REAL ID Act of 2005 Implementation:

An Interagency Security Committee Guide

August 2015

Interagency Security Committee

This page left intentionally blank.

Message from the Interagency Security Committee Executive Director

One of the Department of Homeland Security's (DHS) priorities is the protection of Federal employees and private citizens who work within and visit U.S. Government-owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS, consists of 54 Federal departments and agencies, and has as its mission the development of security standards and best practices for nonmilitary Federal facilities in the United States.

As Executive Director of the ISC, I am pleased to introduce the new ISC document titled *REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide*. This ISC guide details the purpose and background of the REAL ID Act of 2005 (the Act), and outlines the phased implementation schedule for enforcement. The guide also contains options in accordance with the Act for creating access control procedures, communicating those procedures, and establishing alternate access control procedures if necessary. Lastly, the guide contains appendices which reference information on the Act, a list of acceptable forms of identification, visual references for acceptable forms of identification, and a flow chart aid for developing access control decisions.

Consistent with Executive Order 12977 (October 19, 1995), *REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide* is intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include existing owned, to be purchased, or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities.

This guide represents exemplary collaboration within the ISC working groups and across the entire ISC. ISC primary members approved this guide with full concurrence on June 15, 2015 and will review and update this document as required.

Bernard Holt
Acting Executive Director
Interagency Security Committee

This page left intentionally blank.

Table of Contents

Table of Appendices

Glossary of Terms

Access Control:[1] The use of physical and procedural controls to ensure only authorized individuals or items are given access to a facility or secure area.

Designated Official: The highest ranking official of the primary occupant agency of a Federal facility, or alternately, a designee selected by mutual agreement of tenant agency officials.

Enhanced Driver's License (EDL): State-issued driver's licenses issued in accordance with the Western Hemisphere Travel Initiative (WHTI) that denote identity and U.S. citizenship and are acceptable for entry into the United States at land and sea ports of entry. States currently issuing EDLs to their residents who are U.S. citizens include: Michigan, Minnesota, New York, Vermont, and Washington. For more information on Enhanced Driver's Licenses, please visit the U.S. Customs and Border Control website.

Facility Security Committee (FSC): A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The Facility Security Committee (FSC) consists of representatives of all Federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee (BSC).

Facility Security Level (FSL): A categorization based on the analysis of several security-related factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

Extended Definition: The five factors quantified to determine the FSL are: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies, as well as additional intangible factors.

Federal Facility: Government leased and owned facilities in the United States (inclusive of its territories) occupied by Federal employees for nonmilitary activities.

ID-based Access Control: Policies and practices requiring the presentation, inspection, and acceptance of a visitor's photo identification document for accessing a Federal facility.

Knowledge-based Authentication: A method of authentication which seeks to prove the identity of someone using the knowledge of personal information associated with the asserted identity. It may use information sent to the individual in advance as part of the access control process or use answers to questions generated from a wider base of personal information (e.g., previous addresses) to which the agency has access.

Restricted Area: A Federal facility (or part of a facility) only available to agency personnel, contractors, and their guests. Also referred to as Controlled, Limited, or Exclusion areas.

Semi-restricted Area: A Federal facility (or part of a facility) available to the general public but subject to ID-based access control.

[1] As defined by the ISC in Best Practices for Armed Security Officers in Federal Facilities.

State: One of 56 jurisdictions covered by the Act, which includes the 50 U.S. states, the District of Columbia, and the U.S. Territories of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

State-Issued Card: A driver's license or non-driver identification card issued by a state Department of Motor Vehicles or equivalent office. It does not include identification cards issued by other state agencies, such as an employee ID, hunting license, library card, or student ID.

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
BSC	Building Security Committee
DHS	Department of Homeland Security
DO	Designated Official
DOD	Department of Defense
EDL	Enhanced Driver's License
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ID	Identification
IPC	Interagency Policy Committee
ISC	Interagency Security Committee
OEP	Occupant Emergency Plan
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	United States Coast Guard
WHTI	Western Hemisphere Travel Initiative

1 Purpose

Implementation of the *REAL ID Act of 2005* ("the Act") (P.L. 109-13[2]) creates an opportunity to develop and promote a common set of access control procedures for Federal facilities. This document outlines guidance for Federal departments and agencies, including the Department of Defense (DOD), and Facility Security Committees (FSC), specifically with regards to alternate access control options for individuals who are unable to present a driver's license or identification card issued by a REAL ID compliant state.

