ICE at the Gates and Beyond: Law Enforcement Compliance Risks for Community Associations
Wednesday, Jan 14, 1:40-2:50 pm

State and local law enforcement requests are a familiar part of association operations. Now, ICE raids and immigration-related demands have added a new layer of complexity. Boards, managers, and their counsel are left asking: What are our legal obligations? Where does liability begin? This session delivers a nationwide overview of law enforcement compliance risks for community associations with a focus on the emerging intersection of ICE activity and traditional investigative requests. Packed with practical guidance and strategies, this session equips association counsel to answer the next knock with confidence and compliance.
Leslie S. Brown, Esq., Rees Broome, P.C., Tysons Corner, VA
Sandra L. Gottlieb, Esq., CCAL fellow, SwedelsonGottlieb, Los Angeles, CA
Daniel Heaton, Esq., DeNichilo Law, APC, Ladera Ranch, CA

ISBN: 978-1-59618-103-8

2026 Community Association Law Seminar

Speakers/authors are solely responsible for obtaining all necessary permissions or licenses from any persons or organizations whose materials are included or used in their presentations and/or contributed to this work.

Community Associations Institute
6402 Arlington Blvd., Suite 500
Falls Church, VA 22042
www.caionline.org

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought. —From a Declaration of Principles, jointly adopted by a Committee of the American Bar Association and a Committee of Publishers

Printed in the United States of America


community
ASSOCIATIONS INSTITUTE
2026
COMMUNITY ASSOCIATION
Law Seminar
JAN. 14–16 | SAN DIEGO
©2026 Community Associations Institute
www.caionline.org | #WeAreCAI

2026 COMMUNITY ASSOCIATION Law Seminar

community ASSOCIATIONS INSTITUTE

ICE at the Gates – and Beyond:

Law Enforcement Compliance Risks for Community Associations

What Every Community Association Lawyer Needs to Know (Even if They Think They Don't)

2026 COMMUNITY ASSOCIATION Law Seminar

JAN. 14–16 | SAN DIEGO

Sandra L. Gottlieb, Esq., CCAL
SwedelsonGottlieb (CA)

Leslie S. Brown, Esq.
Rees Broome, P.C. (VA)

Daniel C. Heaton, Esq.
DeNichilo Law, APC (CA)

Why This Matters Now

Routine Demands

Records, surveillance footage, and contractor information requests from local law enforcement are increasingly common.

Recent ICE Activity

Immigration enforcement actions (workplace raids and residential sweeps) create new liability concerns.

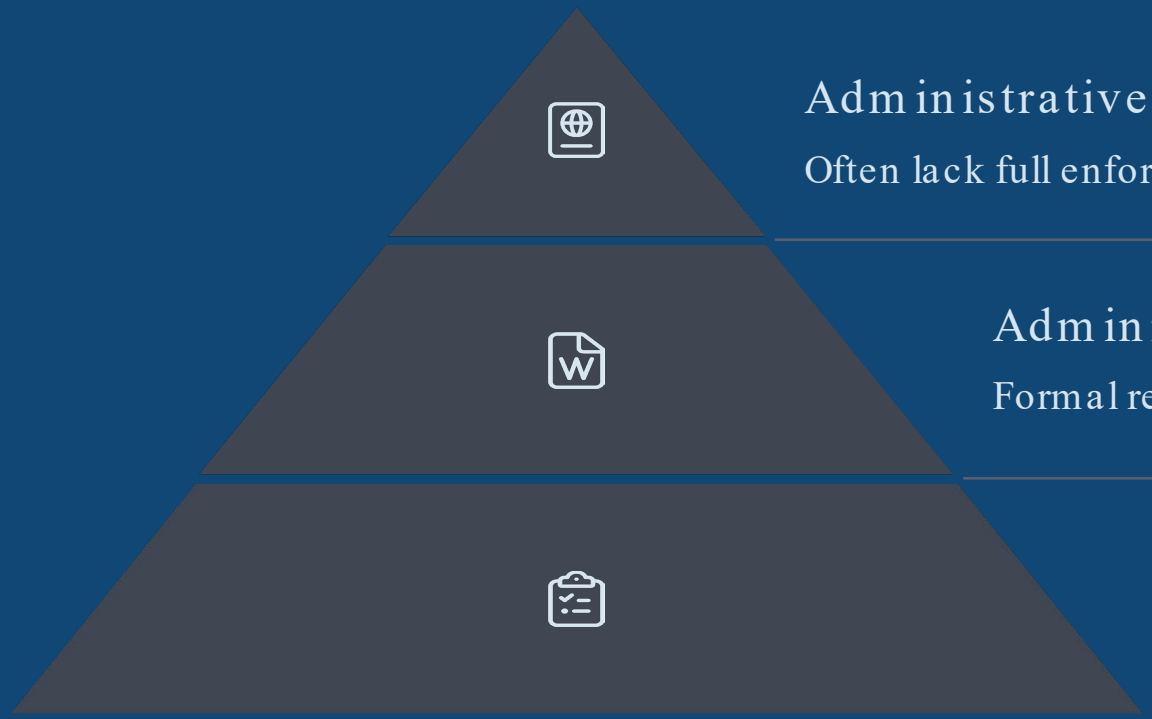
National Relevance

All jurisdictions face these issues, even "sanctuary" areas with protective policies.

Legal Triage

Communities need clear protocols and policy guidance to handle enforcement encounters professionally and mitigate risk.

Authority & Access Issues



Administrative Demands

Often lack full enforcement authority; consent still required for property access

Administrative Notices and Judicial Subpoenas

Formal requests that may require legal review

Judicial Warrants

Valid court-approved documents require response and permit forced entry into private spaces

Associations are private entities under the Fourth Amendment with distinct legal obligations different from government agencies.

Surveillance & Data Requests

Camera Footage

Requests must specify time frames, locations, and legal basis. Consider retention policies and chain of custody.

License Plate Data

Reader systems collect sensitive movement information. Balance security benefits against privacy expectations.

Facial Recognition

Emerging technology raises serious privacy concerns. Require strong legal justification before sharing.

Surveillance & Data Requests

- Legal and privacy considerations
- Responding to law enforcement requests: process and protocols

Surveillance & Data Requests

- Balancing law enforcement needs with association governance
- Best practices for protecting resident privacy

Surveillance & Data Requests

- Responding to law enforcement requests: process and protocols

Employment & Contractor Risks

Direct Employees

On-site staff under association control may require I-9 verification.

