



AIRPORTS SECURITY OFFICE

✈ NATIONAL AVIATION DAY AUGUST 19TH

Effective May 7, 2025.

You must have a REAL ID or acceptable alternative to avoid delays at airport security checkpoints.

BE YOUR **REAL ID** SELF
BY MAY 7, 2025
See tsa.gov for additional information.

LOOK FOR THE STAR

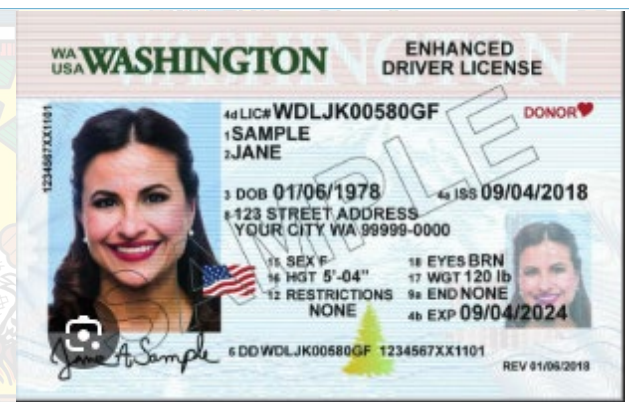


In general, a REAL ID features a star in the upper right or left corner.

REAL ID & the Alternative

Congress passed the REAL ID Act in 2005 that set standards on the issuance of sources of ID establishing minimum security standards for state-issued driver's licenses and ID cards. This prohibits certain federal agencies from accepting (for official purposes) licenses and ID cards from states not meeting the minimum standards. Thus, the need for a REAL ID or alternative when going through airport security checkpoints.

See TSA website for more info:
<https://www.tsa.gov/real-id/real-id-faqs>.



The Alternative: Did you know there is something that can be used in place of the REAL ID "gold star" that TSA approved for a few states? It is the Enhanced Driver's License (EDL).

It must have the word ENHANCED on the ID for validity, have a chip, a symbol of the US Flag, and a machine-readable zone (MRZ). States offering EDLs are Michigan, Minnesota, New York, Vermont, and Washington.

See TSA website for acceptable ID:
<https://www.tsa.gov/travel/security-screening/identification>. **Page 1**

CONTENTS

Editorial Series: Cybersecurity Coordinator	3
Equipment Safety: ULD	4
HNL Airport App – Did you know?	5
HNL Security Procedures: Vehicle Access	5
LIH Conducts Emergency TTX	2
National Internet Safety Month: June	2
New Location: HNL Overnight Passenger	4
Personal Safety: Stay Alert	4
REAL ID & The Alternative	1

**OFFICES CLOSED*:**

**SATURDAY, SUNDAY
AND UPCOMING STATE
HOLIDAYS**

*Closures may vary by office.

August 15, 2025 – Statehood Day
September 1, 2025 – Labor Day
November 11, 2025 – Veterans' Day
November 27, 2025 – Thanksgiving

**OAHU (HNL) – PASS AND ID
OFFICE**

Phone: (808) 836-6427

Email:
dot.air.hnl.badge@hawaii.gov

Security Dispatch:

(808) 836-6641
(808) 836-6642

**HILO (ITO) – PASS AND ID
OFFICE**

Phone: (808) 961-9350

Email:
dot.air.ito.pass.and.id@hawaii.gov

Security Dispatch: (808) 961-9308

**KAUAI (LIH) – PASS AND ID
OFFICE**

Phone: (808) 241-3902

Email:
dot.air.lih.pass.and.id@hawaii.gov

Security Dispatch: (808) 274-3814

**KONA (KOA) – PASS AND ID
OFFICE**

Phone: (808) 327-9517

Email:
dot.air.koa.pass.and.id@hawaii.gov

Security Dispatch: (808) 329-1083

**MAUI (OGG) – PASS AND ID
OFFICE**

Phone: (808) 872-3874

Email:
dot.air.ogg.pass.and.id@hawaii.gov

Security Dispatch: (808) 872-3875

NATIONAL INTERNET SAFETY MONTH: JUNE

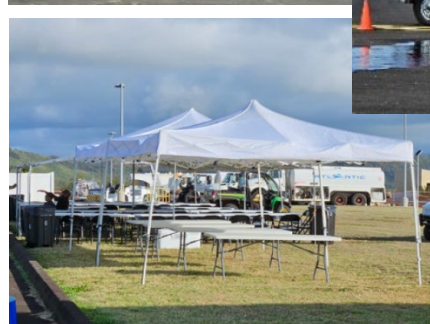
June was National Internet Safety month. The Internet is an integral part of both our personal and professional lives, that's why it's a good reminder to be aware of the data stored and shared on and over our computer and the Internet. It is important to keep computer data and systems secure. This can be done with a little effort by following some guidelines provided by the National Cybersecurity Alliance (2024):

- Keep software and Internet connected devices current with security updates.
- Create passwords that are at least 12-16 characters long and unique.
- Where available enable multi-factor authentication (MFA), 2-factor authentication like biometrics, security keys, or one-time codes to confirm valid logins.
- Think before you click. Does the site or email look "phishy".
- Use secure wifi. If you must use public wifi, be cautious what data you share. Never conduct sensitive or financial business, if possible.

**LIHUE AIRPORT (LIH)
CONDUCTS EMERGENCY TRAINING EXERCISE**

Kauai conducted an interagency mass rescue training exercise on April 15, 2025, at the Lihue Airport (LIH). Participants were the Hawaii Department of Transportation (HDOT) and Aircraft Rescue Fire Fighters (ARFF), along with mutual aid partners Kauai Fire Department (KFD), Kauai Police Department (KPD), American Medical Response (AMR) and Wilcox Medical Center.

The full-scale mass rescue exercise simulated passengers in distress. The Airport and local agencies worked together to test and evaluate interagency communications, response plans, and responders' actions in the event of a downed commercial airliner. (Excerpt from the State of Hawai'i DOT Website).





The Expanding Perimeter: Why Airport Security Must Include Cybersecurity

Editorial Series

By Maurice Edwards, Cybersecurity Coordinator

As professionals charged with securing some of our state's most critical infrastructures – our airports – we're familiar with perimeter breaches, access control challenges, and insider threats. But as the line between physical and digital security blurs, one thing becomes increasingly clear: cybersecurity is perimeter security.

Physical Infrastructure, Digital Threats

From badge readers and access control systems to CCTV and intercoms, much of what we rely on for day-to-day airport security is now IP-based. These devices often run outdated firmware, use default credentials, or are managed by third-party vendors who may not follow strong cybersecurity practices.

Known Weak Points in Airport Cyber Defenses

Recent assessments across U.S. transportation hubs have revealed recurring gaps that deserve our attention. The threat is real. In August 2024, the Port of Seattle (which oversees Seattle-Tacoma Airport) was targeted by a ransomware group. The attack disrupted baggage handling, check-in kiosks, ticketing, Wi-Fi, FIDS, the Port's website, and the flySEA app. Staff had to resort to manual processes to maintain operations.

What Can Employees Do?

While much of cybersecurity involves technical remediation, physical security professionals play a vital role:

- **Know your assets:** Understand which physical systems are network-connected (badge readers, cameras, HVAC, elevator controls, etc.) and ask if they are up to date and isolated.
- **Challenge defaults:** Never leave a device with default credentials or open remote access settings. Work with your IT/cyber team to enforce baseline hardening practices. If it comes with the device from the vendor, hackers already have your password.
- **Report anomalies:** Treat odd system behavior the way you'd treat a forced door or tampered badge. Early reporting often prevents escalation.
- **Champion training:** Cybersecurity is a shared responsibility. Advocate for training across all staff who touch systems, including contractors.

Final Thoughts

Airport security is no longer just about fences, badges, and patrols. It now includes ensuring that the digital gateways controlling those protections are secure as well. As we harden our physical defenses, let's make sure we're not leaving digital doors wide open.

The line between cyber and physical security is gone. We defend both, or we defend neither.