2 Background

The Act was enacted to implement the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance…of sources of identification, such as driver's licenses."[3] It established minimum security standards for license issuance and production and assigned responsibility for determining whether a state is meeting these standards to the Department of Homeland Security (DHS). DHS issued the REAL ID regulation on January 29, 2008 and began issuing compliance determinations on December 20, 2012.

The Act prohibits Federal agencies from accepting for official purposes driver's licenses and identification cards from states not meeting the Act's minimum standards. Official purposes defined in the Act and regulations include: accessing Federal facilities, entering nuclear power plants, and boarding Federally regulated commercial aircraft. In early 2013, the National Security Council Staff convened an Interagency Policy Committee (IPC) to develop a plan to ensure that enforcement of the Act's prohibitions is done fairly and responsibly. This plan, announced by DHS on December 20, 2013, defined the initial enforcement phases and established a schedule for their implementation (see Appendix A).

The Act covers 56 jurisdictions, including the 50 states, the District of Columbia, and the U.S. Territories of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

2.1 Current Status

DHS announced on December 20, 2013 a phased enforcement plan for the Act that implements the statutory prohibition on acceptance of driver's licenses and identification cards issued by noncompliant states by Federal agencies for official purposes — that is, entering nuclear power plants, accessing Federal facilities, and boarding commercial aircraft — in a measured, fair, and responsible way. The deployment of enforcement measures is cumulative, with measures in each phase remaining in effect through successive phases.

Phase 1 of enforcement began April 21, 2014, at DHS's Nebraska Avenue Complex headquarters in Washington, D.C.

Phase 2 began on July 21, 2014. This phase applies to restricted Federal facilities (or parts of a facility), which are only accessible to Federal employees, contractors, and their guests. It applies

[2] Public Law 109-13, May 11, 2005 (http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/pdf/PLAW-109publ13.pdf)

[3] National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report." The 9/11 Commission Report. January 1, 2004. Accessed January 1, 2015. http://www.9-11commission.gov/report/911Report.pdf.

to about 217 facilities in the custody and control of the General Services Administration (GSA) – mostly law enforcement agencies and laboratories – as well as many agency headquarters facilities.

Phase 3 applies to "semi-restricted" Federal facilities (or parts of a facility), which are accessible to the general public but subject to ID-based access control. The start date for each facility is based on its Facility Security Level classification, with facilities having a Facility Security Level of 1 or 2 beginning on January 19, 2015 (Phase 3A), and facilities having a Facility Security Level of 3, 4, or 5, as well as military facilities, beginning on October 10, 2015 (Phase 3B).

Subsequent phases, including enforcement for boarding Federally regulated commercial aircraft, will be set following a review and evaluation of the first three phases and will be posted on the DHS website. For further information, please visit the DHS REAL ID Enforcement in Brief.

3 Applicability

The Act only affects access control policies where individuals are required to present an identification document for accessing Federal facilities, entering nuclear power plants, or boarding Federally regulated commercial aircraft. The Act does not require agencies to accept, or individuals to present, identification where it is not required for access (e.g., to enter the public areas of the Smithsonian). The Act also does not prohibit an agency from accepting other forms of identification as alternatives to state-issued driver's licenses or identification cards, such as a passport or military ID card.

The Act's prohibitions do not affect the use of state-issued driver's licenses or identification cards – including licenses and cards from noncompliant states – for purposes unrelated to official purposes as defined in the Act and applicable regulations. For example, the Act's prohibitions do not apply to voting, registering to vote, issuing Homeland Security Presidential Directive 12 (HSPD-12) cards, or for applying for or receiving Federal benefits.

In the access control environment, the purpose for which the ID is required governs whether the Act prohibits an agency from accepting a license or identification card from a noncompliant state. If the reason for the collection is to make an access control decision, the Act applies and licenses from noncompliant states may not be accepted in accordance with the phased enforcement schedule. The Act would not apply for reasons unrelated to the access control decision, such as a mechanism to assure visitor badges are returned or for the accountability of visitors in case of emergency.

