LABOR RELATIONS

UNITED STATES
POSTAL SERVICE

July 30, 2020

Mr. Brian J. Wagner
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Dear Brian:

The Postal Service plans to revise Administrative Support Manual (ASM), Section 517.2, *Interchange of Space in Postal Service and GSA Buildings*.

The purpose of the revisions is to ensure compliance with Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, as it pertains to access to buildings the Postal Service leases from the General Services Administration (GSA). As a result of these revisions, certain postal employees will be required to obtain Personal Identity Verification – Inoperable (PIV-I) cards issued by GSA.

We have enclosed:

- Two copies of the revisions to ASM 517.2, one with and one without tracked changes
- A list of facilities impacted and the number and type of employees who access each
- A document explaining the purpose and impact of the changes to ASM 517.2
- A copy of HSPD-12
- A copy of "Your Credential," which outlines the steps necessary to obtain a PIV-I card
- A copy of "USAccess Acceptable Forms of Identification Guide," which outlines the identification types required to obtain a PIV-I card
- A copy of "Personal Identity Verification – Interoperable (PIV-I) Credential," which provides a diagram of the PIV-I credential

Please contact Bruce Nicholson at 7773 if you have questions concerning this matter.

Sincerely,

for David E. Mills
Manager
Labor Relations Policies and Programs

Enclosures

The Postal Service leases operating space from the General Services Administration (GSA) throughout the country. Postal employees are provided access to most of these buildings through postal-only entrances. However, in 12 buildings (details attached), postal employees must use public access points to enter the buildings. The Postal Service intends to execute a new lease with GSA effective October 1, that will require postal employees who use these public access points to possess a Personal Identity Verification-Inoperable (PIV-I) card.

The requirement for a PIV-I card is based on Homeland Security Presidential Directive – 12 (HSPD-12), issued in 2004, which requires federal agencies to use a standard credential to verify the identities of all employees and contractors accessing federal buildings and information systems. Effective with the execution of the October 1, 2020, lease, GSA will require compliance with HSPD-12 for admittance to buildings at which postal-only entrances are not available[1].

PIV-I cards (example provided below) are similar to postal identification badges, however they do not signify an individual has completed a background investigation as defined by postal policy. To obtain a PIV-I card, individuals must meet in-person with an organization authorized to issue PIV-I cards and must present identification documents as detailed in *USAccess Acceptable Forms of Identification* and a signed Privacy Act Statement, both of which are attached. Fingerprints would also have to be captured, but would only be used for identity verification, not for any type of criminal background check. A detailed accounting of the steps necessary to receive a PIV-I card can be found here: https://www.fedidcard.gov/your-credential#Step (print-out attached).

Whether individual employees will be required to obtain a PIV-I card will be determined by local operations based on needs of the service and the efficiency and cost of facilitating employees obtaining PIV-I cards compared to guest building access procedures. When the determination is made that an employee will need a PIV-I card for his/her assignment, local management will coordinate with the Inspection Service and the employee to schedule the necessary appointments. All costs associated with obtaining a PIV-I card, including travel time pursuant to Handbook F-15, *Travel and Relocation*, will be compensated by the Postal Service. PIV-I cards issued to employees will be considered accountable property and must be surrendered to the Inspection Service when the PIV-I card is no longer needed by the employee (e.g. if the employee resigns from USPS or changes assignment).

The attached proposed revisions to Administrative Support Manual, Section 517, *Interchange of Space in Postal Service and GSA Buildings* capture the requirements listed above.

Tom Russell

Digitally signed by Tom Russell
DN: cn=Tom Russell, o=Facilities,
ou=Planning,
email=tom.russell@usps.gov, c=US
Date: 2020.07.30 10:22:54 -04'00'

Tom Russell
Manager, Facilities Real Estate & Assets

[1] In limited instances, employees may be provided guest access to these buildings, provided the employee complies with the GSA security procedures for admission of visitors to that building.

517.2 Interchange of Space in Postal Service and GSA Buildings

517.21 GSA-Postal Service Agreement

Occupancy of space by the Postal Service in GSA-controlled buildings, and by the GSA and other federal agencies in Postal Service-controlled buildings, is governed by the *Agreement Between General Services Administration and the United States Postal Service Covering Real and Personal Property Relationships and Associated Services* (GSA-Postal Service Agreement)

517.22 Rent

Rent is the payment by which each agency compensates the other for space occupancy and for standard levels of building operation, utilities, cleaning, and security.

517.23 GSA-Postal Service Relationship

The relationship between the GSA and the Postal Service is on a landlord-tenant basis. Other federal agencies including the U.S. courts and members of Congress) occupying space in Postal Service buildings are considered subtenants of the GSA.

517.24 Access to GSA-Controlled Buildings

Certain GSA-controlled buildings have restricted access points that require a Personal Identity Verification-Interoperable (PIV-I) credential for entrance. Postal employees who need to regularly access one of these GSA-controlled buildings will be required to obtain and possess a PIV-I credential.

In the event a postal employee does not possess a PIV-I credential, guest access to the GSA-controlled building may be granted, provided the employee complies with the GSA security procedures for admission of visitors to that building.

517.2 Interchange of Space in Postal Service and GSA Buildings

517.21 GSA-Postal Service Agreement

Occupancy of space by the Postal Service in GSA-controlled buildings, and by the GSA and other federal agencies in Postal Service-controlled buildings, is governed by the *Agreement Between General Services Administration and the United States Postal Service Covering Real and Personal Property Relationships and Associated Services* (GSA-Postal Service Agreement)

517.22 Rent

Rent is the payment by which each agency compensates the other for space occupancy and for standard levels of building operation, utilities, cleaning, and security.

517.23 GSA-Postal Service Relationship

The relationship between the GSA and the Postal Service is on a landlord-tenant basis. Other federal agencies including the U.S. courts and members of Congress) occupying space in Postal Service buildings are considered subtenants of the GSA.

517.24 Access to GSA-Controlled Buildings

Certain GSA-controlled buildings have restricted access points that require a Personal Identity Verification-Interoperable (PIV-I) credential for entrance. Postal employees who need to regularly access one of these GSA-controlled buildings will be required to obtain and possess a PIV-I credential.

In the event a postal employee does not possess a PIV-I credential, guest access to the GSA-controlled building may be granted, provided the employee complies with the GSA security procedures for admission of visitors to that building.

Building Name	Building Address	State	City	Area	District	Anticipated Impacted Employees	Closest PIV-I Credentialing Facility
JFK FEDERAL BUILDING	15 New Sudbury St	MA	BOSTON	Northeast	Greater Boston	Two city carriers, two clerks	Same building
JAMES M HANLEY FB	100 S CLINTON ST	NY	SYRACUSE	Northeast	Albany	11 carriers, 7 clerks	.4 miles away
PEACHTREE SUMMIT FB	401 W PEACHTREE ST NW	GA	ATLANTA	Capital Metro	Atlanta	One city carrier	Same building
HOLLINGS JUD CTR	83 MEETING ST	SC	CHARLESTON	Capital Metro	Greater So Carolina	One clerk	TBD
G W HEANEY F.B. & US COURTHOUS	515 W 1st St	MN	DULUTH	Western	Northland	One clerk	.2 miles away
A J CELEBREZZE FB	1240 E 9TH ST	OH	CLEVELAND	Eastern	Northern Ohio	Two clerks	Same building
BRICKER FEDERAL BLDG	200 N HIGH ST	OH	COLUMBUS	Eastern	Ohio Valley	One clerk	Same building
RICHARD BOLLING FB	601 E 12TH ST	MO	KANSAS CITY	Western	Mid-America	One clerk	1.5 miles away
F. EDWARD HEBERT FEDERAL	600 S MAESTRI PL	LA	NEW ORLEANS	Southern	Louisiana	One clerk	.8 miles away
DENNIS CHAVEZ FEDERAL BUILDING	500 GOLD AVE SW	NM	ALBUQUERQUE	Western	Arizona	Three clerks	TBD
HOUSTON CUSTOM HOUSE	701 SAN JACINTO ST	TX	HOUSTON	Southern	Houston	Two clerks	1 mile away
BOB CASEY FEDERAL BUILDING	515 RUSK ST	TX	HOUSTON	Southern	Houston	One clerk	1 mile away
FEDERAL BUILDING	300 N LOS ANGELES ST	CA	LOS ANGELES	Pacific	Los Angeles	One clerk	Same building
PHILLIP BURTON,FB CT	450 GOLDEN GATE AVE	CA	SAN FRANCISCO	Pacific	San Francisco	One clerk	Same building

REVISION CHART

Version	Primary Author(s)	Description of Version	Date Completed
1.0		Original	9/2016
1.1	Tavia Bazemore	Updated revision chart and footnote	5/21/19
1.2	Tavia Bazemore/Angela Gibson	Changed section 2.1, page 3, to add Congressional ID as an acceptable form of secondary identification for the FIPS 201-2, Personal Identity Verification (PIV)	2/26/2020

USAccess Acceptable Forms of Identification Guide

1.0 Overview

All USAccess PIV card applicants are required to provide identification at the time of Enrollment. This guidance is provided to clarify the Identity Proofing requirements for USAccess PIV cards and to follow **FIPS 201-2** standards.