Contractor Oversight

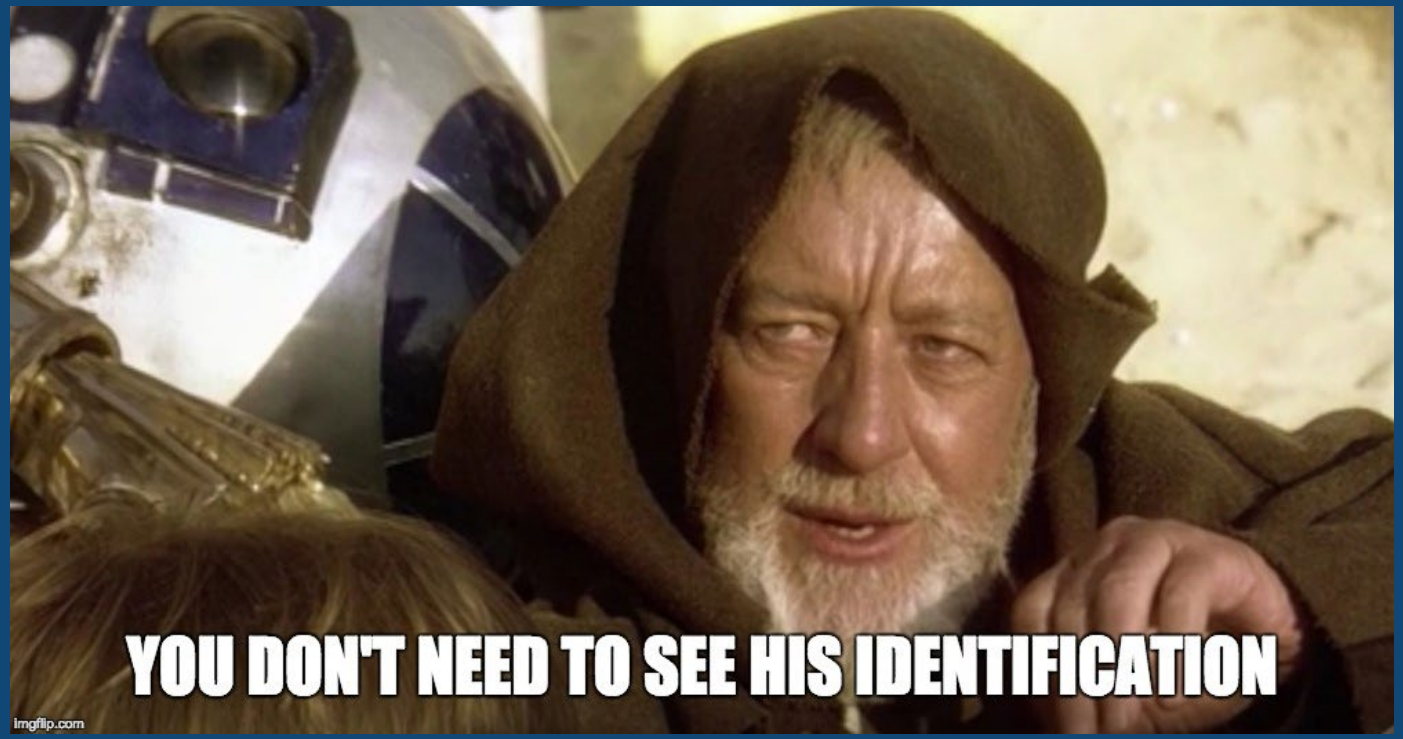
Verify licenses, insurance, and compliance history.

Response Protocols

Pause, verify credentials, contact legal counsel immediately.

Associations have different legal obligations depending on worker classification.

Employer Verification Considerations for Associations



Employment Verification Requirements

- Immigration Reform and Controls Act of 1986 (IRCA) makes it illegal for an ***employer*** to knowingly hire a person for employment without going through the employment verification process.
- Employers must verify that the person is not an unauthorized alien by examining documentation establishing both:
  - 1) employment authorization, and
  - 2) identity through a combination of documents, such as passport, green card, social security and/or driver's license
- The hiring person must attest, under penalty of perjury, that the person is authorized for employment within the U.S.

Record Keeping Requirements

- Form I-9 must be maintained by the employer
- Employer may also keep copies of verifying docs (driver's license, SSN card, etc.)
- Documents must be retrievable in accordance with federal regulations
- Form I-9 must be maintained for 3 years after the date of hiring, or 1 year after the date employment is terminated, whichever is later.

Employment Eligibility Verification

Department of Homeland Security

U.S. Citizenship and Immigration Services

USCIS
Form I-9
OMB No.1615-0047
Expires 05/31/2027

The "Notice of Inspection"

- DHS, DOL and DOJ all have right to inspect Form I-9 and verifying docs
- Typically, a formal letter is issued; subpoena or warrant not required
- 3 business days to respond

Homeland Security Investigations
Office of the Special Agent in Charge

U.S. Department of Homeland Security
SAC Boston

[redacted]

NOTICE OF INSPECTION

Dear Sir/Madam:

Employers are required under section 274A(b) of the Immigration and Nationality Act (INA), as amended by the Immigration Reform and Control Act of 1986 (IRCA) to verify the identity and employment eligibility of all individuals hired in the United States after November 6, 1986. Federal regulation, 8 C.F.R. Section 274a.2, designates the Employment Eligibility Verification Form I-9 (Form I-9) as the means of documenting this verification.

Pursuant to Section 274A of the INA, the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) SAC Boston is serving this Notice of Inspection ("Notice" or "NOI") to commence an inspection of your company's Forms I-9. Federal regulations afford employers **three (3)** business days' notice prior to the start of a Form I-9 inspection. This Notice serves as your advanced notification that HSI has scheduled an inspection of your company's original (wet ink) Forms I-9, or electronically generated with audit trails and/or retained Forms I-9, as applicable, to commence **three (3)** business days from the date of service of this Notice. The Forms I-9 and supporting documents listed in the associated administrative subpoena, if any, must be received by HSI no later than 7/11/2025 5:00 PM . As of the service date of this Notice, do not make any amendments to the existing Forms I-9. Any Forms I-9 that are prepared or completed after the service date of this Notice will not be part of this inspection.

After "Notice of Inspection" - 6 Possible Outcomes:

1. Notice of Inspection Results Letter
   Employer is compliant
2. Notice of Suspect Documents
   Employer has additional time for proper verification of employee
3. Notice of Discrepancies
   Employer is obligated to notify employee; additional time allowed
4. Notice Technical or Procedural Failures
   10 business days to correct form
5. Warning Notice
   Violations identified, but expectation of future compliance
6. Notice of Intent to Fine
   Employer may request ALJ hearing w/in 30 days

Employment Verification Red Flags

- Form I-9s with no boxes checked or multiple boxes checked
- Form I-9s with missing signatures
- Incorrect verification documents provided
- Not completing the Form I-9s timely
- Clearly falsified or missing documentation
- Social security number mismatches
- History of non-compliance

Good Faith Defense and E-Verify

- Rebuttable, affirmative defense that employer is not in violation of IRCA
- Agency must show "actual" knowledge
- E-Verify
  - voluntary, free, online system for employers
  - Takes Form I-9 information and compares to DHS and SSA records
  - Instant case result regarding whether employee's verification records match DHS or SSA's records
  - "Tentative Nonconfirmation" - mismatch; employer must notify employee
- PROS: quick; reduces unauthorized employment; may -> reduced penalties
- CONS: not a substitute for I-9; does not stop a workplace audit; not a safe harbor; does not work if government shutdown

The "Workplace Inspection" - A Real World Example

Considerations for Community Associations

- Who should the Association be concerned about?
  - Direct hires
  - Management personnel
  - Contractors

- Who undergoes employee verification process?
  - General Manager
  - Management Agent
  - Compliance Company

- How is the verification documentation stored?
  - On site or offsite?
  - Physically or electronically?

Considerations for Community Associations

- How is it retrieved?
  - Who has access?
  - What are the security protocols?

- How can the Association protect itself?
  - Shift liability - contractual indemnification for employment-related claims
    - IRCA caution - using labor subcontractors to avoid direct hiring liability can also be red flag for agencies
  - Adequate insurance - employment practices; cyber liability
  - Vetting process for direct hires and contractors

Discrimination &Fair Housing Concerns

National Origin

Protected by federal law in all jurisdictions.

