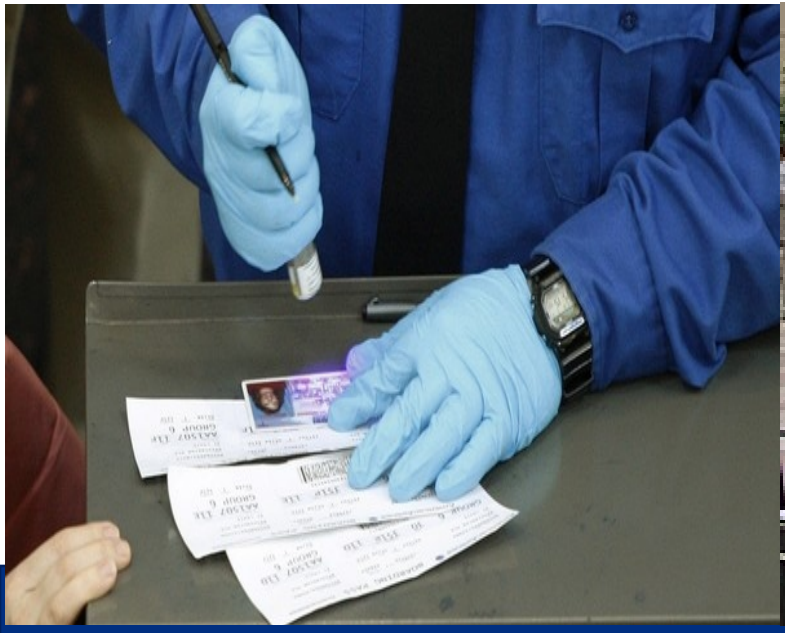

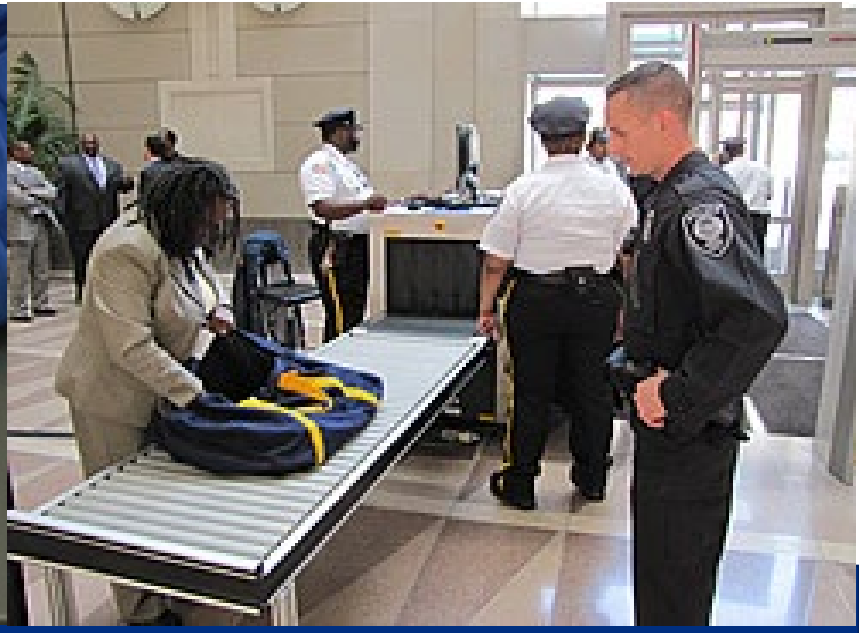

REAL ID Act of 2005 Implementation:

An Interagency Security Committee Guide

2019

Interagency Security Committee

Revision History

Year	Changes	Approver
2015	Initial issue	ISC
2017	Added definitions; Updated Phase 4 implementation guidelines; Updated the internet link to the REAL ID information page; Deleted Appendix E: Sample Report	ISC
2019	Document updated per DHS REAL ID Program Office	ISC

Message from the Chief, Interagency Security Committee

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

As Chief of the ISC, I am pleased to introduce the updated 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 that reference information on the Act, a list of recommended acceptable forms of identification, and a flow chart aid for developing access control decisions.

Consistent with Executive Order 12977 (October 19, 1995), which established the Interagency Security Committee, the *REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide* applies to all buildings and facilities in the US occupied by federal employees for nonmilitary activities. These include existing owned, to be purchased, or leased facilities; standalone facilities; federal campuses; individual facilities on federal campuses; and special-use facilities.

Daryle Hernandez
Chief, Interagency Security Committee

This page intentionally left blank.

Table of Contents

Table of Appendices

1.0 Purpose

This document outlines guidance for federal departments and agencies, including the Department of Defense (DoD) and Facility Security Committees (FSCs), regarding access control requirements of the REAL ID Act ("the Act") and access control options for individuals who do not have an acceptable form of identity document.