2.0 Identity Document Requirements

Applicants are required to provide two forms of identification.

During the identity proofing phase of the USAccess credentialing process, applicants are required to provide two forms of identity source documents in their original form. These documents must be brought to Enrollment appointments. All identity source documents shall be bound to that applicant and shall be **neither expired nor canceled**.

The current list of acceptable primary and secondary source documents is listed in the Primary and Secondary identification tables below. **At a minimum one of the identity source documents must be from the Primary list**.

2.1 Approved Identity Source Documents

The following primary and secondary Identity Source documents are approved for use by USAccess.

Primary Forms of Identification
1. U.S. Passport or a U.S. Passport Card;
2. Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
3. Foreign passport;
4. Employment Authorization Document that contains a photograph (Form I-766);
5. Driver's license or an ID card issued by a state or possession of the United States provided it contains a photograph;
6. U.S. Military ID card;
7. U.S. Military dependent's ID card; or
8. PIV Card.

Note: Photos are required for all forms of primary identification above

The information contained in this document is proprietary and may not be transmitted or disclosed to anyone outside of the Government or authorized representatives without written permission.

Secondary Forms of Identification

1. U.S. Social Security Card issued by the Social Security Administration *Laminated SSA cards cannot be used without Security Officer approval.*	2. Original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal;
3. ID card issued by a federal, state, or local government agency or entity, provided it contains a photograph; EXCEPTIONS APPLY – See Section 2.4 below	4. Voter's registration card;
5. U.S. Coast Guard Merchant Mariner Card;	6. Certificate of U.S. Citizenship (Form N-560 or N-561);
7. Certificate of Naturalization (Form N-550 or N-570);	8. U.S. Citizen ID Card (Form I-197);
9. Identification Card for Use of Resident Citizen in the United States (Form I-179);	10. Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350);
11. Temporary Resident Card (Form I-688);	12. Employment authorization document issued by Department of Homeland Security (DHS);
13. Reentry Permit (Form I-327);	14. Refugee Travel Document (Form I-571);
15. Employment authorization document issued by Department of Homeland Security (DHS);	16. Employment Authorization Document issued by DHS with photograph (Form I-688B);
17. Driver's license issued by a Canadian government entity;	18. Native American tribal document; or
19. Congressional Identification (ID) that meets FIPS 201-2 requirements (Must have a visible expiration date in red font)	

2.2 General Rules for Acceptance

The following rules apply to all presented identity source documents:

- All documents must be in their original forms - no photocopies other than a certified copy of birth certificate bearing an official seal.
- Expired or canceled identity documents are not acceptable.
    - All Primary forms of ID contain an expiration date; however some Secondary forms of ID do not. Not having an expiration date does not make a Secondary ID Source unacceptable. Secondary forms of ID without an expiration date can be accepted.
- Updating or replacing identity source documents is not required after successfully completing the identity proofing process.

2.3 Examples of Acceptable Identity Source Documents

The USAccess Help Desk often receives questions regarding acceptable forms of ID. Some of the more frequently asked about forms of identification that are **ACCEPTABLE** are listed below:

- PIV Card – Acceptable *Primary* form of ID
- Agency ID Badge – Acceptable *Secondary* form of ID
    - Must be issued by federal, state, or local government agency or entity
    - Must contain a photograph

      Note that an Agency ID badge differs from a Facility Badge, which is not acceptable, in that an Agency ID badge is an Agency-wide identity card issued by the Agency itself, rather than a badge used specifically for accessing a facility
- TSA Transportation Worker Identification Credential (TWIC) – Acceptable *Secondary* form of ID
- DHS Trusted Traveler Cards – Acceptable *Secondary* form of ID. This includes:
    - Global Entry cards
    - SENTRI cards
    - NEXUS cards
    - FAST cards

2.4 Examples of Identity Source Documents Not Accepted

Identity proofing documents **NOT ACCEPTED** by USAccess include, but are not limited to:

- Student ID Cards (including public/state universities, as well as private universities)
- Gun or Firearms permits
- License to Carry
- Hunting/Fishing permits
- Facility Badge
- Temporary driver's licenses
- Selective service card
- Company ID Card

- Foreign Driver's License (other than Canada)
- Library Card
- Temporary PIV Card
- Marriage license

  Note that Marriage license is an acceptable linking document, but not an acceptable Primary or Secondary form of identification

2.5 Primary and Secondary Combination Examples

The following examples of source identification documentation are representative of acceptable combinations of Primary and/or Secondary source documents that can be used to successfully validate an applicant's identity:

Acceptable Combination 1:

a. Virginia State Driver's license (Primary)
b. US Social Security Card (Secondary)

Acceptable Combination 2:

a. US Passport (Primary)
b. Maryland State Driver's license (Primary)

Acceptable Combination 3:

a. US Military ID Card (Primary)
b. Department of State ID Card (Secondary)

The following examples of source identification documentation are representative of unacceptable combinations of Primary and/or Secondary source documents that CANNOT be used to successfully validate an applicant's identity:

Unacceptable Combination 1:

a. US Social Security Card (Secondary)
b. Voter's registration card (Secondary)

Reason: At least one form of identification must be Primary

Unacceptable Combination 2:

a. Virginia State Driver's license (Primary #5)
b. Virginia State ID card (Primary #5)

Reason: While on their own, these are both valid Primary forms of ID, the language in the Primary forms of ID table above states the applicant should present "Driver's license *or* an ID card issued by a state." One may be accepted, but not both, as these are essentially the same form of ID.

The information contained in this document is proprietary and may not be transmitted or disclosed to anyone outside of the Government or authorized representatives without written permission.

3.0 Linking Documents

If any of the identity source documents presented for identity proofing bear different names then **evidence of a formal name change must be provided linking the names.** More information on linking documents is provided below.

3.1 Requirements for Identity Source Linking Documents

Identity source documents with different names can only be accepted when an official linking document is presented.

All linking documents must include both the former and current legal names. All linking documents must be valid and not expired.

Example: A married woman may use both a current driver's license with her married name, and her birth certificate with her maiden name, as primary and secondary sources of identification as long as they are accompanied by an approved linking document. For this example an approved linking document would be a marriage license – original or certified copy - with both her maiden name and married name on it.

3.2 Approved Linking Documents

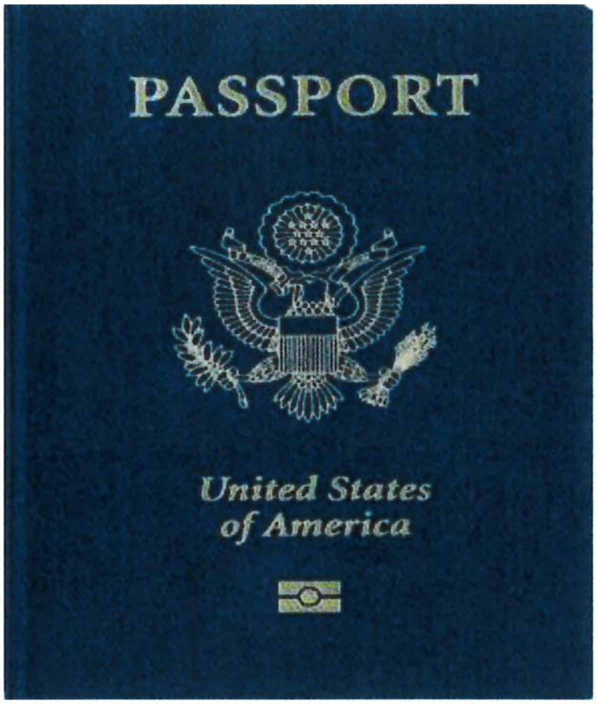
The following are approved linking documents:

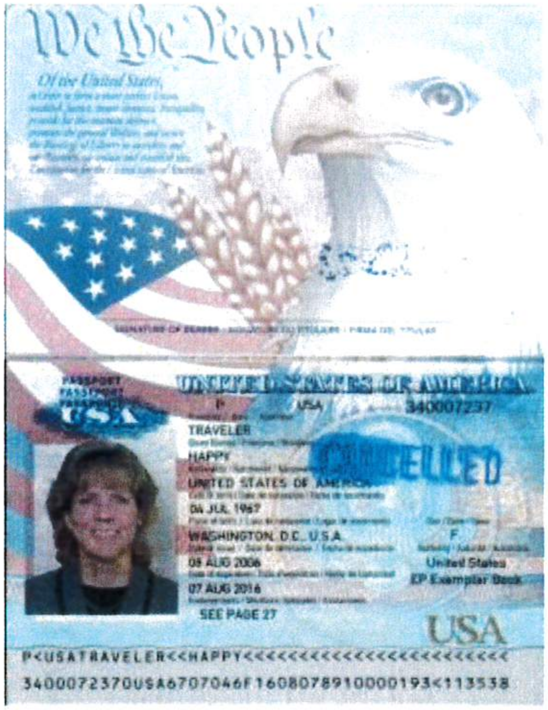
- Marriage Certificate
- Court record linking the two names

USAccess requires that linking document be scanned into the *Document 3* window located on the USAccess Enrolment page.

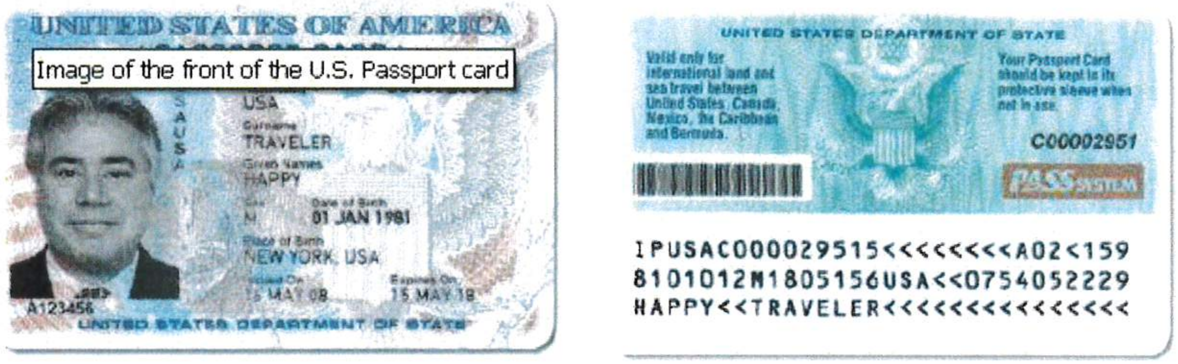
Appendix: ID Card Type Examples

U.S. Passport



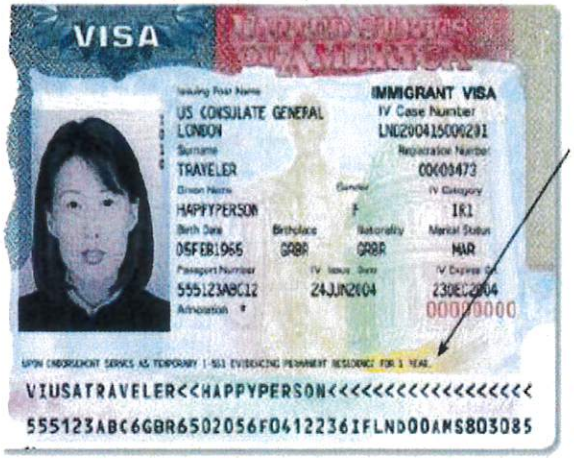


U.S. Passport or U.S. Passport Card


UNITED STATES OF AMERICA
Image of the front of the U.S. Passport card
USA
TRAVELER
HAPPY
M
01 JAN 1981
NEW YORK, USA
15 MAY 08
15 MAY 18
A123456
UNITED STATES DEPARTMENT OF STATE
UNITED STATES DEPARTMENT OF STATE
Valid only for international land and sea travel between United States, Canada, Mexico, the Caribbean and Bermuda.
Your Passport Card should be kept in its protective sleeve when not in use.
C00002951
PASS SYSTEM
IPUSAC000029515<<<<<<<<A02<159
8101012M1805156USA<<0754052229
HAPPY<<TRAVELER<<<<<<<<<<<<<<<

Passport Card front and back

Foreign Passport



VISA

UNITED STATES OF AMERICA

Issuing Post Name
US CONSULATE GENERAL
LONDON

IMMIGRANT VISA
IV Case Number
LND2004150000291

Surname
TRAVELER

Registration Number
00003473

Given Name
HAPPYPERSON

Gender
F

IV Category
IR1

Birth Date
05FEB1965

Birthplace
GRBR

Nationality
GRBR

Marital Status
MAR

Passport Number
555123ABC12

IV Issue Date
24JUN2004

IV Expires On
23DEC2004

Annotation *

00000000

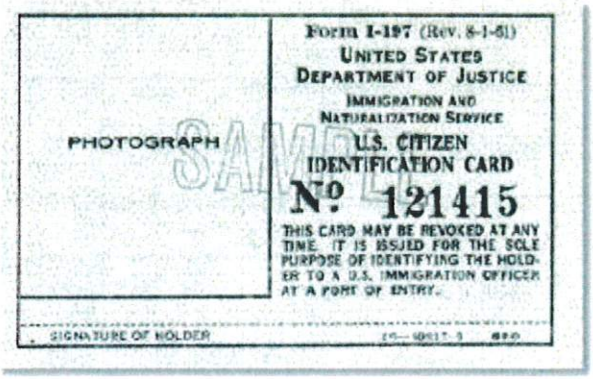
UPON ENDORSEMENT SERVES AS TEMPORARY I-551 EVIDENCING PERMANENT RESIDENCE FOR 1 YEAR.

```
VIUSATRAVELER<<HAPPYPERSON<<<<<<<<<<<<<<<<<<<
555123ABC6GBR6502056F0412236IFLND00AMS803085
```

Upon endorsement serves as temporary I-551 evidencing permanent residence for 1 year

Temporary I-551 printed notation on a machine-readable immigrant visa (MRIV)

U.S. Citizen ID Card (Form I-179) - Must Have Photograph



PHOTOGRAPH

Form I-197 (Rev. 8-1-61)

UNITED STATES
DEPARTMENT OF JUSTICE

IMMIGRATION AND
NATURALIZATION SERVICE

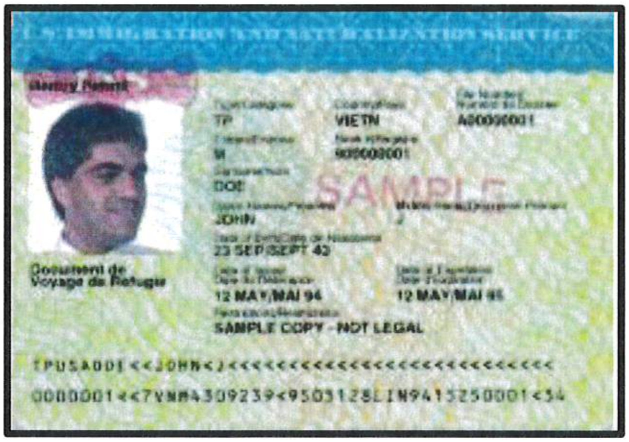
U.S. CITIZEN
IDENTIFICATION CARD

Nº 121415

THIS CARD MAY BE REVOKED AT ANY TIME. IT IS ISSUED FOR THE SOLE PURPOSE OF IDENTIFYING THE HOLDER TO A U.S. IMMIGRATION OFFICER AT A PORT OF ENTRY.