Immigration Status

Protection varies by state and locality.

Documentation

Neutral procedures protect associations from claims.

Liability Traps

Over-compliance with authorities may violate resident rights.

Balancing risks: (1) trouble for improperly refusing valid enforcement requests, or (2) discrimination claims for targeting specific residents

Fair Housing: Immigration Status and Citizenship

POLL: Are immigration status and citizenship protected classes under the federal Fair Housing Act?

1. Yes
2. No
3. Maybe
4. I don't know

42 U.S.C. § 3604

- The federal Fair Housing Act ("FHA") prohibits housing providers from discriminatory practices based on one's race, color, religion, sex, national origin, familial status, and disability.
- If Congress wanted to extend to immigration status and/or citizenship, it could have..but it didn't...
- BUT! Discrimination on the basis of immigration status and/or citizenship can also trigger *race* and/or *national origin.*

A Case Study- *Reyes v. Waples Mobile Home Park*

- Mobile Home Park policy requiring all occupants to provide documentation evidencing legal status in the U.S. to renew their leases
- Plaintiffs were/are 4 Latino couples living in the Park
- Claimed policy violated FHA because it disproportionately ousted Latinos from residing in the mobile home park based on *race* and *national origin*
- Plaintiffs all non-citizens of Salvadorian or Bolivian national origin, BUT!
  - 4 male plaintiffs had SSNs in compliance with the policy
  - 4 female plaintiffs were illegal immigrants
  - Their children…all U.S. citizens

E.D. VA - 2016 Ruling

- Dismissed disparate impact under Rule 12(b)(6) and disparate treatment claim on MSJ

4th Circuit - 2018 Ruling

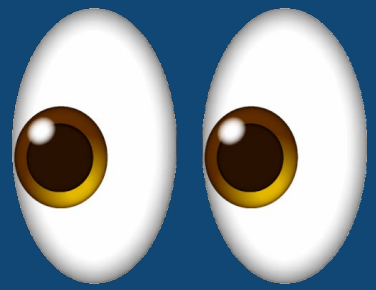
- Disparate treatment claim conflated with disparate impact
- Remand back to E.D. VA, but…

Eastern District of Virginia - 2022 Ruling

- New Judge!
- Grants MSJ in favor of the mobile home park
- IRCA's anti-harboring statute constituted a valid "business necessity"
- 8 U.S.C. § 1324(a):
  - makes it a criminal offense to knowingly or recklessly assist an undocumented immigrant from entering or remaining in the U.S. illegally, such as providing shelter, transportation, or other similar assistance, with certain exceptions.
- Appeal…

4th Circuit - 2024 Ruling

- *De novo* review
- *Inclusive Communities* framework:
    1. robust causal connection between the defendant's challenged policy and the disparate impact on the protected class.
    2. discriminatory policy was necessary to achieve a legitimate non-discriminatory interest.
    3. interest could be served through less discriminatory means
- Facts do not establish "business necessity"
- Lease agreement does not constitute "harboring"
- Case is back on remand to EDVA …again! Stay tuned!



State Immigration Status and Citizenship Protections

- States
  - California - AB 291, Civil Code § 1940.3
  - Illinois - 775 ILSC 5/3-101 - Added in 2024

- Local Jurisdictions
  - New York City - N.Y.C. Admin. Code 8-107.5(a)
  - Look to counties, cities, and towns.

Real World Implications for Community Associations

- Claims may present as a hostile environment under HUD regulations as perceived immigration status based on race or national origin.
- Members of the community with an animus towards certain groups may want to assist ICE officials.
- ICE activity on the premises could lead to gossip and defamation.
- Nosy neighbors may want to inspect books and records about ICE activity or perceived immigration status of others.

Considerations for Community Associations

- Keep communications about ICE activity neutral and the subject of any investigation confidential.
- Reassure residents that files will not be turned over without a proper judicial warrant.
- Remind residents not to take matters into their own hands.
- Have an anti-discrimination policy in place.
- Bring in a trusted official to discuss ICE concerns in general terms (community resource officer, local elected official, etc.).

Creating Effective Policies: *Guiding Boards and Managers*

Stop

Never immediately comply without verification

Identify

Request and verify credentials from all law enforcement visitors

Review

Examine documentation carefully (administrative vs judicial warrants)

Consult

Contact association counsel immediately before proceeding

Key Takeaways &Next Steps

1. **Update Governing Documents**

   Review CC&Rs and rules for gaps in enforcement response procedures.

2. **Create Response Templates**

   Develop standardized forms for tracking requests and maintaining documentation.

3. **Train Key Personnel**

   Ensure managers, security staff, and board members understand protocols.

4. **Consult Specialized Counsel**

   Engage attorneys with immigration and fair housing expertise for policy review.

Proactive planning mitigates liability. Balance cooperation with protecting rights.

Questions?

ICE at the Gates and Beyond

Law Enforcement Compliance Risks for Community Associations

What Every Community Association Lawyer Need to Know (Even if They Think They Don't)

January 14, 2026

Sandra L. Gottlieb, Esq., CCAL fellow, SwedelsonGottlieb, Los Angeles, CA

Leslie S. Brown, Esq., Rees Broome, P.C., Tysons Corner, VA

Daniel C. Heaton, Esq., DeNichilo Law, APC, Ladera Ranch, CA

I. Introduction: *Why This is Real?*

Interactions with state and local law enforcement are not new territory for community associations. Sometimes, these interactions are as simple and innocuous as a local community resource officer speaking to homeowners about routine safety matters and ongoings in the community. Other times, the interactions relate to an active criminal investigation through requests for association surveillance[1] camera footage, license plate information, or the taking of witness statements.

Associations are now experiencing a new type of interaction with law enforcement through Immigration and Customs Enforcement (ICE) raids and other immigration-related demands. These interactions add an additional layer of complexity and concern for associations. Boards, managers, and their counsel are left asking: What are our legal obligations? Where does liability begin? This manuscript answers those questions and more by providing an overview of the intersection of traditional investigative requests by law enforcement versus immigration enforcement action within associations, highlighting compliance risks and best practices for community associations.

A. "Real World" Examples of Recent Activity Impacting Communities

In the Wilshire Corridor of Los Angeles, CA, a high-rise experienced ICE descending on the building, making a demand for employment records and documents reflecting verification policies. By the time counsel learned of the event, ICE had already taken action on two outsourced employees that were working in valet. One eventually returned on-site; the other, not a U.S. Citizen, was not returned, and their employer has not been able to obtain any further information. During the incident, ICE refused to provide the on-site general manager names, contact information, or credentials. They indicated they'd come back with a warrant; however,

[1] We specifically highlight out intentional description of association cameras as "surveillance," in lieu of "security," as an important distinction in limiting potential liability exposure.

there has not been any further activity. A plan of action was created in the event that they come back.

An FBI Agent contacted members of the board, management, and financial representatives of a San Jose condominium association through email and from his cell phone, asking to verify certain personnel and financial information. The individual claimed to be acting in response to a complaint about financial mismanagement and fraud by the board of directors. Before returning contact or providing information, legal counsel was looped in to verify that the individual was indeed an Agent and had authority to make demands from the association's representatives. This verification process was not quick, requiring an online report and multiple conversations with FBI field office supervisors before the Agent was finally connected with counsel to resolve the concern.