4 Access Control

In multi-tenant facilities the FSC (or in a single tenant facility the individual responsible for security decisions) should take into consideration the access needs of the facility's visitors and their purpose for accessing the facility when developing access policies. As there is **no requirement** to produce a REAL ID Act compliant ID to enter a Federal facility for accessing health or life preserving services (including hospitals and health clinics), law enforcement (including participating in law enforcement proceedings or investigations), participating in constitutionally protected activities (including a defendant's or spectator's access to court proceedings, access by jurors or potential jurors), voting or registering to vote, or applying for or receiving Federal benefits, policies developed should not require the visitor to produce an ID for entry. Checking identity documents is least effective when there is no use for that information. It

creates the appearance of security without directly furthering the needs of security. The FSC in multi-tenant facilities, or the Designated Official (DO) in a single tenant facility, should take into consideration the access needs of the facility's visitors and their purpose for accessing the facility when developing access policies. The facility access control policy should be consistent with:

- Interagency Security Committee (ISC) standards;[4]
- The facility's current Facility Security Level (FSL), countermeasures, and security procedures;
- The current occupants, the potential visitors, the volume of visitors, and security staff for tenant agencies;
- Reason for the identification or identity document;
- The facility's Occupant Emergency Plan (OEP) for essential information about facility visitors; and
- Pre-approval and denial access lists.

The access control policy can take appropriate action to preserve access to Federal facilities for activities directly relating to:

- Safety and health or life preserving services (including hospitals and health clinics);
- Law enforcement (including participating in law enforcement proceedings or investigations); and
- Participating in constitutionally protected activities (including access to court proceedings, access by jurors or potential jurors).

4.1 Considerations When Developing Identity Document-based Access Control Procedures

When developing a facility security policy for a Federal facility, the FSC should match security procedures with the threat against the tenant agencies that occupy the facility. Checking identity documents is useful when a tenant agency has a defined use for the resulting information, such as matching against a security watch list or an invitation list. Checking identity documents is least effective when the action does not tie into an overall security strategy.

A common access control use for a validated identity is to match against an inclusion or exclusion list that establishes a visitor's appropriateness to enter the facility. An inclusion list names individuals who have been pre-approved for entry and an exclusion list names individuals who are to be denied entry. The document check provides evidence of the visitor's identity, enhancing the effectiveness of inclusion or exclusion lists. Similarly, the Transportation Security Administration (TSA) has a need to validate a traveler's identity at an airport checkpoint by comparing the traveler with information on their identity document and matching it with the biographical information submitted upon purchase of the ticket.

The type of identification document to be accepted depends on the level of assurance that the agency needs to have about the validity of the visitor's identity. The level of assurance of a particular identity document depends on the process used by the issuer of the document to

[4] Interagency Security Committee standards can be accessed or requested at the ISC website, http://www.dhs.gov/isc.

authenticate the document holder's identity as part of its issuance. For example, in issuing a Personal Identity Verification (PIV) card, Federal agencies use a standardized process that provides the high identity assurance appropriate to be able to access Federal information systems and Federally controlled facilities.

Where additional assurance of identity is needed, an agency should consider enacting policies to check the identity document for signs of fraud or tampering, and provide the checker with training in fraud detection techniques and/or tools (e.g., magnifying devices and black lights) to assist in determining the validity of the documents presented.

4.2 Communicating Access Control Procedures

Agencies are encouraged to make information about access control procedures readily available to visitors in order to avoid confusion and facilitate access by helping to ensure that visitors have appropriate identification upon their arrival. It is a best practice to make this information available through multiple channels in order maximizes its exposure to visitors. The contents do not need to be all inclusive but should include, at a minimum, the most commonly accepted identity documents and a general statement of what the visitors should expect if they are unable to produce an acceptable identity document. See Appendix E for a sample.

- **Standardized Language** – To the extent possible, agencies should standardize the language used about identification requirements for visitors to a Federal facility. For example:

  "[AGENCY] requires visitors to present government-issued identification for access to its facilities. For visitors presenting a state-issued driver's license or identification card, [AGENCY] only accepts such documents if they are issued by states that are REAL ID compliant. If the state that issued your license is listed as noncompliant to facilitate access please bring an alternate form of government-issued photo ID – such as a passport or Federal employee, military, or veteran identification card."