SIGNATURE OF HOLDER

Reentry Permit with photograph (Form I-327)



Reentry Permit

TP VIETN A00000001

M 000000001

DOE

SAMPLE

JOHN J

23 SEP/SEPT 42

Document de Voyage de Refugie

12 MAY/MAI 94 12 MAY/MAI 95

SAMPLE COPY - NOT LEGAL

TPUSA0001<<JOHN<J<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
0000001<<7VNM4309239<9505128LIN9415250001<54

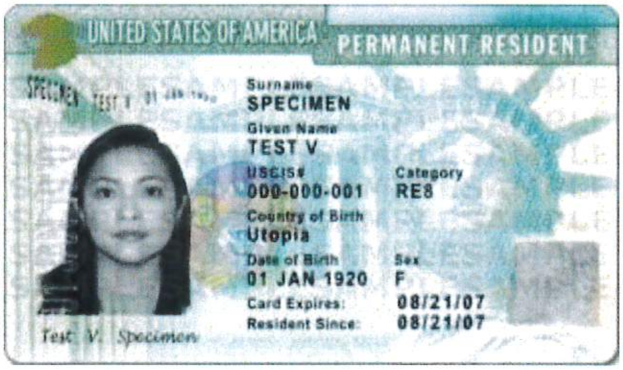
ALIEN REGISTRATION RECEIPT CARD

SAMPLE

[illegible]

UNITED STATES DEPARTMENT OF JUSTICE

Permanent Resident Card or Alien Registration Receipt Card (Form I-551)



UNITED STATES OF AMERICA
PERMANENT RESIDENT

Surname
SPECIMEN

Given Name
TEST V

USCIS#
000-000-001

Category
RE8

Country of Birth
Utopia

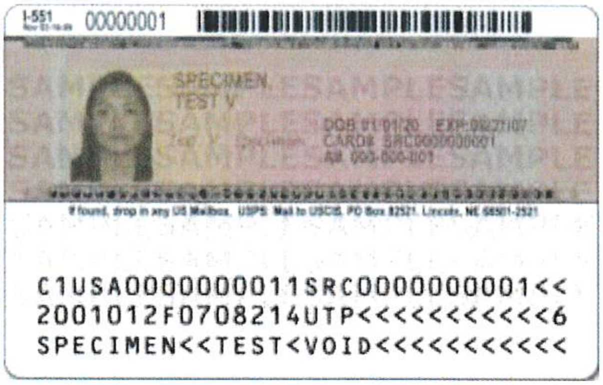
Date of Birth
01 JAN 1920

Sex
F

Card Expires: 08/21/07

Resident Since: 08/21/07

Test V. Specimen



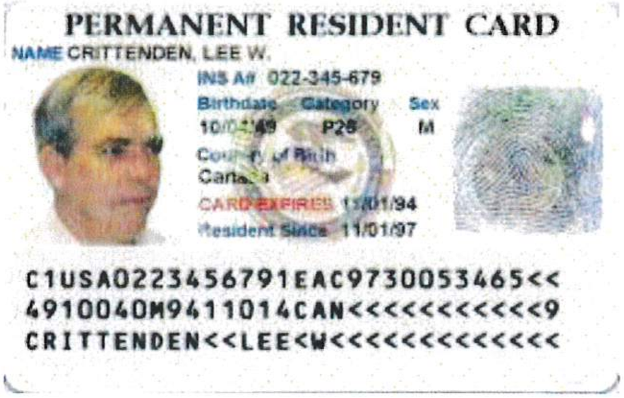
I-551 00000001

SPECIMEN
TEST V

DOB 01/01/20 EXP 08/21/07
CARD# SRC0000000001
A# 000-000-001

If found, drop in any US Mailbox. USPS: Mail to USCIS, PO Box 82521, Lincoln, NE 68501-2521

C1USA0000000011SRC0000000001<<
2001012F0708214UTP<<<<<<<<<<<6
SPECIMEN<<TEST<VOID<<<<<<<<<<<



PERMANENT RESIDENT CARD

NAME CRITTENDEN, LEE W.

INS A# 022-345-679

Birthdate 10/04/49

Category P26

Sex M

Country of Birth Canada

CARD EXPIRES 11/01/94

Resident Since 11/01/97

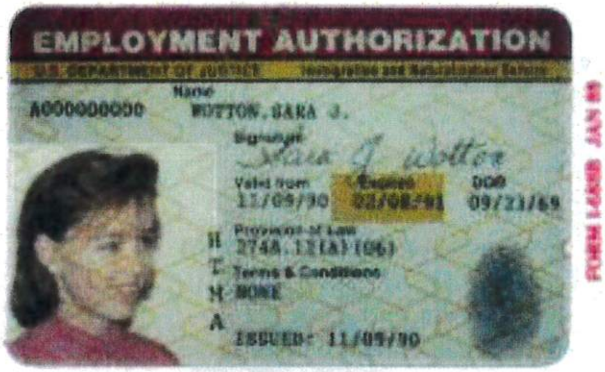
C1USA0223456791EAC9730053465<<
4910040M9411014CAN<<<<<<<<<<<9
CRITTENDEN<<LEE<W<<<<<<<<<<<<<

U.S. DEPARTMENT OF JUSTICE Immigration and Naturalization Service

PERMANENT RESIDENT CARD

The person identified by this card is authorized to work and reside in the U.S.

Employment Authorization Document (Card) with photograph (Form I-688)



EMPLOYMENT AUTHORIZATION

U.S. DEPARTMENT OF JUSTICE Immigration and Naturalization Service

A000000000

Name
WOTTON, SARA J.

Signature
Sara J. Wotton

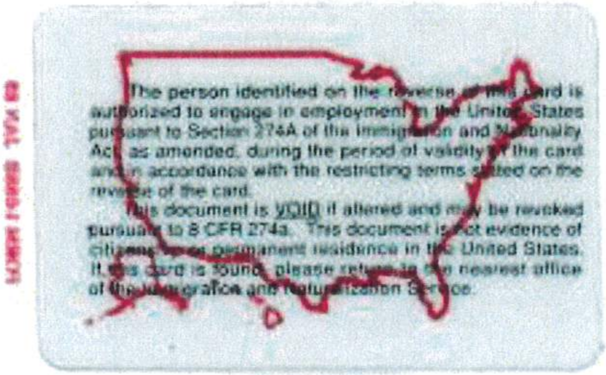
Valid from 11/09/90
Expires 02/08/91
DOB 09/23/69

Provision of Law
274A.12(A)(06)

Terms & Conditions
NONE

ISSUED: 11/09/90

FORM I-688B JAN 89

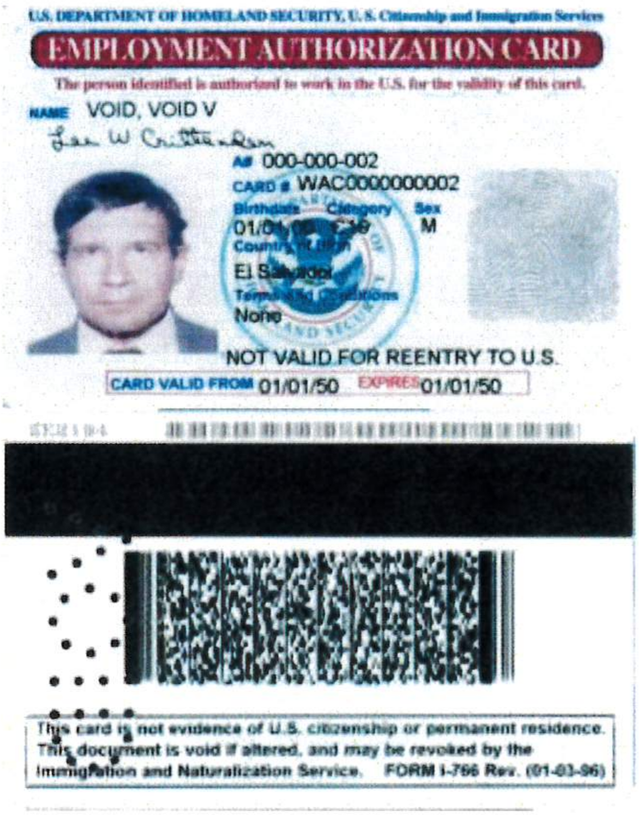


The person identified on the reverse of this card is authorized to engage in employment in the United States pursuant to Section 274A of the Immigration and Nationality Act as amended, during the period of validity of the card and in accordance with the restricting terms stated on the reverse of the card.

This document is VOID if altered and may be revoked pursuant to 8 CFR 274a. This document is not evidence of citizenship or permanent residence in the United States. If this card is found, please return to the nearest office of the Immigration and Naturalization Service.

FORM I-688B JAN 89

Employment Authorization Document (Card) with photograph (Form I-766)



U.S. DEPARTMENT OF HOMELAND SECURITY, U. S. Citizenship and Immigration Services

EMPLOYMENT AUTHORIZATION CARD

The person identified is authorized to work in the U.S. for the validity of this card.

