with the PIV-I control objectives, departments and agencies shall meet the requirements defined below when issuing identity credentials

a) The organization shall use an approved PIV credential issuance and maintenance process. [*PIV-I Approval*, *PIV-II Approval*, *Assignment to roles*]

b) The process shall ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment. The PIV credential shall be revoked if the results of the investigation so justify. [*Completing the investigation*, *Negative investigation*, *Further investigation*]

c) At the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority. [*Secure credential delivery*]

d) The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited). [*PIV-I Approval*, *PIV-II Approval*, *Externally provided services*, *Approved external services*, *External service oversight*]

[6] Note: a completed National Agency Check is sufficient for credential issuance; however, the required National Agency Check with Inquiries must still be performed.

2.4 PIV Privacy Requirements

2.4.1 HSPD 12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. As such, all departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies, as applicable, including but not limited to:[*PIA Scope*]

a) the E-Government Act of 2002 [E-Gov];
b) the Privacy Act of 1974 [PRIVACY] and;
c) Office of Management and Budget (OMB) Memorandum M-03-22 [OMB322].

2.4.2 Departments and agencies may have a wide variety of uses of the PIV system and its components that were not intended or anticipated by the President in issuing [HSPD-12]. In considering whether a proposed use of the PIV system is appropriate, departments and agencies shall consider the aforementioned control objectives and the purpose of the PIV standard, namely "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." [HSPD-12] No department or agency shall implement a use of the identity credential inconsistent with these control objectives. [*Use of PIV System*]

2.4.3 To ensure the privacy of applicants, departments and agencies shall do the following:

a) Assign an individual to the role of senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard. The individual serving in this role may not assume any other operational role in the PIV system. [*Separation of roles*]

b) Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with [E-Gov] and [OMB322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system. [*Privacy Impact Assessment*, *PIA Scope*]

c) Write, publish, and maintain a clear and comprehensive document: [*Published Privacy Policy* *(all below)*]

i) listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]);

ii) stating the purpose of collection;

iii) stating what information may be disclosed to whom during the life of the credential;

iv) stating how the information will be protected, and;

v) stating the complete set of uses of the credential and related information at the department or agency; [*Credential usage*]

vi) ~~PIV applicants shall be provided~~ giving full disclosure of the intended users [sic] of the PIV credential and the related privacy implications. [*Credential usage*]

d) Assure that systems that contain IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY]. [*PIA Scope*]

e) Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.[*Appeal of denial/revocation*]

f) Ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance. *[Rights and Privileges*]

g) Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system. [*Policy Violations*]

h) Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program. [*Security-event audit*, *Record Retention*]

i) Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable. [SP800-53] [*PIA Scope*, *Use of PIV System*]

j) Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contact-less access to information stored on a PIV credential. [*No negative impact*, *Compliant identity credential*]

From the FIPS 201 §5.3, "PIV Issuance and Maintenance Requirements:

5.3.1 PIV Card Issuance

5.3.1.1 Section 2.3 of this standard requires the adoption and use of an approved issuance and maintenance process. All PIV-II issuance and maintenance systems must satisfy the PIV-I objectives and requirements stated in Sections 2.3 in order to be approved. [*PIV-I Approval*, *PIV-II Approval*]

5.3.1.2 An employee or contractor may be issued PIV Card and logical credentials while a National Agency Check with Written Inquiries (NACI) or other OPM or National Security community investigation required for Federal employment is pending. In such cases, the process must verify successful completion and adjudication of the investigation within six months of PIV card issuance, or the PIV card and the PIV authentication certificate for the card shall be revoked. [*Negative investigation outcome*, *Timed-out investigation*]

5.3.1.3 An additional requirement is that the issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record. On successful match, the PIV Card shall be released to the applicant. [*Verified credential delivery*]

5.3.1.4 Two examples of PIV issuance process sets that satisfy the requisite PIV-II objectives and requirements are provided in Appendix A, Sections A.1.2 and Appendix A Sections A.2.2 through A.2.4. The heads of Federal departments and agencies may approve other identity proofing, registration, issuance process sets that are accredited as satisfying the requisite PIV-I objectives and requirements. Departments and agencies may enhance their issuance process to meet their local constraints and requirements. [*Enhanced PIV system*]

5.3.2 PIV Card Maintenance

5.3.2.0.1 The PIV Card shall be maintained via processes that comply with the specifications in this section.

5.3.2.0.2 The data and credentials held by the PIV Card may need to be invalidated prior to the expiration date of the card. The cardholder may retire, change jobs, or the employment is terminated, thus requiring invalidation«*revocation*» of a previously active card. The card may be damaged, lost, or stolen, thus requiring a replacement.[*Credential revocation*, *Revocation validation*] The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card management. [*Credential status management*]