A high-rise condominium in Arlington, Virginia recently received a visit from a lone law enforcement officer asking for information about a potential resident. The officer did not have a warrant. The general manager, rightly, did not provide information, without more authority, took the officer's name and badge number, and sent it to legal counsel for further counsel.

These examples reflect not only traditional law enforcement efforts, but also the expansion of immigration enforcement operations into residential settings. ICE agents may arrive at association properties looking for specific individuals, requesting access to secured areas or common spaces, and/or demanding resident information, employee records, or vendor documentation. These often-unannounced visits create immediate practical challenges for unprepared boards and management who then must make on-the-spot decisions about compliance while protecting association interests. The frequency of these encounters has increased as enforcement priorities shift toward workplace and residential enforcement strategies.

B. Everyday Law Enforcement Demands and the New Layer of ICE Raids

ICE has increasingly extended operations into community spaces, through workplace raids and residential sweeps that directly impact common interest developments and homeowners associations. This activity creates unprecedented challenges for community association attorneys nationwide, regardless of whether they practice in "blue" states or sanctuary jurisdictions. The legal complexities arise at the intersection of federal immigration enforcement, private property rights, and potential discrimination claims. Community associations and their counsel must be prepared to navigate these waters carefully, balancing compliance obligations with resident protections.

C. Nationwide Relevance, Even in "Blue" or Sanctuary Jurisdictions

A "sanctuary city" is a state, city, county, or other municipality that has a adopted a policy to limit its cooperation with federal immigration enforcement to protect undocumented immigrants from being detained or deported solely because of their immigration status.

Technically, there is no formal legal definition of "sanctuary city." The term merely pertains to the application of local policies to limit local assistance in federal immigration enforcement cases. The policies do not prevent ICE from operating in a locality. Instead, they limit the amount of support that is provided at the local level.

Conversely, more than 600 state and local agencies have signed agreements to cooperate with ICE through the federal government's 287(g) Program.[2] Section 287(g) of the Immigration and Nationality Act (INA) allows the delegation of certain immigration enforcement functions to state and local law enforcement agencies.[3] Law enforcement agencies interested in participating in the "287(g) Program" must sign a Memorandum of Agreement (MOA) with ICE. The state and local law enforcement agencies will nominate officers to participate in the program. Nominees must possess U.S. citizenship, engage in, complete and pass a background investigation, and have knowledge of and have enforced laws and regulations related to law enforcement activities at their jurisdictions, among other criteria. The nominees then receive training related to immigration duties under the MOA.[4]

D. Key Takeaways: Legal Triage, Policy Drafting, and Liability Mitigation

Without proper legal guidance, community associations risk significant liability from multiple directions. They need comprehensive understanding of their actual legal obligations (or lack thereof) regarding immigration enforcement, the proper handling of different warrant types, appropriate documentation of enforcement encounters, and safeguards against discrimination claims. The liability landscape is complex. Actions can trigger Fair Housing violations, privacy lawsuits from residents, or potential obstruction issues with authorities. There is a clear need for established protocols, proper training, and specific policies to help associations navigate these situations legally and ethically.

This manuscript aims to 1) provide an overview of various immigration law enforcement laws impacting associations, and 2) practical guidance on three key fronts: (i) legal triage when

---

[2] Chernikoff, Sara, *et. al.* "More than 600 local police agencies are partnering with ICE: See if yours is one of them," June 17, 2025, www.usatoday.com/story/graphics/2025/06/17/map-shows-where-police-law-enforcement-can-partner-with-ice-raids/84185758007 (accessed Nov 1, 2025).

[3] *See* 8 U.S.C. §1357(g).

[4] https://www.ice.gov/identify-and-arrest/287g.

confronted with enforcement activities, (ii) policy development to establish clear protocols, and (iii) risk mitigation strategies to protect associations from potential liability. Understanding these three areas has become essential for community association attorneys to provide competent representation to their clients.

II. Searches and Seizures: Understanding Warrants, Subpoenas, and Administrative Demands

A. Fourth Amendment Basics for Community Associations

Community associations occupy a unique position as "private actors" under the Fourth Amendment of the U.S. Constitution. Unlike government entities, they maintain constitutional protections against unreasonable searches. However, these protections have limitations depending on property configuration, access controls, and management structure.

The Fourth Amendment, which protects against unreasonable searches and seizures, creates the legal foundation for evaluating the scope of associations' rights regarding government access. It provides:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[5]

The Fourth Amendment establishes a simple baseline that when the government obtains information by physically intruding on persons, houses, papers, or effects, a "search" within the original meaning of the Fourth Amendment has "undoubtedly occurred."[6] Law enforcement does not have the right to enter a home or a private business unless they have a warrant signed by a judge, or unless certain constitutional exceptions apply, such as the property owner providing consent or in exigent circumstances (risk of destruction of evidence, imminent damage, etc.).

Fourth Amendment protections extend not just to the interior of the dwelling, but to the area "immediately surrounding and associated with the home," referred to as the "curtilage."[7] The classic example of curtilage is a home's front porch.[8] While a police officer not armed with a warrant may approach a home and knock,[9] precisely because that is "no more than any

---

[5] U.S. Const. Amend. IV.
[6] See *U.S. v. Jones*, 565 U.S. 400, 431 n.3 (2012).
[7] *Florida v. Jardines*, 569 U.S. 1, 6 (2013).
[8] *See id.* at 7 (*citing Oliver v. United States*, 466 U.S. 170, 182 n.12 (1984)). Curtilage can also be a small fenced-in yard, a gated walkway along the side of a house. *See also U.S. v. Sweeny*, 821 F.3d 893, 901 (7th Cir. 2016).
[9] This is referred to as the "knock and talk" exception to the 4th Amendment.

private citizen might do,"[10] using a drug-sniffing dog on a front porch of a home to search for narcotics does not constitute a routing visit. Without a warrant, the additional investigative activity triggers Fourth Amendment concerns unless it is otherwise supported by probable cause.[11]

The same logic applies to bringing a police dog to sniff for drugs outside an apartment door. The 7th Circuit held in *U.S. v. Whitaker*, 820 F.3d 849 (7th Cir. 2016) that such activity also amounts to a search of the apartment interior that requires a warrant.[12] While the court acknowledged that the plaintiff in that case did not have a reasonable expectation of complete privacy in his apartment hallway, a lack of a reasonable expectation of complete privacy in the hallway does not also mean that he had no reasonable expectation of privacy against persons in the hallway snooping into his apartment using sensitive devices not available to the general public.[13]

When it comes to community associations, there are many common areas that are not considered curtilage. For example, a common basement garage of a condominium building is not considered "curtilage" affording Fourth Amendment protection.[14] Neither is a walkway adjacent to condominium building, but located behind gate, nor is a shared duplex hallway.[15]

When determining the scope of curtilage, courts will take into account "(1) the proximity of the area in question to the home; (2) whether the area is included in an enclosure surrounding the home; (3) how the owner uses the area; and (4) the measures taken to protect the area from observation."[16] "Generally speaking, courts that have considered whether common areas in a multi-family dwelling are part of the curtilage of a dwelling have been reluctant to recognize curtilage protection for those areas"[17] as there is usually no reasonable expectation of privacy in shared and common areas in multiple-dwelling residential buildings.