NAME VOID, VOID V

Lee W Crittenden

A# 000-000-002

CARD # WAC0000000002

Birthdate	Category	Sex
01/01/[illegible]	[illegible]	M

Country of Birth

El Salvador

Terms and Conditions

None

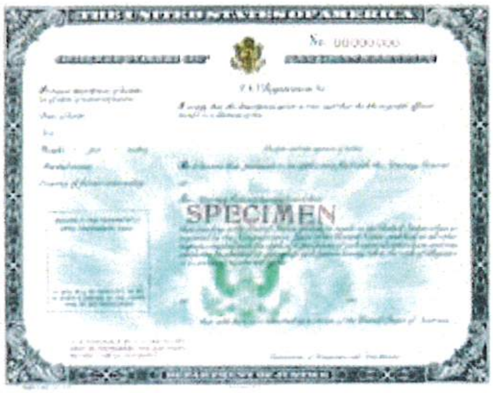
NOT VALID FOR REENTRY TO U.S.

CARD VALID FROM 01/01/50 EXPIRES 01/01/50

[redacted]

This card is not evidence of U.S. citizenship or permanent residence. This document is void if altered, and may be revoked by the Immigration and Naturalization Service. FORM I-766 Rev. (01-03-96)

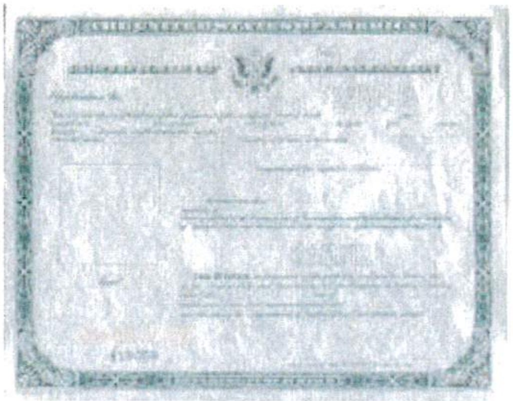
Certificate of naturalization (Form N-550 or N-570)



THE UNITED STATES OF AMERICA

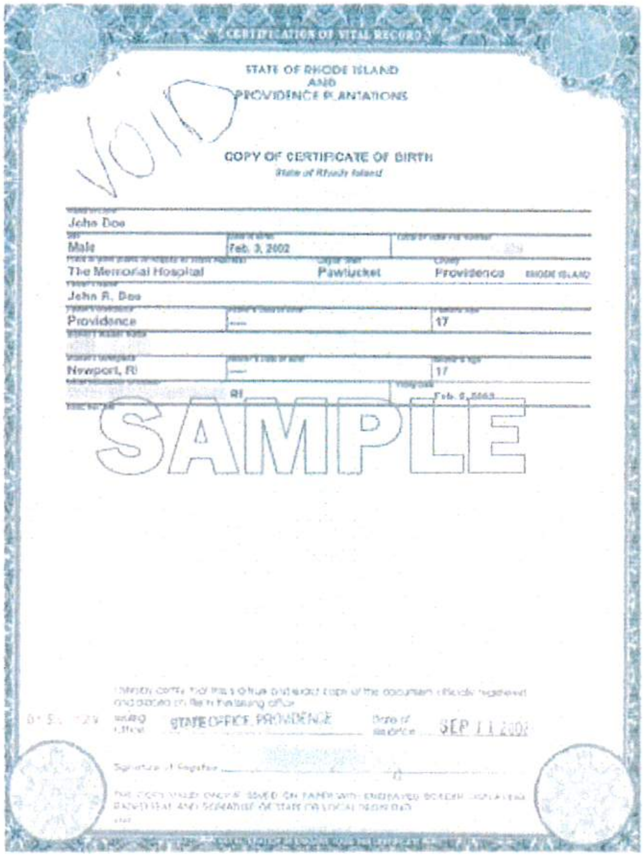
No. 00000000

SPECIMEN



THE UNITED STATES OF AMERICA

Birth Certificate Issues by State



CERTIFICATION OF VITAL RECORDS

STATE OF RHODE ISLAND
AND
PROVIDENCE PLANTATIONS

VOID

COPY OF CERTIFICATE OF BIRTH
State of Rhode Island

John Doe			
Male	Feb. 3, 2002		
The Memorial Hospital	Pawtucket	Providence	RHODE ISLAND
John R. Doe			
Providence	----	17	
Newport, RI	----	17	
RI		Feb. 6, 2002	

SAMPLE

I hereby certify that this is a true and exact copy of the document officially registered and placed on file in the issuing office.

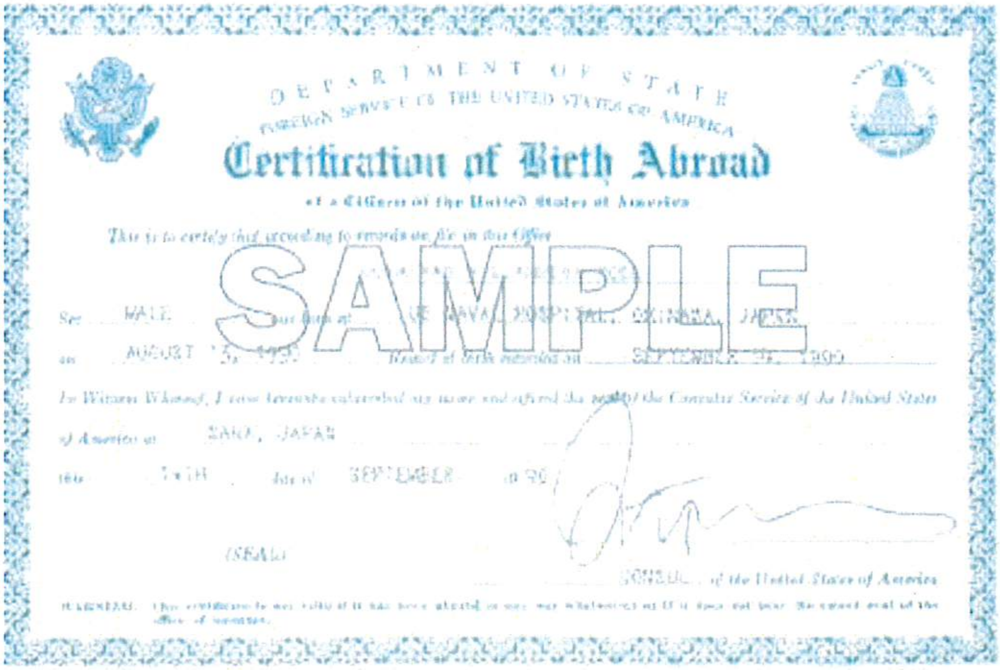
Issuing Office STATE OFFICE, PROVIDENCE Date of Issuance SEP 11 2002

Signature of Registrar

THIS COPY VALID ONLY IF ISSUED ON PAPER WITH ENGRAVED BORDER DISPLAYING RAISED SEAL AND SIGNATURE OF STATE OR LOCAL REGISTRAR

The information contained in this document is proprietary and may not be transmitted or disclosed to anyone outside of the Government or authorized representatives without written permission.

Certification of Birth Abroad Issued by the U.S. Department of State



DEPARTMENT OF STATE
FOREIGN SERVICE OF THE UNITED STATES OF AMERICA

Certification of Birth Abroad

of a Citizen of the United States of America

This is to certify that according to records on file in this Office

[illegible]

Sex MALE was born at US NAVAL HOSPITAL, OKINAWA, JAPAN

on AUGUST 15, [illegible] Report of birth recorded on SEPTEMBER [illegible], 1990