- **Communication Materials** – DHS and GSA have electronic files for posters and handouts available for agencies to use at access control points to inform visitors of REAL ID-related access control requirements. Obtain more information on the DHS website.

- **Web-based Information** – Agencies are encouraged to post access control requirements on their public web page as a reference to individuals planning to visit their facilities. For example, TSA has a web page informing travelers of many forms of identity documents that it accepts at airport security checkpoints.

4.3 Alternate Access Control Options

Alternate access control procedures may include, but are not limited to, the following (subject to adoption by the implementing Federal agency, FSC, or DO):

- The agency may choose to establish a list of identification documents that it will accept for access control purposes as an alternative to a state-issued driver's licenses or identification cards (See Appendix B and C).

- The visitor may be listed in an appointment book and the guard can call the agency point of contact for access and escort without having to present identification.

- The agency may escort a visitor presenting a driver's license or identification card from a noncompliant state or who is otherwise unable to present an acceptable form of ID.
- The agency may use a form of knowledge-based authentication, where available.

See Appendix D for a flow chart for applying these policies.

4.4 Reporting Requirements

Your agency should also have a process for recording the number of encounters of individuals presenting driver's licenses from noncompliant states for purpose of accessing Federal facilities. This data should be sent monthly to DHS (OSIIS@hq.dhs.gov) for collection no later than the tenth day of each month. DHS will use this data to evaluate the impact of REAL ID enforcement on the public.

See Appendix E for a sample report template.

5 References

- The REAL ID Act of 2005: http://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf (Title II of Division B of Pub. L. 109-13, 49 U.S.C. § 30301)
- REAL ID Regulation (6 CFR Part 37) and amendments: http://www.dhs.gov/secure-drivers-license-documentation
- REAL ID Act Phased Enforcement Plan: http://www.dhs.gov/real-id-enforcement-brief
- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard – August 2013: http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf

6 Interagency Security Committee Participants

Interagency Security Committee
Bernard Holt
Acting Executive Director

Working Group Chair
Ted Sobel
Office of Policy
Department of Homeland Security

Interagency Security Committee Representatives
Tony Evernham
Megan Drohan
Kyle Macken

Working Group Participants

Sue Armstrong
Federal Protective Service

Selden Biggs
Office of Policy
Department of Homeland Security

Denis Brady
Nuclear Regulatory Commission

Gregory Brock
National Labor Relations Board

Jeff Campbell
Environmental Protection Agency

Maggie Dugan
General Services Administration

Laura Forest
U.S. Citizenship and Immigration Service

Mark Hartz
Administrative Office of the U. S. Courts

Bernie Minakowski
General Services Administration

Elizabeth Newman
Department of Justice

Donna Rivera
Department of Defense

Nicholas Schnare
Department of Commerce

Paul Stevens
Federal Bureau of Investigations

Matt Weese
Federal Protective Service

Appendix A: REAL ID Implementation Phases

The full phased enforcement plan for REAL ID and a list of compliant and noncompliant states may be found on the DHS website. As the list of states is subject to periodic revisions, the most recent version can always be found at the above site.

Phase	Enforcement	Notification Period	Full Enforcement
1	Restricted areas for DHS/NAC	1/20/14	04/21/14
2	Restricted areas for all Federal facilities & for nuclear power plants	04/21/14	07/21/14
3	Semi-restricted areas for all Federal facilities		
3a	Facility Security Levels 1 and 2	10/20/14	01/19/15
3b	Facility Security Levels 3, 4, and 5, and military facilities	07/13/15	10/10/15
2015 Review and Evaluation			
4	Aircraft (Acceptable with 2nd form of ID)	No sooner than 2016	

Appendix B: List of Acceptable Forms of Identification

Each agency may determine which identification documents it will accept for the purpose of accessing its facilities based on the facility's risk-profile. The REAL ID Act only applies to the circumstances when an agency may accept a state-issued driver's license or identification card.

The ISC recommends that agencies accept a Federal, state, or foreign government issued identification card containing a photograph, first and last name, expiration date, and any additional elements that the agency uses in its verification processes, but also do not have visible signs of tampering. ISC recommends a preference be given to documents that have not expired, in particular for facilities at greater risk such as facilities designated at Facility Security Level 3 or greater.