B. Judicial Warrants and Subpoenas v. ICE Administrative Warrants: Knowing the Difference

It is critical for community associations to understand the distinction between judicial warrants (issued by the courts) and the administrative warrants commonly utilized by ICE

[10] *Jardines,* at 8 (*citing Kentucky v. King*, 563 U.S. 452, 469 (2011)).
[11] *Id.* at 9.
[12] *See U.S. v. Whitaker*, 820 F.3d 849, 853–54 (7th Cir. 2016).
[13] *Id.*
[14] *U.S. v. Cruz Pagan*, 537 F.2d 554, 558 (1st Cir.1976).
[15] *See Harney v. City of Chicago*, 702 F.3d 916, 925 (7th Cir. 2012) (walkway adjacent to condominium building but behind gate); *U.S. v. Villegas*, 495 F.3d 761, 767–68 (7th Cir. 2007) (internal duplex hallway).
[16] *U.S. v. Dunn*, 480 U.S. 294, 301 (1987).
[17] See Sweeny at 901 (*quoting Cops, Canines, and Curtilage: What Jardines Teaches and What It Leaves Unanswered*, 52 Houston L. Rev. 1289, 1303 (2015)).

officials, which are internal documents that are not reviewed or authorized by the judicial system.

Judicial warrants are issued by federal or state judges after reviewing probable cause evidence and typically provide broader authority for searches and seizures. This distinction fundamentally determines whether a particular law enforcement official has legal authority to enter association property without permission. Association staff must be trained to identify each type and understand that only judicial warrants can compel access to private or restricted areas.

Conversely, ICE frequently relies on administrative warrants. Administrative warrants are limited in the sense that they do not authorize ICE to enter private or restricted-access areas, including most common areas of gated or secured communities, without consent. Only judicial warrants signed by a judge can compel such access. Association counsel must understand this critical distinction to properly advise clients on legally required compliance.

However, immigration officials do not need judicial warrants to detain persons who entered the U.S. illegally, who have been deported previously and then return, or who overstayed their authorized stay. Instead, immigration officials are empowered with the use of administrative warrants. Section 8 U.S.C. § 1226(a) provides that, upon issuance of an administrative warrant, an immigration officer may arrest and detain an alien, pending a decision as to whether the alien is subject to removal. These "ICE warrants" are issued by certain empowered immigration officials who have been authorized or delegated such authority and are exclusively for use by immigration officers who have successfully completed immigration law enforcement training.

Unlike judicial warrants issued in criminal cases, ICE warrants do not require a detached and neutral magistrate; instead, ICE warrants require the officer to establish that "there is probable cause to believe" that the individual named in the warrant ***is subject to removal*** (not merely just being in the country illegally). The warrants issued by ICE are purely administrative, as they are neither reviewed nor issued by a judge or magistrate, and therefore do not confer the same authority as judicially approved arrest warrants. Thus, some lower courts have ruled that ICE agents violated the Fourth Amendment by forcibly entering homes without a judicial warrant when no recognized exceptions to the Fourth Amendment's warrant requirement existed, such as exigent circumstances (risk of harm to the public, potential destruction of evidence, etc.) or the owner's consent to the entry of the home.[18]

[18] *See Cotzojay v. Holder*, 725 F. 3d 172, 183 (2d Cir. 2013).

Despite lower court rulings, immigration officials are empowered to make arrests even without an administrative warrant under 8 U.S.C. §1357(a) when:

1. the alien, in the presence or view of the immigration officer, is entering or attempting to enter the United States unlawfully; or

2. the immigration officer has "reason to believe" (aka "reasonable cause") that the alien is in the United States unlawfully and is likely to escape before a warrant can be obtained.

Finally, Department of Homeland Security (DHS) regulations provide that immigration officers may question an individual so long as the officer "does not restrain the freedom of an individual, not under arrest, to walk away." The information obtained from the immigration officer's questioning "may provide the basis for a subsequent arrest" (*e.g.*, if the immigration officer forms probable cause that the alien is unlawfully present in the United States). An immigration officer may "briefly detain" an individual for questioning only if there is reasonable suspicion that the person is "engaged in an offense against the United States or is an alien illegally in the United States."[19]

ICE Warrant v. Judicial Warrant – Reference Chart[20]

Ice Warrant	**Judicial Warrant (Search or Arrest)**
• Issued by an administrative agency and directed to immigration officials, not police • Grants ICE officers right to arrest a non-citizens suspected of committing immigration violations • Signed by immigration officer, not a neutral adjudicator, like a judge • Does not identify probable cause for local law enforcement • No right to enter private property to arrest • No right to search or seize private property (both as to ICE officers and local police)	• Issued by Court, not an administrative agency • Signed by a Judge or Magistrate • Directed to local police • Will be current and have a time limit • Gives police right to enter private property to conduct a search or make an arrest • Describes in detail the place to be searched and/or the persons or things to be seized • Limits activity to locations and persons specifically within judicial warrant

[19] *See* 8 C.F.R. 287.8(c).

[20] Sample ICE and federal judicial warrants are included in the Appendix.

C. Implications of Public vs. Private Areas; Specifics Pertaining to Gated or Secured Communities

The legal classification of public versus private areas has significant implications for immigration enforcement interactions. As private actors, rather than government entities, associations possess property rights that include controlling access to their premises and determining who may enter restricted areas (unless state statutes provide otherwise). This private status grants associations the legal authority to establish and enforce access policies, request identification from those seeking entry, and refuse access when proper documentation is not provided. Unlike public housing or government-owned businesses, private associations maintain stronger legal standing to resist warrantless entry attempts.

This status creates both rights and responsibilities regarding enforcement encounters. Associations aren't simply passive participants, but active stakeholders with legal authority to protect their property and residents. Associations not only have the right, but the obligation, to ask to see identification, request copies of any warrant, and consult counsel before granting access. Following this type of due diligence process should not be seen as obstruction, but a proper exercise of the association's responsibilities to its members. Staff should be trained to courteously, but firmly, request proper identification, document the purpose of the visit, examine any warrants presented (noting whether they are administrative or judicial), and consult with legal counsel before making access decisions. This verification process protects both the association from liability and the residents from potential rights violations.

Additionally, practitioners are advised to note their jurisdictions' laws governing process servers' access to gated communities, which vary state by state. A handful of jurisdictions have enacted statutes explicitly granting process servers entry for the purpose of lawful service of process, such as California, Florida, and Illinois.[21] These laws aim to prevent obstruction of legal proceedings by ensuring that physical barriers do not impede due process. However, in states without such statutes, process servers encountering a gated community typically must rely on normal service methods (personal delivery, substituted service, posting/mailing) and may need to seek alternative methods or court permission if access is blocked. Legal access often hinges on whether the community is staffed by security and whether the server can present proper credentials. Associations that are not mandated under state law to automatically admit a process server simply because they are carrying legal papers, may rely on community rules, gate policies, security guard discretion, etc., unless a court order or other statute intervenes.

[21] *See* Cal. Civ. Proc. Code § 415.21 (2025); Fla. Stat. § 48.031(7) (2025); 735 ILCS 5/2-203 (2025). Virginia attempted to pass legislation in 2017 that would require gated communities to admit process servers, but the legislation failed. Similar attempts were made in New Jersey in 2020 and 2024.