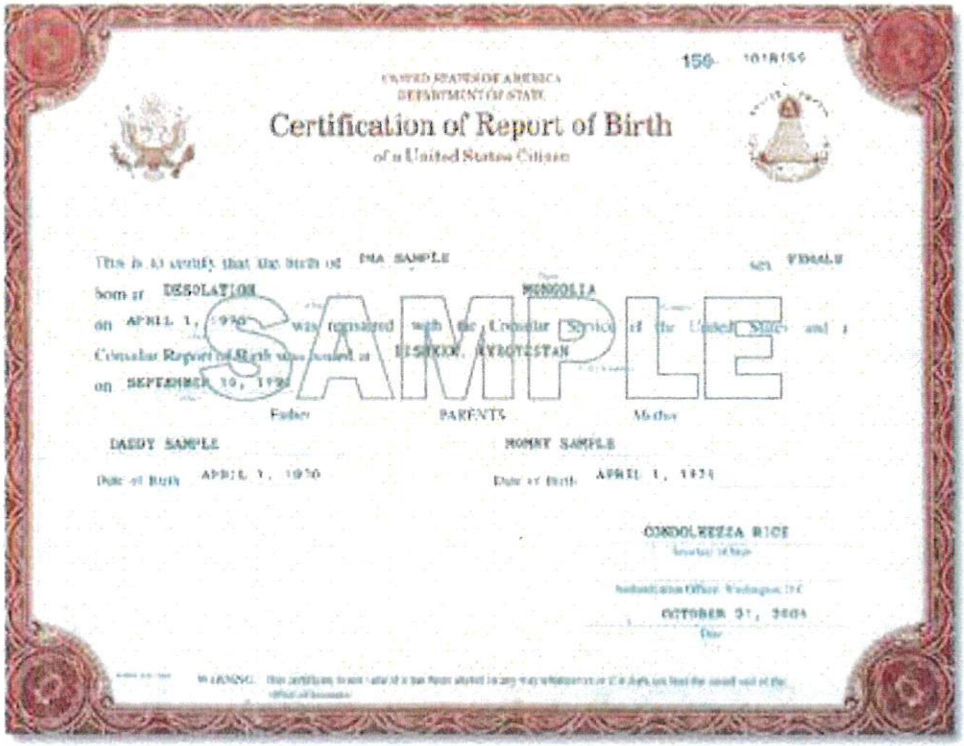
In Witness Whereof, I have hereunto subscribed my name and affixed the seal of the Consular Service of the United States of America at NAHA, JAPAN

this 14TH day of SEPTEMBER 19 90

(SEAL)

CONSUL of the United States of America

WARNING: This certificate is not valid if it has been altered in any way whatsoever or if it does not bear the raised seal of the office of issuance.



150- 1018155

UNITED STATES OF AMERICA
DEPARTMENT OF STATE

Certification of Report of Birth

of a United States Citizen

This is to certify that the birth of IMA SAMPLE sex FEMALE

born at DESOLATION MONGOLIA

on APRIL 1, 1990 was registered with the Consular Service of the United States and a Consular Report of Birth was issued at BISHKEK, KYRGYZSTAN

on SEPTEMBER 10, 1990

Father PARENTS Mother

DADDY SAMPLE MOMMY SAMPLE

Date of Birth APRIL 1, 1930 Date of Birth APRIL 1, 1934

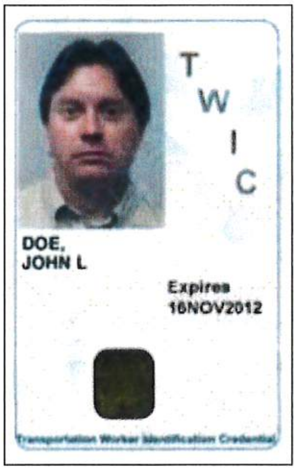
CONDOLEEZZA RICE
Secretary of State

Authentication Office, Washington, D.C.

OCTOBER 31, 2005
Date

WARNING: This certificate is not valid if it has been altered in any way whatsoever or if it does not bear the raised seal of the office of issuance.

TSA Transportation Worker Identification Credential (TWIC)



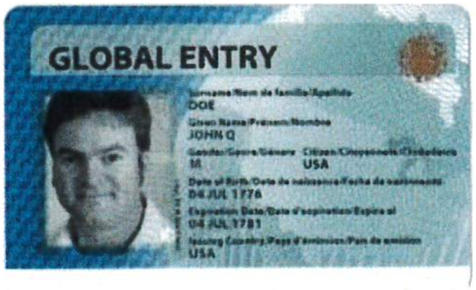
T
W
I
C

DOE,
JOHN L

Expires
16NOV2012

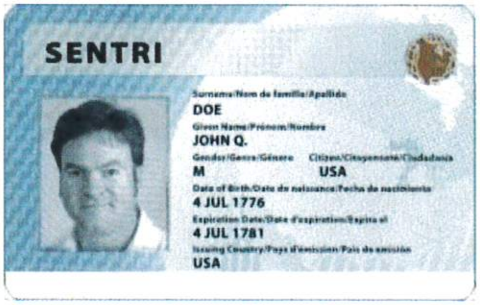
Transportation Worker Identification Credential

DHS Trusted Traveler Cards



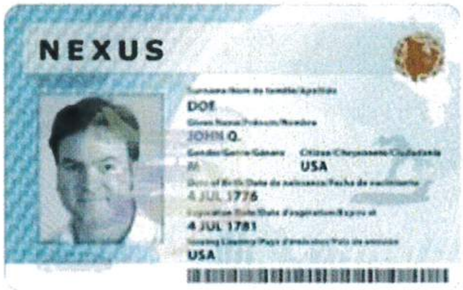
GLOBAL ENTRY

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q
Gender/Genre/Género Citizen/Citoyenneté/Ciudadanía
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
04 JUL 1776
Expiration Date/Date d'expiration/Expira el
04 JUL 1781
Issuing Country/Pays d'émission/País de emisión
USA



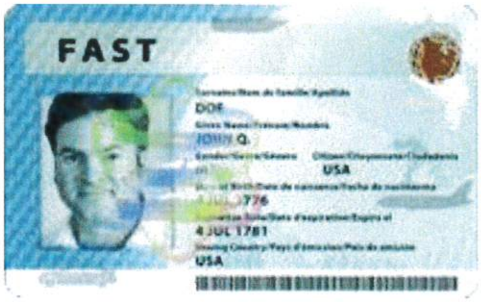
SENTRI

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q.
Gender/Genre/Género Citizen/Citoyenneté/Ciudadanía
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776
Expiration Date/Date d'expiration/Expira el
4 JUL 1781
Issuing Country/Pays d'émission/País de emisión
USA



NEXUS

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q.
Gender/Genre/Género Citizen/Citoyenneté/Ciudadanía
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776
Expiration Date/Date d'expiration/Expira el
4 JUL 1781
Issuing Country/Pays d'émission/País de emisión
USA



FAST

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q.
Gender/Genre/Género Citizen/Citoyenneté/Ciudadanía
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776
Expiration Date/Date d'expiration/Expira el
4 JUL 1781
Issuing Country/Pays d'émission/País de emisión
USA

USACCESS Program

Personal Identity Verification-Interoperable (PIV-I) Credential

WHAT IS A PIV-I CREDENTIAL?

PIV-I is a standards-based credential issued by the USAccess Program to individuals who may not qualify for a PIV card. It provides physical and logical access to Federal buildings and systems when and where Agencies deem appropriate. The enrollment and identity proofing processes for PIV-I are the exact same as the processes used for PIV.

WHO GETS A PIV-I CREDENTIAL?

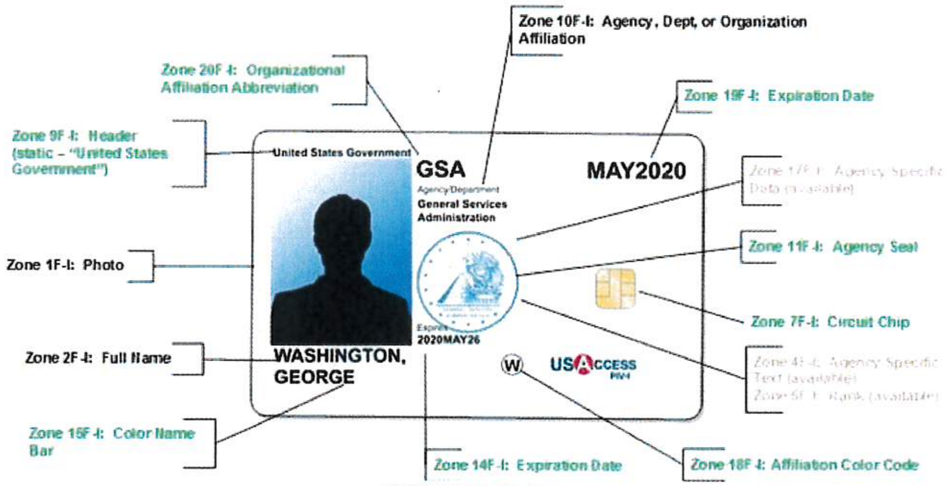
Not all USAccess Customer Agencies have opted-in to use PIV-I, and of those Agencies, only a small subset of Applicants are issued PIV-I credentials. Examples include, but are not limited to, Foreign Nationals who have not been in the country long enough to receive a full background investigation, short-term employees and contractors, or anyone the Agency determines should have a PIV-I credential rather than a PIV credential.