2.0 Background

The REAL ID Act of 2005 was enacted in response to a 9/11 Commission recommendation that the federal government "set standards for the issuance […] of sources of identification, such as driver's licenses."[1] The Act 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. The official purposes defined in the Act and regulations are as follows:

- 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 to develop a plan to ensure that enforcement of the Act's prohibitions is done fairly and responsibly. This plan, announced 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 US states, the District of Columbia, and the US territories of Puerto Rico, the US Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

2.1 Current Status

On December 20, 2013, DHS announced a phased enforcement plan to implement the statutory prohibition on the ability of federal agencies to accept driver's licenses and identification cards issued by noncompliant states by federal agencies for official purposes. The deployment of enforcement measures is cumulative, with measures in each phase remaining in effect through successive phases.

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

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

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 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 public but subject to ID-based access control. The start date for each facility is based on its Facility Security Level (FSL) classification. Facilities with an FSL of 1 or 2 began on January 19, 2015 (Phase 3A). Facilities with an FSL of 3, 4, or 5, as well as military facilities, began on October 10, 2015 (Phase 3B).

Phase 4A, enforcement for boarding federally regulated commercial aircraft, based on the compliance status of the state/territory, began on January 22, 2018.

Phase 4B, enforcement for all official purposes, based on the compliance status of the card, begins on October 1, 2020. For more information, please visit https://www.dhs.gov/real-id.

3.0 Applicability

The Act only affects access control policies where individuals are required to present an identification document for official purposes. 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). Nor does it prohibit an agency from accepting other forms of identification such as a US 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 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 state license or identification card from a noncompliant state without an extension. If the reason for requiring an identification document is to make an access control decision, the Act applies and licenses or identification cards from noncompliant states may not be accepted for official purposes 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 an emergency.

4.0 Access Control

When developing access policies, 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. Checking identity documents is least effective when there is no use for identity information. Unnecessary ID checks create the appearance of security without directly furthering the needs of security. The facility access control policy should be consistent with:

- Interagency Security Committee (ISC) standards;[2]
- The facility's current FSL, countermeasures, and security procedures;
- The current occupants, potential visitors, volume of visitors, and security staff for tenant agencies;
- The 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 recommend appropriate action (see Section 4.3) to preserve access to federal facilities for purposes unrelated to the official purposes as defined in the Act and applicable regulations, such as:

- Safety and health or life-preserving services (including responding to an emergency and accessing hospitals and health clinics for health services and access to benefits);
- Law enforcement (including responding to an emergency, conducting investigations, and participating in law enforcement proceedings); and
- Participating in constitutionally protected activities (including access to court proceedings, including 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. 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 identifies people who have been pre-approved for entry. An exclusion list identifies people who

[2] Interagency Security Committee Standards are available on the ISC website: https://www.dhs.gov/isc

should 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 acceptable identification document depends on the level of assurance the agency requires about the validity of the visitor's identity. The level of assurance of an identity document depends on the process used by the issuer of the document to 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 to maximize 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.

- **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 or have an extension from the US Department of Homeland Security. If the state that issued your license is listed as noncompliant without an extension, please bring an alternate form of government-issued photo ID—such as a passport, Enhanced Driver's License (EDL), or federal employee, military, or veteran identification card—to facilitate access."

- **Communication Materials:** DHS and TSA have electronic files for posters and handouts available for agencies to use at access control points to inform visitors about

REAL ID-related access control requirements. Agencies may obtain more information about these requirements at https://www.dhs.gov/real-id and https://www.tsa.gov/real-id.

- **Web-based Information:** Agencies are encouraged to post access control requirements on their public website as a reference to individuals planning to visit their facilities. For example, TSA has a website informing travelers about the forms of identity documents that it accepts at airport security checkpoints. This page is available at https://www.tsa.gov/traveler-information/acceptable-ids.

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, including state-issued driver's licenses or identification cards. (See Appendix B.)
- The visitor may be listed in an appointment book so that the guard can call the agency point of contact for access and escort without having to present identification.
- The agency may use a form of knowledge-based authentication, where available.

See Appendix C for a flow chart to apply these policies.

5.0 References

5.1 Glossary of Terms

Access Control: The use of physical and procedural controls to ensure only authorized individuals or items are given access to a facility or secure area.[3]

Designated Official (DO): The highest-ranking official of the primary occupant agency of a federal facility or a designee selected by agreement of tenant agency officials.

Enhanced Driver's License (EDL) or Enhanced Identification Card (EIC): State-issued driver's license or identification card issued in accordance with the Western Hemisphere Travel Initiative (WHTI) that denotes identity and US citizenship and that is acceptable for entry into the US at land and sea ports of entry. States currently issuing EDLs and EICs to their residents who are US citizens include: Michigan, Minnesota, New York, Vermont, and Washington. For more information, please visit: https://www.dhs.gov/enhanced-drivers-licenses-what-are-they

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 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).