D. Practical Considerations for Associations

In sum, for community associations, the real-world implications are as follows:

- ICE officials may be looking for a resident or contractor on the premises for purposes of making an arrest:
    - *In general, the public common areas, like lobbies, hallways are not going to be considered "private" for purposes of entry, but non-public places like the management office would be.*[22]
- ICE officials may want to obtain residency or employment information from association books and records to locate deportable persons (address, vehicle information, etc.):
    - *The association does not have a duty to answer questions or provide such information without a judicial warrant or subpoena. However, in the context of a workplace audit for employment verification purposes pursuant to a Notice of Inspection, the Association does have to respond within 3 business days, as discussed further in this manuscript.*
- ICE officials may request association agents to deliver immigration notices (Notice to Appear):
    - *The association has no obligation to deliver such notices to residents and should advise the ICE officials of same.*
- Process servers may try to enter gated communities to serve residents with subpoenas and warrants.
    - *The association needs to conform with state law requirements regarding access to premises for process servers.*

III. Requests for Surveillance Footage and Similar Data

With the increased use of security technologies like cameras, license plate readers, and even facial recognition, boards and managers are receiving more requests for access to this data, from residents and law enforcement alike. Associations should have in place clear,

[22] *See* 8 C.F.R. 287.8(f)(2) ("An immigration officer may not enter into the non-public areas of a business, a residence including the curtilage of such residence, or a farm or other outdoor agricultural operation, except as provided in section 287(a)(3) of the Act, for the purpose of questioning the occupants or employees concerning their right to be or remain in the United States unless the officer has either a warrant or the consent of the owner or other person in control of the site to be inspected. When consent to enter is given, the immigration officer must note on the officer's report that consent was given and, if possible, by whom consent was given. If the immigration officer is denied access to conduct a site inspection, a warrant may be obtained.")

written policies for what data is stored, retention periods, who may access the data, and how it will be used.

A. Types of Association Data: Surveillance Camera Footage, License-Plate Reader Logs, and Facial-Recognition Data

1. Surveillance Camera Footage

Surveillance video footage for community associations typically refers to video recordings captured by access control cameras installed in common areas of residential communities, such as entrances and exits, parking areas, common area amenities, lobbies, hallways, and exteriors. Practitioners need to address the following with respect to surveillance videos and crafting policies:[23]

- Data is only to be used for clear purposes (like public safety or investigations).
- Verify that collection/deployment is permitted (public-space vs private-space)
- Confer with applicable state law on audio recordings of conversations (1 party v. 2 party consent states) and wire-taping/unlawful recordation laws. Fo*r these reasons, it is recommended, that only video, not audio recording is captured.*
- Residents should be informed when the cameras are recording, if possible.
- Footage should be kept for a brief period time, unless it's evidence; then, the footage should be stored securely.
- Access to footage needs to be limited to authorized staff and association officers, if applicable; policies need to address and track who views or copies it.
- Policies should be created with the protection of privacy in mind; avoid using footage to monitor protests or private activity.

2. License-Plate Reader Logs

License plate readers (LPRs) or automatic license plate readers (ALPRs) are specialized camera systems that capture and analyze images of vehicle license plates. They use high-speed cameras to take pictures of vehicles and their license plates, often mounted on police cars, traffic lights, toll booths, or road signs. Specialized optical character recognition (OCR) software processes the images to extract the alphanumeric characters from the plates. Then, the extracted plate numbers are compared against databases for various purposes, such as

[23] A sample Surveillance Video Policy is included in the Appendix.

identifying stolen vehicles, tracking vehicles involved in crimes, checking for expired registrations or unpaid fines, and monitoring traffic patterns.

Typically, LPRs are integrated with gate systems to allow residents' vehicles to enter automatically, improving convenience and reducing the need for key cards or remotes.

However, practitioners need to confer with their states' laws, as state law addresses how such data can be used and shared. For example, California prohibits sharing ALPR (automated license plate reader) data with out-of-state law-enforcement agencies (broadly) unless certain conditions are met.[24] California local law enforcement should verify whether sharing surveillance data (ALPR, camera footage, driver/vehicle records) with ICE or out-of-state agencies is permissible under SB 34/SB 54 (Statutes of 2015; effective 2016). If not permissible, data requests should be denied or vetted. Starting in 2024, Virginia law creates privacy protection for data captured by ALPRs used specifically by law enforcement.[25]

If associations are utilizing LPRs, they need to keep in mind the following considerations:

- Collect only what's needed — don't store data from every car for years.
- Delete quickly if the plate isn't linked to a crime or investigation.
- Control access and record all lookups or data sharing.
- Be transparent about how long data is kept and who can see it.

3. Facial-Recognition Data

Facial recognition software is a type of biometric technology that uses algorithms to identify or verify a person's identity based on their facial features. A camera captures an image or video of a person's face. The software then detects the presence of a face in the image and analyzes key facial features. These features are converted into a mathematical representation (a faceprint) and compared to a database of known faces for identification and verification.

A community association might consider using facial recognition software for access control, like touchless entry, visitor logging, incident investigation and overall operational efficiency. However, it's a practice that has significant privacy considerations. Accordingly, associations should take into account the following considerations:

- Use only when truly necessary — not for mass or real-time surveillance.
- Check accuracy and inherent bias before using the system.

[24] California Senate Bill 34 (2015) (amending Civil Code §§ 1798.29, 1798.82 and adding Sections 1798.90.5 *et seq.*)
[25] Virginia Code § 2.2-5517 (effective Jan. 1, 2026).

- Don't keep non-matches or unnecessary biometric data.
- Limit access and log all searches or matches.
- Get legal or court approval for investigative uses when required.
- Provide transparency and oversight to prevent misuse.

Training Tip: *Many surveillance systems are operated via private vendors. Legal counsel should review all third-party data-sharing clauses in vendor contracts and confirm that vendors have privacy safeguards that align with the association's governing documents, as applicable, state law, limitation on access by ICE/local law enforcement, clear terms regarding data exports and cross-jurisdictional sharing, maintenance of audit logs, and adequate insurance covering data breach claims and unauthorized disclosures.*

B. Requests for Data Access: Balancing Law Enforcement Demands with Privacy Obligations and Association Governance

As made clear earlier in this manuscript, if law enforcement appears without a subpoena or judicial warrant, associations and management can (and should) decline immediate compliance and escalate the matter to legal counsel. The Fourth Amendment protects against unreasonable searches and seizures by government, to include surveillance system data. However, validly issued subpoenaed-sharing confirms that the request is legally binding. Association counsel needs to review the request, even though there is a legal basis to release the data.

Whether faced with a judicial warrant or subpoena, or considering voluntarily responding to requests for data without judicial process, associations need to balance requests by law enforcement for personal data against other legal forces governing the Association's operations, like the governing documents. Association boards have fiduciary obligations to protect member rights and maintain confidentiality of personally identifiable information (PII), not just comply with police requests.

At the federal level, currently there is no comprehensive "immigration-enforcement" privacy statute covering all of ICE's data-surveillance activities. The lack of such clear regulation can lead to gaps in regulatory oversight. Security and data-sharing agreements between federal agencies and ICE sometimes involve surveillance/data access (including FOIA releases) with limited public transparency. While this manuscript is not meant to specifically address specific governing agencies' practices regarding data access, retention, destruction of non-targets, inter-agency sharing of data, jurisdictional/scope issues, etc., surveillance or data requests should be limited to a clear enforcement purpose - not a blanket dragnet collection of data about innocent persons.