The ISC, in the interest of promoting consistent policies across the Federal Government, provides the following list of possible forms[5] of identification to assist agencies in setting their facility's access control policies. This list is neither authoritative nor exhaustive.

1) Federally-issued Identification
    a. U.S. Passport
    b. U.S. Passport Card
    c. PIV or Federally-issued Personal Identification Verification – Interoperable (PIV-I) Cards
    d. Driver's License issued by the U.S. Department of State
    e. Border Crossing Card (Form DSP-150)
    f. DHS "Trusted Traveler" Cards (Global Entry, NEXUS, SENTRI, FAST)
    g. U.S. Military ID (all members of the U.S. Armed Forces [including retirees and dependent ID card holders]) and veterans. (Visit the Department of Defense's Common Access Card website for more information)
    h. Veterans Health Identification Card issued by the U. S. Department of Veterans Affairs
    i. U.S. Permanent Resident Card (Form I-551)
    j. U.S. Certificate of Naturalization or Certificate of Citizenship (Form N-550)
    k. Employment Authorization Document issued by DHS (Form I-766)
    l. U.S. Refugee Travel Document or other travel document or evidence of immigration status issued by DHS containing a photograph (Permit to Re-enter Form I-327 and Refugee Travel Document Form I-571)

[5] The intent of this list is to provide options for consideration regarding acceptable forms of identification. Ultimately, the FSC and/or Security Organization should determine which of these would be acceptable at the facility based on the facility's purpose, department/agency mission, facility security level, and required level of protection.

m. Transportation Worker Identification Credential (TWIC)

n. Merchant Mariner Card issued by DHS/United States Coast Guard (USCG)

2) State-issued Identification

o. A driver's license or identification card issued by a state that meets the REAL ID standards or has an extension

p. State-issued EDLs (https://help.cbp.gov/app/answers/detail/a_id/1269/~/what-is-an-enhanced-drivers-license-(edl)%3F)

q. State prisoner identification cards

r. Interim Driver's License[6] issued by a state that meets the REAL ID standards or has an extension

3) Other

s. Native American Tribal Photo ID

t. Foreign government-issued passport

u. PIV-I cards (issued by non-Federal Government entities)

Facilities may also consider the following higher risk identity documents, which may be appropriate for facilities with a low risk profile or that have relationship with the issuing body that mitigate the risk of fraud.

v. Identification card issued by local government (including county or city) and containing a photograph, name, and expiration date

w. University, library or school card containing a photograph, name, and expiration date

x. Any identification that is not state-issued, but deemed acceptable by the FSC or DO

[6] This form of identification will not have a photograph of the individual.

Appendix C: Images of Acceptable Forms of Identification

1) Federally-issued Identification

a) U.S. Passport

1994 Version

1998 Version

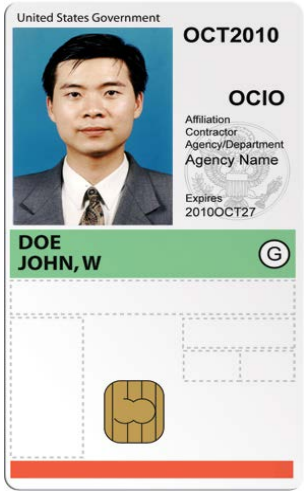
Chip Symbol

b) U.S. Passport Card

Figure 1: Front of Sample U.S. Passport Card

Figure 2: Back of Sample U.S. Passport Card

c) PIV or Federally-issued PIV-I Cards

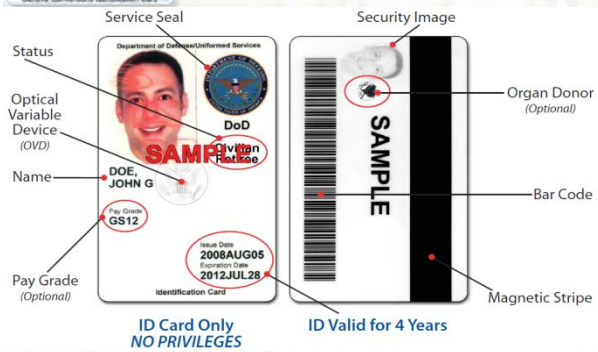


d) Driver's license issued by the U.S. Department of State

e) Border Crossing Card (Form DSP-150)

f) Department of Homeland Security "Trusted Traveler" Cards (Global Entry, NEXUS, SENTRI, FAST)