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 additional intangible factors.

Federal Facility: Government leased and owned facilities in the US (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 based on knowledge of personal information associated with the asserted identity. This may involve the use of 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.[4]

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

[4] Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, *Digital Identity Guidelines*. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

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

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

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

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

5.1.1 Glossary of REAL ID Compliance Terms

Compliant States/Territories: States/territories that are compliant with the REAL ID Act.

Noncompliant States/Territories with Extension: States/territories that have been found noncompliant with the REAL ID Act but have a current valid extension from DHS.

Grace Period States/Territories: The period following the expiration of an extension or determination of noncompliance during which federal agencies may continue to accept licenses and identification cards for official purposes. At the end of the grace period, federal agencies may no longer accept licenses and identification cards from the noncompliant state or territory without an extension.

5.2 List of Acronyms/Abbreviations/Initializations

Term	Definition
DHS	Department of Homeland Security
DO	Designated Official
DoD	Department of Defense
EDL	Enhanced Driver's License
EIC	Enhanced Identification Card
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
ISC	Interagency Security Committee
NAC	Nebraska Avenue Complex
OEP	Occupant Emergency Plan
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
US	United States
USCG	United States Coast Guard
WHTI	Western Hemisphere Travel Initiative

5.3 Resources

- The REAL ID Act of 2005: https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf
- REAL ID Regulation (6 Code of Federal Regulations [CFR] Part 37) and amendments: https://www.ecfr.gov/cgi-bin/text-idx?SID=daf01a89f25874673f2ebc305f63cffc&mc=true&tpl=/ecfrbrowse/Title06/6cfr37_main_02.tpl
- REAL ID Enforcement: https://www.dhs.gov/real-id
- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard: https://www.dhs.gov/publication/isc-risk-management-process

6.0 ISC Working Group Participants (Initial Edition)

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 at https://www.dhs.gov/real-id. As the list of states is subject to periodic revisions, the most recent version can always be found on this website and is not listed in this document.

Phase	Enforcement	Full Enforcement Date
1	Restricted areas for DHS/Nebraska Avenue Complex (NAC)	2014-04-21
2	Restricted areas for all federal facilities and nuclear power plants	2014-07-21
3	Semi-restricted areas for all federal facilities	N/A
3a	FSLs 1 and 2	2015-01-19
3b	FSLs 3, 4, and 5 and military facilities	2016-10-10
4a	TSA airport security checkpoints (state-based enforcement)	2018-01-22
4b	Card-based enforcement for all official purposes (Phases 1-4a). State-issued license or ID card must be REAL ID-compliant.	2020-10-01

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 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 or foreign government-issued passport containing a photograph, first and last name, expiration date, and any additional elements the agency uses in its verification processes. The ISC does not recommend accepting a document if it has visible signs of tampering. The ISC recommends that preference be given to documents that have not expired, particularly for facilities at greater risk, such as facilities designated at FSL 3 or greater.

In the interest of promoting consistent policies across the federal government, the ISC 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. US Passport

    b. US Passport Card

    c. PIV or federally issued Personal Identification Verification – Interoperable (PIV-I) Card

    d. Driver's License issued by the US Department of State

    e. Border Crossing Card (Form DSP-150)

    f. DHS "Trusted Traveler" Card (Global Entry, NEXUS, SENTRI, FAST)

    g. US Military ID (All members of the US Armed Forces, including retirees and dependent ID card holders, and veterans. Visit the DoD's Common Access Card website for more information: https://www.cac.mil)

    h. Veteran Health Identification Card issued by the US Department of Veterans Affairs

    i. US Permanent Resident Card (Form I-551)

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

[5] This list is intended 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, FSL, and required level of protection.

k. Employment Authorization Document issued by DHS (Form I-766)

l. US Refugee Travel Document or other travel document or evidence of immigration status issued by DHS and containing a photograph (Permit to Reenter Form I-327 and Refugee Travel Document Form I-571)

m. Transportation Worker Identification Credential (TWIC)

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

2. State-Issued Identification

o. A driver's license or identification card issued by a REAL ID-compliant state or a noncompliant state that has been granted an extension. Beginning October 1, 2020, only REAL ID-compliant cards issued by a compliant state will be accepted.

p. State-issued EDL: https://www.dhs.gov/enhanced-drivers-licenses-what-are-they

q. State prisoner identification card

3. Other

r. Federally Registered Native American Tribal Photo ID

s. Foreign government-issued passport

t. PIV-I card 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 a relationship with the issuing body that mitigates the risk of fraud.

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

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

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

Appendix C: Flow Chart for Access Control Decision