5.3.2.1 PIV Card Renewal

5.3.2.1.1 Renewal is the process by which a PIV Card is replaced without the need to repeat the full registration procedure. The card issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials to current employees, the NACI checks shall be followed in accordance with the OPM guidance. [*Verification on renewal*]

5.3.2.1.2 The PIV Card shall be valid for no more than five years. A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card.[*Credential renewal*] The card issuer will verify the cardholder's identity against the biometric information stored on the expiring card.[*Verified credential delivery*] The expired PIV Card must be collected and destroyed. [*Credential destruction*]

5.3.2.1.3 The same biometric data may be reused with the new PIV Card while the digital signature must be recomputed with the new FASC-N.

5.3.2.1.4 The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card. Hence, a new PIV authentication key and certificate shall be generated. If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.

5.3.2.2 PIV Card Reissuance

5.3.2.2.1 In case of reissuance, the entire registration and issuance process, including fingerprint and facial image capture, shall be conducted. The card issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.[*Request to issue credential*]

5.3.2.2.2 A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. [*Request to issue credential*]

5.3.2.2.3 When these events are reported, normal operational procedures must be in place to ensure the following:

a) The existing PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status;

b) The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers;

c) Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server’s internal revocation records).

5.3.2.2.4 It is recommended that the old PIV Card, if available, is collected and destroyed. If the card cannot be collected, normal operational procedures shall complete within 18 hours of notification.[*Revocation notification*] In some cases, 18 hours is an unacceptable delay. In that case, emergency procedures must be executed to disseminate this information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.[*Emergency revocation*]

5.3.2.3 PIV Card PIN Reset

The PIN on a PIV Card may need to be reset if the contents of the card are locked resulting from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency. PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder’s biometric matches the stored biometric on the reset PIV Card. Departments and agencies may adopt more stringent procedures for PIN reset (including disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency.

5.3.2.4 PIV Card Termination

5.3.2.4.1 The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. The PIV Card shall be terminated under the following circumstances:[*Credential revocation*, *Revocation validation*, *Revocation reason*, *Credential destruction*]

a) An employee separates (voluntarily or involuntarily) from Federal service

b) A Contractor employee separates (voluntarily or involuntarily) from a Federal contractor

c) A Federal contractor changes positions and no longer needs access to Federal buildings or systems

d) A cardholder is determined to hold a fraudulent identity

e) A cardholder passes away.

5.3.2.4.2 Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following:[]

a) The PIV Card is collected and destroyed.[*Credential destruction*]

b) The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. [*Credential revocation*, *Revocation validation*, *Revocation reason*, *Revocation notification*]

c) The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers. [*Revocation notification*]

d) OCSP responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).[*Revocation notification*]

e) The IIF that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.[*Published Privacy Policy*, *Record Retention*, *Record Destruction*]

Appendix B: References

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974*, December 31, 1974 (effective September 27, 1975).
(Available at http://www.archives.gov/research_room/foia_reading_room/privacy_act/privacy_act.html.)

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002*, December 17, 2002.
(Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf.)

United States Office of Management and Budget, *Circular No. A-130*, Appendix III, Security of Federal Automated Information Resources, February 1996.
(Available at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.
(Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Security Controls for Federal Information Systems*, projected for publication December 2005.
(Will be available at http://csrc.nist.gov/publications.)

Committee for National Security Systems, Instruction 4009, *National Information Assurance Glossary*, Revised May 2003.
(Available at http://staff.washington.edu/dittrich/center/4009.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, February 2005.
(Available at http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
(Available at http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Version 2.0, June 2003 draft.
(Available at http:/csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, Version 1.9, October 2003.
(Available at http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
(Available at http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-73, *Interfaces for Personal Identity Verification*, April 2005.
(Available at http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, Draft, February 2005.
(Available at http://csrc.nist.gov/piv-project/fips201-support-docs/SP800-76-Draft.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, March 2005.
(Available at http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-79, Guidelines for the Certification and Accreditation of the Reliability of Personal Identity Verification Card Issuing Organizations, July, 2005.

(Available at http://csrc.nist.gov/piv-project/nistpubs/800-79-Final.pdf .)

Executive Office of the President, Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953.
(Available at http://www.archives.gov/federal_register/codification/executive_order/10450.html.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.
(Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.)

Federal Identity Credentialing Committee, *Federal Identity Management Handbook*, Draft Version 0.2, March 2005.
(Available at http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf.)