HOW DO I HANDLE ENROLLMENTS/ACTIVATIONS FOR PIV-I CREDENTIALS?

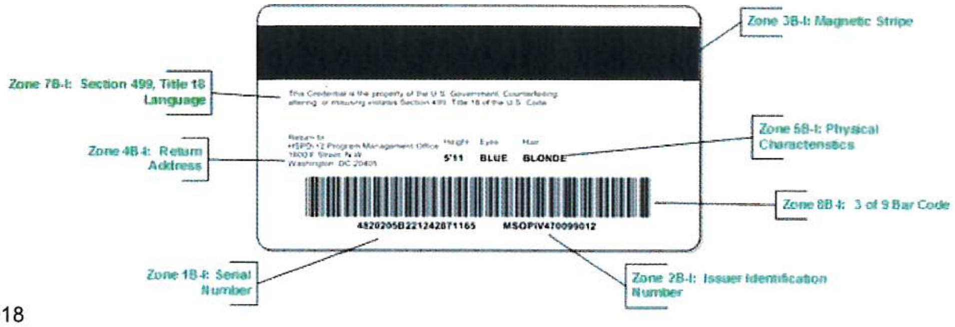
The enrollment and identity proofing processes for PIV and PIV-I are exactly the same. Activators should follow the same process to activate PIV-I cards as they do with PIV cards.

WHAT DOES A PIV-I CREDENTIAL LOOK LIKE?

PIV-I Credential Front


Zone 10F-I: Agency, Dept, or Organization Affiliation
Zone 20F-I: Organizational Affiliation Abbreviation
Zone 19F-I: Expiration Date
Zone 9F-I: Header (static – "United States Government")
United States Government
GSA
Agency/Department
General Services Administration
MAY2020
Zone 17F-I: Agency Specific Data (available)
Zone 1F-I: Photo
Zone 11F-I: Agency Seal
Zone 7F-I: Circuit Chip
Expires
2020MAY26
Zone 2F-I: Full Name
WASHINGTON, GEORGE
W
USACCESS PIV-I
Zone 4F-I: Agency Specific Text (available)
Zone 5F-I: Rank (available)
Zone 15F-I: Color Name Bar
Zone 14F-I: Expiration Date
Zone 18F-I: Affiliation Color Code

PIV-I Credential Back


Zone 3B-I: Magnetic Stripe
Zone 7B-I: Section 499, Title 18 Language
This Credential is the property of the U.S. Government. Counterfeiting altering, or misusing violates Section 499, Title 18 of the U.S. Code.
Zone 5B-I: Physical Characteristics
Zone 4B-I: Return Address
Return to
HSPD-12 Program Management Office
1800 F Street, N.W
Washington, DC 20405
Height
Eyes
Hair
5'11
BLUE
BLONDE
Zone 8B-I: 3 of 9 Bar Code
4820205B221242871165
MSOPIV470099012
Zone 1B-I: Serial Number
Zone 2B-I: Issuer Identification Number

GSA

For more information, please contact your Agency Lead or the GSA MSO: GSAMSO@gsa.gov.

May 2018

Official website of the Department of Homeland Security

U.S. Department of
Homeland Security

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

HSPD 12 Full Text (#)

Homeland Security Presidential Directive-12

August 27, 2004

SUBJECT: Policies for a Common Identification Standard for Federal Employees and Contractors

1. Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of

identification issued by the Federal Government to its employees and contractors (including contractor employees).

2. To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

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. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

4. Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

5. Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of

the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

6. This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

7. Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

8. The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

# # #

COVID-19 Pandemic Temporary Credentialing Procedures (#)

The DHS Office of the Chief Security Officer (OCSO) is committed to protecting our workforce during the COVID-19 pandemic. To support social distancing requirements, OCSO is offering an alternate DHS credential known as a Derived Alternate Credential (DAC) to employees in lieu of a DHS Personal Identity Verification (PIV) credential so that personnel can still gain logical access to the DHS network without visiting a DHS Credentialing Facility (DCF). Personnel who obtain a DAC will have to get a DHS PIV Card later. Additional information can be found on the Security Information and Reference Materials (/publication/security) page.

Additional Resources (#)

Your Credential

Identity management has become an important part of our homeland security since September 11, 2001.The 9/11 Commission Report recommends that all federal employees or contractors be screened with biometric identifiers across all government agencies as a global strategy to protect against terrorist attacks.

The U.S. General Services Administration (GSA) developed the USAccess Program as an efficient way for federal agencies to issue common HSPD-12 approved credentials to their employees and contractors. You will receive a USAccess credential if your agency has elected to participate in the USAccess Program. (You may hear the credential referred to with another name within your agency because some agencies have opted to re-brand their program and credential.)

- Why do I need this card?
- What information about me is stored on this card?
- How does this credential ensure my security?
- Your roles and responsibilities as a credential holder
- Maintaining your USAccess credential
- How to obtain a credential
- Steps to obtain a credential

Most of the contents of this page are also printed in the About The USAccess Credential Guide (/document/about-usaccess-credential?download=1).

Why Do I Need This Card?

As a federal employee or contractor, you may need your USAccess credential in order to gain access to buildings and systems for which you are authorized. Over time, all existing federally issued badges will be replaced with a PIV-compliant credential. Without a PIV credential, you may not be able to enter certain buildings, or will need to be registered as a guest.

What Information about me is Stored on this Card?

The information about you that is stored on your PIV credential includes:

- A printed picture of your face
- Your full name
- Agency and organization with which you are associated
- Credential expiration date
- Credential serial number
- Agency particular data and an issuer identification number
- Your Personal Identification Number (PIN)
- Two electronic fingerprint templates
- Digital certificates

The digital certificates stored on your credential can be used for authenticating your identity, digital signatures, and encrypting email.

How Does This Credential Ensure My Security?

Your credential can ensure your security by allowing you to easily, quickly, and reliably identify yourself to any federal agency using a single credential, as well as, trust the identity of other USAccess credential holders.

Your Roles and Responsibilities as a Credential Holder

As a USAccess credential holder, you have important responsibilities to do your part to safeguard the security of the nation, your fellow employees, and yourself.

1. Safeguard Your PIN:

When activating your card, you will be prompted to select a unique PIN. Your new PIN:

- Must contain 6-8 numbers
- Must not be too simple (e.g., 1234)
- Must not contain number strings (e.g., 4444)
- Must be correctly confirmed

IMPORTANT: Never store your PIN with your USAccess credential or share your PIN with anyone!

2. Report Lost or Stolen Cards Immediately:

Contact your agency's security officer if you have lost your credential or believe it has been tampered with. Your current credential will be terminated, and the process for issuing you a new credential will be initiated.

3. Know Your Privacy Rights:

View the complete directives and policies governing the USAccess Program available on this website and the USAccess Privacy Statement (/document/usaccess-privacy-act-statement?download=1). It is important that you understand how data is collected and stored on your USAccess credential, not only for your security, but also as a reminder of how important it is to protect and safeguard your credential.

Maintaining Your USAccess Credential

It is your responsibility to protect your USAccess credential and exercise the same care with it as you do with other identification credentials. For best protection, please keep your card in your badge holder when not in use.

Other Protective Measures:

- Do not mark on, punch holes in, or bend your credential, as this will void the card warranty and could cause the protective plastic covering to peel away prematurely.
- Do not scratch the magnetic stripe on your credential
- Avoid storing your credential in areas subject to excessive heat (e.g., clothes dryer) or in direct sunlight (e.g. car dashboards) as the card could warp.
- Do not allow the credential near magnetic fields (e.g., stereo equipment, magnets, or other magnetic stripe cards, etc.)

Updating or Rekeying Your Credential Certificates

Your USAccess credential contains digital certificates. The certificates must be renewed 3 years after initial activation to keep your credential active. The start of the 3 year period begins on the day your credential is activated when the certificates are encoded on your card. As the certificate renewal date of your credential nears you will be contacted by email (i.e., 90, 60 and 30 days before expiration) to make an appointment at a nearby enrollment/activation center to update your certificates. If you do not update your certificates your credential will be terminated.

Renewing Your Credential:

Your USAccess credential is active for a period of 5 years. The credential expiration date appears on the front of your credential. As the expiration date of your credential nears, you will be notified by email to make an appointment at a nearby enrollment/activation center to renew your credential.