When counseling boards, it is important for legal practitioners to understand applicable laws governing data disclosure, including federal, state, and local regulations (e.g., privacy laws, data protection statutes), in addition to what the governing documents may require as far as data use and sharing. Practitioners should confer with state-specific privacy laws regarding disclosures of personal identifying information, as voluntary sharing could expose the association to liability if it violates someone's rights. Some states, like California and New York, impose civil penalties for unlawful disclosures:

- **California:** California Consumer Privacy Act (CCPA). Local agencies in California sharing ALPR or other surveillance data with ICE (or enabling ICE queries) have been subject to legal challenge (e.g., Marin County sheriff case) for violations of SB 34/SB 54. Additionally, California Senate Bill 54 (California Values Act, chaptered Oct. 5, 2017)[26] restricts local and state law-enforcement agencies from using resources or personal data to aid federal immigration enforcement in many circumstances. This limits cooperation with ICE.
- **Texas:** Biometric Privacy Law (HB 3745 – pending updates).
- **Florida:** Florida Information Protection Act (FIPA). Also note that Florida has a broad "Sunshine Law" for public-records access (Fla. Stat. ch. 119) which may impact disclosure of surveillance logs and law-enforcement records. Overall, Florida has fewer legal constraints on local law-enforcement cooperation with ICE than California's sanctuary-style laws. However, even if data is shared with ICE, the fact of sharing may become subject to Sunshine-Law disclosures. Agencies should factor potential reputational risk and require privacy risk evaluations.
- **New York:** SHIELD Act – mandates security measures for personal data.
- **Texas:** Texas Data Privacy and Security Act (TDPSA), effective July 1, 2024; further obligations begin Jan 1, 2025. While primarily business-to-consumer privacy law, it reflects growing state-level expectations for data handling. However, Texas generally has fewer state restrictions than California and many local agencies may have formal or informal MOAs with ICE under the 287(g) Program.

C. Best Practices for Maintaining Privacy of Association Data

1. Written Policies

Association boards and management should work with legal counsel on written policies to address maintaining and releasing association data. The policy should address the following:

[26] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB54.

- Avoid verbal agreements or informal data sharing, especially when involving immigration issues.
- Set clear data retention periods
    - *30 days' maximum, unless otherwise required.*
- Who is authorized to request to inspect and request and how such persons are vetted or verified.
- Who is authorized to fulfill the request?
    - *Only senior management staff or the board should access raw surveillance data (in circumstances when needed).*
- Notify residents annually of surveillance and privacy policies.
- Adopt a neutral policy for all law enforcement or third-party data requests.
- Require written requests (e.g., subpoena, court order, or warrant) before disclosing any surveillance or resident data.

Practitioner's Note: *Legal counsel also needs to confer with their state's specific laws pertaining to the right to access to association books and records laws by members.*

2. Data Protection

Community associations handle significant amounts of personally identifiable information, such as assessment payment information, residency information, vehicle information, phone numbers, email addresses, etc. making data protection a critical responsibility. Here are some basic data protection guidelines for associations, based on current legal frameworks and best practices:

- Systems should have data encryption features, with strong authentication (like multi-factor identification).
- Keep software, systems, and networks current to patch vulnerabilities.
- Use reputable antivirus and anti-malware tools.
- Restrict access to sensitive data to only necessary personnel.
    - Ensure managers know where data is stored and who controls it.
    - *Include association leaders in training sessions on these issues to ensure alignment, understanding, and approval.*

- Encourage periodic audits for compliance.
- Check queries, sharing, access, vendor compliance, and retention standards.
- Conduct privacy impact reviews before using new technology.
- Retain a request-log: who requested, when requested, what data was provided, retention term, reason, and legal review (if any).

D. Responding to Law Enforcement Requests: Process and Protocols

If association representatives are required to respond to law enforcement requests for Association information and/or data, the following are guidelines to follow:

- Always be respectful:
    - *But there is no legal requirement to engage in a discussion with an ICE agent.*
- Obtain officer's name and badge number as it may not be clear what agency the official is from:
    - *"Officer, please give me your name, badge number and provide me with any warrant you have with you today. Are you with the police or ICE?"*
- Verify the authenticity and scope of the request:
    - *Look for valid subpoenas, court orders, or warrants. When in doubt, contact legal counsel.*
    - *Requests should be in writing and specify the exact data sought and the timeframe.*
    - *Do not provide data without proper authorization—avoid informal or verbal requests.*
- Generally, law enforcement officers may not enter private areas of the association premises, such as the management office or clubhouse, without a warrant signed by a judge or with consent of an authorized association representative.
    - *"I am not authorized to provide consent. May I take your contact information for follow-up?"*
    - *If state law prohibits or restricts sharing with immigration enforcement (as in California), implement mechanisms to detect and block unauthorized ICE queries or access.*

- Do not interfere:
    - *Do not physically interfere with officials even if they exceed authority.*
    - *If the situation escalates, contact local police to de-escalate the situation*.
- Notify someone:
    - *Designate a Board member or management supervisor with authority to speak with law enforcement (and train them as to the appropriate response).*
    - *Contact legal counsel.*
- Keep a record - follow a formal procedure to document the request, the data provided, and any communications.
    - *Make copies of all documents provided, **do not provide originals!***
    - *Maintain a record, including notes of the interaction that identify who said what and when.*

IV. Employment and Contractor Risks

Community associations face multilayered immigration compliance exposure through their employment and contracting relationships. Direct employees (on-site managers, maintenance personnel) create immediate verification obligations, while independent contractors (landscaping crews, security guards, janitorial services) may introduce secondary risks that some associations incorrectly assume they can ignore.

When ICE targets a vendor operating on association property, counsel must be prepared to advise on immediate response protocols, documentation requirements, and communication strategies to minimize disruption and liability exposure.

A. Independent Contractor Vulnerabilities

Due diligence expectations for vendor selection. Proper due diligence encompasses thorough documentation review, including I-9 employment eligibility verification forms, business licenses, contractor licenses, insurance certificates, and W-9 tax forms. If an association has failed to do basic due diligence, it may be roped into a compliance investigation or civil enforcement action. This means associations can't simply hire contractors without vetting their compliance practices. Associations should establish formal vendor review protocols, including obtaining written assurances of compliance with employment laws.

Specifically, contracts should include indemnity and representations of compliance with immigration and employment laws to provide legal protection. This documentation creates both a compliance paper trail and potential legal safeguards if enforcement issues arise later.

Shifting Liability Exposure. When engaging third-party contractors and vendors, community associations should consider shifting liability for employment-related claims to the contract through the terms of the services agreement. Some sample language that can be utilized in the management contract is the following:

> *Contractor shall comply with the Immigration Reform and Control Act of 1986, specifically the requirements with respect to employment eligibility verification, and further agrees to defend, indemnify and hold harmless the Association from any liability, costs, judgments, fines, or expenses, including any attorneys' fees, which the Association may incur as a consequence, directly or indirectly, as a result of Contractor's failure to comply with the requirements of these laws or any other laws.*

B. Overview of Employment Verification Requirements

The Immigration Reform and Controls Act of 1986 (IRCA) makes it illegal for a U.S. employer, regardless of size, to knowingly hire an unauthorized alien for employment or to hire a person for employment without going through the employment verification process.[27] Employers must verify that the person is not an unauthorized alien by examining documentation establishing both 1) employment authorization, and 2) identity through a combination of documents, such as a passport, green card, social security card or driver's license.[28] The hiring person must attest, under penalty of perjury, that the person is authorized for employment within the U.S.[29]

C. Form I-9 and Record-Keeping Obligations

The U.S. Citizenship and Immigration Services (USCIS), an office under the Department of Homeland Security (DHS),[30] has a prescribed form for employers to use to verify an employee or