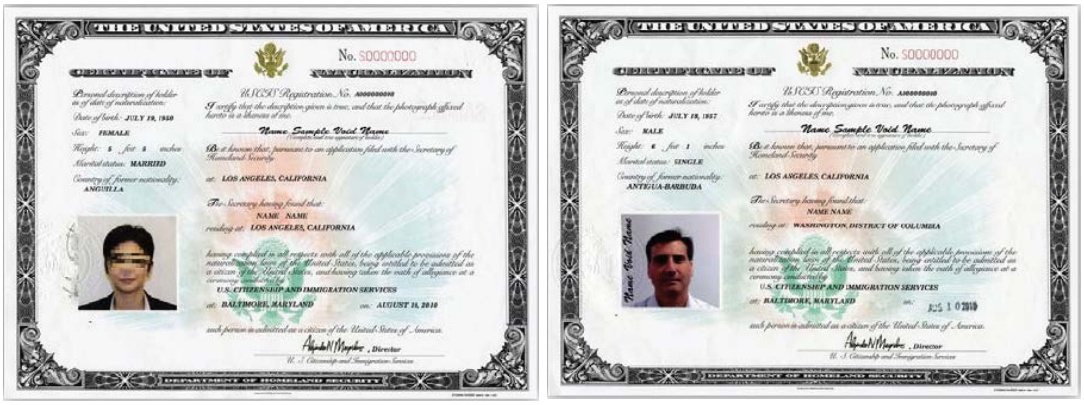
g) U.S. Military ID



h) Veteran's Health Identification Card issued by the U.S. Dept. of Veterans Affairs

i) U.S. Permanent Resident Card (Form I-551)

j) U.S. Certificate of Naturalization or Certificate of Citizenship (Form N-550)



k) Employment Authorization Document issued by Department of Homeland Security (Form I-766)

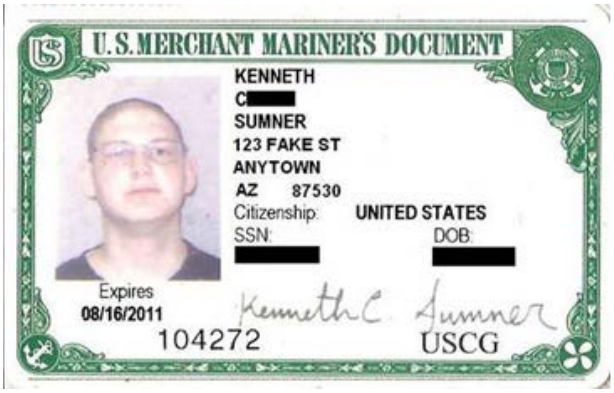
l) U.S. Refugee Travel Document or other travel document of immigration status issued by DHS containing a photograph (Forms I-327 and I-571)

Permit to Re-Enter / Form I-327

Refugee Travel Document / Form I-571

m) TWIC

n) Merchant Marine Card issued by DHS/USCG



2) **State-issued Identification**

p) **State-issued EDLs, which are issued by:**

i) **Michigan**

ii) **Minnesota**

iii) **New York**

iv) Vermont

v) Washington

3) Other

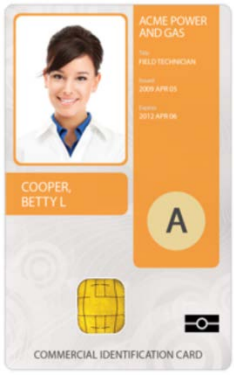
s) Native American Tribal Photo ID Samples