PERSONAL SAFETY

Stay Alert: Tips for Personal Safety During Commutes to and from Work

Whether heading to or from your car, waiting for a ride, or leaving the property, it is important to stay alert. It is easy to get distracted by your phone or lost in thought, but situational awareness is key to staying safe.

As foot traffic increases around work zones and parking areas, being mindful of who and what is around you can help prevent incidents before they happen. Staying off your phone, removing headphones/earbuds, and walking with confidence can make a significant difference in deterring unwanted attention.

Walk in pairs or small groups whenever possible, especially during early morning or late evening hours. If you notice anything suspicious, immediately notify airport security. Report and stay safe.

By staying aware, traveling in groups, and reporting concerns promptly, employees can help maintain a safer environment for everyone.

EQUIPMENT SAFETY: ULD

Safety Focus: Ground service equipment (GSE), like Unit Load Devices (ULD), need to be properly secured. GSE needs to be parked outside of the Vehicle Service Roads (VSR) with the tow bar in the "up" position. Double check that the GSE is not parked on or over the VSR line (see photo below). When parked the tow bar on the ULD activates the parking brake when in the "up" position. See difference in the photo to the right.



NEW LOCATION FOR HNL OVERNIGHT PASSENGERS

NEW LOCATION OF HOLDING ROOM FOR PASSENGERS STRANDED OVERNIGHT AT THE DANIEL K. INOUE INTERNATIONAL AIRPORT



Effective June 15, 2025, the State of Hawaii Department of Transportation relocated the waiting area for passengers who have misconnected and are stranded overnight at the Daniel K. Inouye International Airport (HNL).

The new location is in the public area of Terminal 2 in Baggage Claim 19, ground level.

If a passenger must remain overnight at the airport (HNL) and the security checkpoints are closed, please direct them to this new location. Security will monitor the area and ask the overnight passenger to present documentation of their outbound connecting flight.



Front ULD shows tow bar in the "down" position – brake not activated. Rear ULDs in the background show proper "up" position – brake activated. **(above photo)**

ULD equipment parked on and over the line in the VSR causing a potential hazard. **(left photo)**



DID YOU KNOW? – HNL AIRPORT APP

(Excerpts from the HDOT website)

Did you know that the Daniel K. Inouye International Airport (HNL) has an app to help people find their way around the airport? The HDOT launched the HNL Airport app on April 3, 2025. The app contains:

- Interactive terminal maps.
- The latest flight updates.
- Real time Blue Dot navigation.
- Turn-by-turn highlighted routing.
- The ability to find stops along your route.

The app can be downloaded for both Apple and Android systems. QR code is located on the HNL airport website at: <https://airports.hawaii.gov/hnl/wp-content/uploads/sites/6/2025/04/HNL-TER-MAP-APP-Letter-size-04-20250403.jpg>



HNL SECURITY PROCEDURES: VEHICLE ACCESS TO SECURED AREAS

Security measures have been implemented at the Daniel K. Inouye International Airport (HNL) to enhance safety and security. All passengers in vehicles accessing the Secured Area via access gates or the down ramps will be required to exit the vehicle and swipe their HNL-issued Airport ID Badge.

Passengers must exit the vehicle and proceed to the Pedestrian Access Gate, where available, to swipe their badge and enter their Personal Identification Number (PIN). At locations without a Pedestrian Access Gate, the passenger must exit the vehicle and proceed to the card reader to swipe and PIN. Airport Security will verify the Airport ID Badge, if a card reader is not available.

Important Notice: If the badge does not allow access:

- The badge holder may be denied entry.
- The badge may be confiscated.
- The badge holder must contact the Pass & ID Office through the company's Authorized Signatory.

Important Reminder: Pedestrians are not allowed to walk through vehicle entrance or exit lanes. Your badge may be confiscated, and you may be issued a citation. If work in the entrance lane needs to be done, please coordinate with the Airport On-Duty Manager (Code 22).

**UPCOMING: CYBERSECURITY AWARENESS MONTH
OCTOBER 2025**