How To Obtain A Credential

Acceptable Forms of ID

(/document/acceptable-forms-id?download=1)

View a List of
Acceptable Forms of Identification (/document/acceptable-forms-id?download=1)

How and when applicants get their credentials is based on when their agency decides they are eligible to receive them. GSA MSO does not decide when applicants are eligible to receive their credentials. If you have any questions about when you will be receiving your credential, contact your agency's supervisor.

Steps To Obtain A Credential

(/sites/all/themes/gsa_fedidcard/images/legacy/credentialflow_large.gif)

Steps to Achieve
an Active Credential
(select for full image)

The USAccess Program has developed an integrated, end-to-end system to automate and ease the process of issuing a credential to applicants.

The 9 steps to obtain a credential include:

- Step 1: Applicant data is entered into the USAccess system by agency
- Step 2: Applicant received an email invitation to enroll
- Step 3: Applicant schedules an enrollment appointment online
- Step 4: Applicant attends enrollment appointment as scheduled
- Step 5: Agency completes background checks and approves applicant
- Step 6: Applicant receives email that credential is ready for pick up and to make an appointment to activate the credential
- Step 7: Applicant schedules an activation appointment online
- Step 8: Applicant attends appointment and activates credential
- Step 9: Credential is now active and ready to use

Step 1: Applicant data is entered into the USAccess system.

Applicant data such as name, address, date of birth, employee type, and Emergency Response Official (ERO) status is entered into the system by the sponsoring agency. This completes the applicant sponsorship record in the USAccess system.

Step 2: Applicant receives an email invitation to enroll.

The applicant receives an email invitation to enroll in the USAccess Program

- The email lists the applicant's name as it appears in the sponsorship record and asks the applicant to verify that his or her name is correct.
- Next, the email describes how identity documents must match the name. A link is provided to a document outlining the proper forms of identification that applicants must bring with them to their enrollment appointment. (List of Acceptable Forms of ID (/document/acceptable-forms-id?download=1)).
- If the applicant notices that the name in the email is incorrect and does not match any of their other identity documents, the applicant should contact the agency sponsor before going to enroll.
- The email also provides instructions on how to make an appointment to enroll for the credential at a USAccess center. A link to the GSA Online Scheduling System (https://portal.usaccess.gsa.gov/scheduler) (if used by the agency) is provided for applicants to schedule appointments.

Step 3: Applicant schedules an enrollment appointment online.

Using the GSA Online Scheduling System, the applicant makes an appointment (/credential-appointments) to enroll for the USAccess credential.

- The applicant must first create an account in the scheduling system, and then make an appointment at a nearby center. To find an available center nearby, visit Find USAccess Centers (/find-usaccess-centers). Account setup typically takes less than 5 minutes.
- Once the appointment is made, the applicant will receive a confirmation email confirming the date and time of the appointment.
- Before traveling to a USAccess credentialing center for an appointment, the GSA MSO encourages applicants to check the advisory section located near the top of the USAccess website home page, http://www.fedidcard.gsa.gov (/). Occasionally, the system may be experiencing difficulties or a center may be closed and the applicant's appointment may be affected.
- Note: Service Advisories are updated three times daily, so applicants should check for updates before traveling. If an appointment is canceled by the center, an email will be sent to the applicant noting the appointment was canceled and will request the applicant to make a new appointment.

Step 4: Applicant attends enrollment appointment as scheduled.

During the enrollment appointment, the applicant must present proper identification documents (List of Acceptable Forms of ID (/document/acceptable-forms-id?download=1)) to the registrar at the center, have a photo taken, and have fingerprints captured using an electronic fingerprint capturing system. Provided there are no issues during the enrollment process, the appointment typically takes 15-20 minutes.

If the applicant notices that any information in their record is incorrect prior to the appointment, the applicant must contact the agency sponsor (see FAQs on how to locate your Sponsor (/faq/8)). The registrar is not able to make changes to applicant sponsorship record during the enrollment process.

Step 5: Agency completes background checks and approves applicant.

Following a successful enrollment appointment, a background check is conducted on the applicant by the sponsoring agency. Once the background check is completed, the agency adjudicator will record the adjudication decision for the applicant in the USAccess system. When adjudication is complete and approved, the applicant's credential is printed and shipped to the pick up location.

Step 6: Applicant receives email that credential is ready for pick up and to make an appointment to activate the credential.

When the applicant's credential is ready for pickup, the applicant will receive an email explaining where to pick up the credential. The applicant will also be prompted to make an appointment in the GSA Online Scheduling system to activate the credential.

IMPORTANT NOTE: This email may also contain the temporary one time use password that is needed to activate the credential for self-activation. Applicants must bring this password with them to their appointments, or they may experience difficulties during Activation.

Step 7: Applicant schedules an activation appointment online.

Using the GSA Online Scheduling System, (https://portal.usaccess.gsa.gov/scheduler) or other system per agency:

- The applicant makes an appointment to activate their USAccess credential.
- The applicant logs on to the GSA Scheduling System with the account user name and password. If the applicant cannot remember the user name and password created to make an enrollment appointment, a new account can be created.
- Once logged on, the applicant can make an appointment at the center listed in their "Credential Ready for Pick up" email. Account setup typically takes less than 5 minutes.
- Once the appointment is made, the applicant will receive a confirmation email confirming the date and time of the appointment.

NOTE: If your agency has deployed Light Activation stations, you have the opportunity to use one of those locations to have your credential activated. The GSA Online Scheduling System is not used to make appointments at Light Activation stations at this time. Please contact your agency's program management office or check your agency's intranet for information about Light Activation stations available for your use.

Step 8: Applicant attends appointment and activates credential.

The applicant visits an activation station, and activates the credential using Attended or Unattended Activation. Attended Activation is performed by the activator. Applicants are encouraged to attempt activation unassisted. Please see the Unattended Credential Activities Guide (/document/unattended-activation-activities-guide?download=1) for more infomation on how to complete these steps.

During activation, the applicant is prompted for their temporary password. This password is contained in the "Credential Ready for Pick Up" email sent to the applicant. The applicant's credential is then "personalized" with security certificates and the applicant is prompted to create a PIN for the USAccess credential. Applicants will also be prompted to digitally sign a USAccess Privacy Statement (/document/usaccess-privacy-act-statement?download=1) that explains the USAccess credential holder responsibilities. Provided there are no issues in activating the credential, this appointment can take as little as 10 minutes.

Step 9: Credential is now active and ready to use.

USAccess credential holders can now use the credential and should care for their USAccess credential as they would any other valuable form of personal identification. For guidance on how to care for the credential, as well as what information is stored on the credential, view the Your Credential page and the About the USAccess Credential Guide (/document/about-usaccess-credential?download=1) located on this website.

Print This Page (https://www.fedidcard.gov/print/your-credential)
Email This Link (mailto:?
subject=GSA%20USAccess%20Program%3A%20Your%20Credential&body=I%20think%20you%20might%20like%20to%20see%20thi
credential%22%3EYour%20Credential%3C/a%3E)

About (/about-usaccess)

Program Overview (/program-overview)
USAccess Service (/usaccess-service)
Program Benefits (/program-benefits)
FAQs (/faq/1)

Credential Info (/credential-information)

Your Credential (/your-credential)
Credential Features (/credential-features)
Credential Appointments (/credential-appointments)
Credential PIN (/credential-pin)
Find USAccess Centers (/find-usaccess-centers)
FAQs (/faq/8)

COVID-19 information **CLICK HERE** (/important-covid-19-news)

COVID-19 information **CLICK HERE** (/important-covid-19-news)

Agency Resources (/agencies)

COVID-19 information **CLICK HERE** (/important-covid-19-news)

Forms (/customer-forms)
Onboarding Process (/onboarding-process)
Getting Operational (/getting-operational)
Agency Orders and Services (/agency-orders-and-services)
Credentialing Units and Activation Kits (/credentialing-units-and-activation-kits)
Light Activation (/light-activation)
Existing Customer Agencies (/existing-customer-agencies)
FAQs (/faq/5)
COVID-19 News (/important-covid-19-news)

Training (/training-education)

Meeting/Training Calendar (/monthly-meetings-and-trainings)
Web Based Training (/web-based-training)
Registrar Classroom Training (/registrar-classroom-training)

Contact (/contact-information)

MSO Contact Information (/mso-contact-information)
Submit a Question (/submit-question)

U.S. General Services Administration

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. Privacy and Security (/privacy-and-security-notice)

COVID-19 information **CLICK HERE** (/important-covid-19-news)

COVID-19 information **CLICK HERE** (/important-covid-19-news)

COVID-19 information **CLICK HERE** (/important-covid-19-news)