t) Foreign government-issued Passport

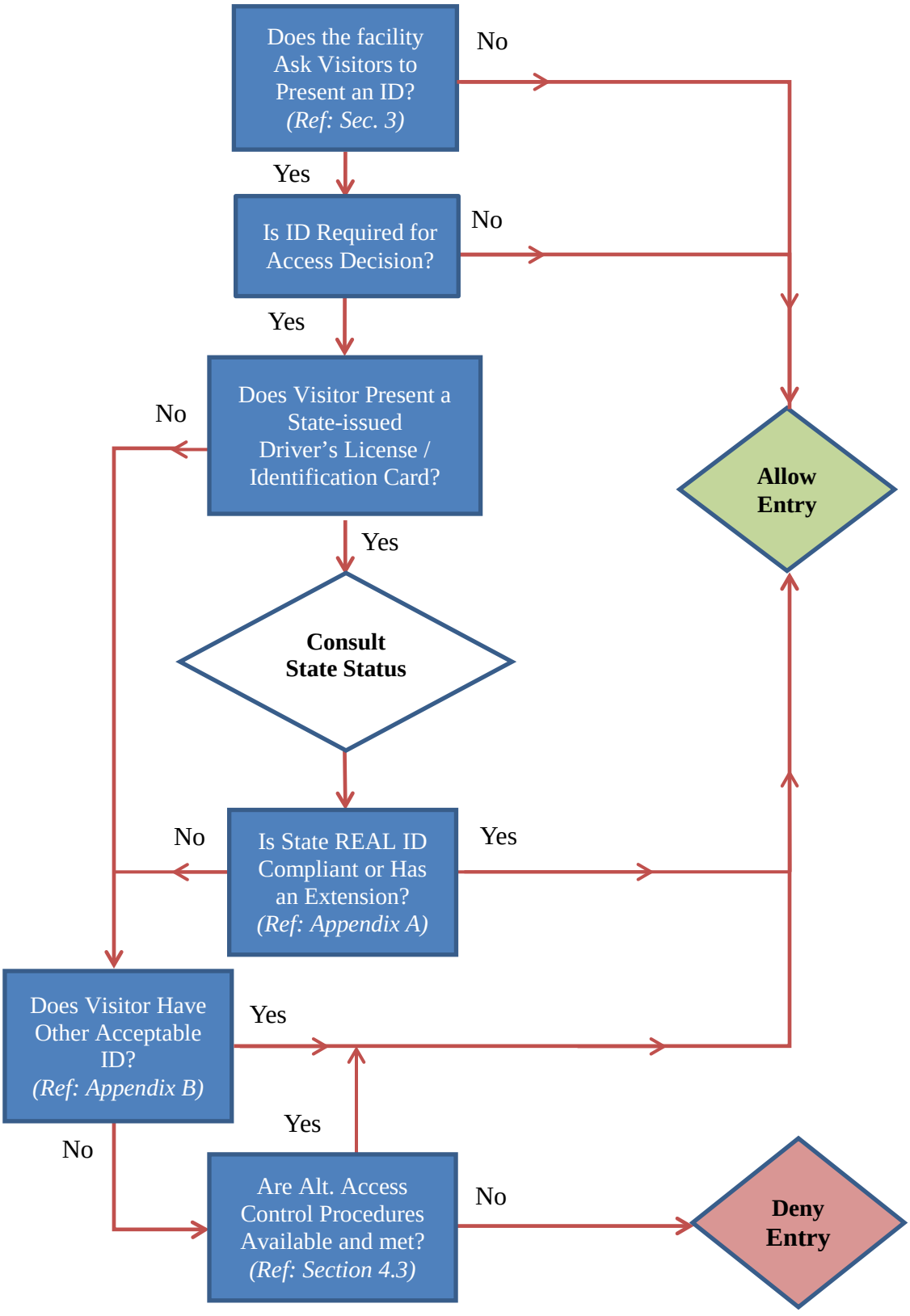
Upon endorsement serves as temporary I-551 evidencing permanent residence for 1 year

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

u) PIV-I cards (issued by non-Federal Government entities)



Appendix D: Flow Chart for Access Control Decision



Appendix E: Sample Report*

Real ID Implementation Tally

	Contact Information				Count								
	Agency	Facility	POC	POC Email	AZ	LA	ME	MN	NY	OK	WA	AM. SAMOA	TOTAL
Jan-15													
Feb-15													
Mar-15													
Apr-15													
May-15													
Jun-15													
Jul-15													
Aug-15													
Sep-15													
Oct-15													
Nov-15													
Dec-15													
Total													

* Data reporting requirements in this sample report were current as of the date this guide was developed. Adjustments will be required as reporting requirements (e.g., list of non-compliant states) change.