[27] *See* 8 U.S.C. 1324a(a).
[28] *See* 8 U.S.C. 1324a(b).
[29] *See id.*
[30] Employment verification used to be handled by the U.S. Immigration and Naturalization Service (INS), an agency under the Department of Justice (DOJ). However, INS was dissolved in 2003 upon the enactment of the Homeland Security Act of 2002 and the creation of the Department of Homeland Security (DHS) after the 9-11 terrorist attacks. *See* 6 U.S.C. § 291. INS' duties were transferred to the U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP), which are agencies under DHS. *See id.* at § 542.

potential employee's eligibility to work in the United States. The prescribed form is known as the *Employment Eligibility Verification* Form or "Form I-9."[31]

Under IRCA, employers must retain a copy of Form I-9s in either paper, microfiche, microfilm, or electronic version, and make the forms available for inspection by officers of USCIS. The employer may also, but is not required to, copy or make an electronic image of the documents presented by the employee or prospective employee under Form I-9 establishing the employee's verification.[32] These documents must (i) be retained with the Form I-9 or stored with the employee's records and be retrievable consistent with federal regulations, which means there are reasonable controls in place to ensure the integrity, accuracy and reliability of the electronic generation or storage system and to prevent and detect unauthorized or accidental access; (ii) have an indexing system in place that permits the identification and retrieval for viewing or reproducing of relevant documents and records maintained electronically; and (iii) be able to be reproduced in legible and readable hard copies.[33] The Form I-9 must be maintained for 3 years after the date of hiring, or one year after the date the individual's employment is terminated, whichever is later.[34]

D. Inspection of Employment Verification Documents

Pursuant to federal regulations, authorized agency officials from the Office of Homeland Security Investigations (HSI) (an officer under DHS), the Department of Labor (DOL), and the Department of Justice (DOJ), to name a few, may request inspection of an employee's Form I-9 and related verifying documentations upon at least 3 business days' notice.[35] This request is referred to by HSI as a "Notice of Inspection." It is a formal letter issued by HSI informing an employer that its Form I-9 records will be audited.[36] A subpoena or warrant of probable cause is not required for officials to request inspection of this documentation, but use of those tools is not precluded.[37]

At the time of inspection, Forms I-9 and copies of the employee's verifying documentation (driver's license, social security card, etc.) must be made available in their original paper, electronic form, a paper copy of the electronic form, or on microfilm or microfiche at the location where the request for production was made.[38] If Forms I-9 are kept at another

[31] *See* 8 C.F.R. § 274a.2,(a)(2). A sample Form I-9 is provided in the exhibits and is available at http://www.uscis.gov.
[32] *See* 8 U.S.C. 1324a(b)(4).
[33] *See* 8 C.F.R. § 274a.2(b)(2).
[34] *See* 8 U.S.C. 1324a(b).
[35] *See* 8 C.F.R. § 274a.2(b)(2).
[36] A sample Notice of Inspection is included in the Appendix.
[37] *See* 8 C.F.R. § 274a.2(b)(2)(ii).
[38] *See id.*

location, the employer must inform the officer of the authorized agency of the location where the forms are kept and make arrangements for the inspection.[39]

The employer must make Forms I-9 available upon request at the location where officers request to see them.[40] The employer may also send Forms I-9 and supporting documents to the agency in electronic format or hard copy, if requested.[41] Inspections may also be performed at an office of an authorized agency of the United States.[42]

E. After the Notice of Inspection – 1 of 6 Possible Outcomes

Once the authorized agency receives the employer's response to the Notice of Inspection, the agency will determine one of the following:[43]

1) the employer is compliant and will issue a "Notice of Inspection Results" letter;

2) the documents presented do not relate to the employee or are otherwise not valid for employment. The agency will issue a "Notice of Suspect Documents", which warns the employer of penalties and allows for additional time to provide proper verification for the employee;

3) it is unable to determine the employee's eligibility. The agency will issue a "Notice of Discrepancies" which requires the employer to notify the employee of the determination and allows for additional time to present validating documentation for employment;

4) there are technical or procedural failures found during the inspection. The agency will issue a "Notice of Technical or Procedural Failures" which gives the employer at least 10 business days to correct the forms. After this correction period ends, uncorrected technical or procedural failures become substantive violations;[44]

5) substantive verification violations were identified, but there is an expectation of future compliance by the employer, in which case, the agency will issue a "Warning Notice." However, a Warning Notice will not be provided if the employer has a history of prior non-compliance; or

[39] *See id.*
[40] *See id.*
[41] *See* Section 10.3 of https://www.uscis.gov/book/export/html/59502.
[42] *See id.*
[43] *See* https://www.ice.gov/factsheets/i9-inspection.
[44] *See* 8 U.S.C. § 1324a(b)(6)(B)).

6) there are substantive violations, uncorrected technical or procedural failures, or knowing and/or continual violations. The agency will issue a "Notice of Intent to Fine." Upon receipt of such notice, the employer may make a request for a hearing before an Administrative Law Judge within 30 days.[45] If a written request for a hearing is not timely received, the agency will issue a Final Order.

F. Establishing a Good-Faith Defense and E-Verify

An employer can establish a "good faith" defense with respect to a charge of knowingly hiring an unauthorized alien, unless the government can show that the employer had *actual* knowledge that the employee was not authorized to work.[46] In other words, it's a rebuttable, affirmative defense that the employer is not in violation of IRCA.[47]

Employers may want to consider, after consultation with legal counsel, enrolling in the federal government's "E-Verify" program. E-Verify is a voluntary, free, online system for employers that takes the information entered by the employee on the Form I-9 and compares that information to records available in DHS and the Social Security Administration (SSA) databases to confirm employment eligibility.[48]

Once the employer goes through the enrollment process, employers have the ability to enter the employee's information into the E-Verify system online. From there, a case result is displayed, within seconds. The system may return one of the following results:

- Employment Authorized - The employee's information matched records available to DHS and/or SSA.
- E-Verify Needs More Time - This case was referred to DHS for further verification.
- Tentative Nonconfirmation (Mismatch) - Information did not match records available to DHS and/or SSA. Additional action is required.
- Case in Continuance - The employee has contacted DHS or visited an SSA field office, but more time is needed to determine a final case result.
- Close Case and Resubmit - DHS or SSA requires that you close the case and create a new case for this employee.

[45] *See* 5 U.S.C. § 554.
[46] *See* 8 U.S.C. § 1324a(a)(3).
[47] *See* 8 C.F.R. § 274a.4.
[48] https://www.e-verify.gov/.

- Final Nonconfirmation - E-Verify cannot confirm the employee's employment eligibility after the employee contacted DHS or SSA, the time for resolving the case expired, or DHS closed the case without confirming the employee's employment eligibility for some other reason.

If the initial case result is a Tentative Nonconfirmation (mismatch), the employer must notify the employee so the employee can decide whether or not to take action to resolve the mismatch. If the initial case result is E-Verify Needs More Time or Case in Continuance, it means E-Verify needs more time before a final case result can be given.[49]

To complete the E-Verify process, the employer must receive a final case result and close the case. Final case results include Employment Authorized, Close Case and Resubmit, and Final Nonconfirmation. E-Verify automatically closes cases resulting in Employment Authorized.[50]

Pros of the E-Verify System:

- Use of the E-Verify system is quick.
- Can reduce unauthorized employment.
- May minimize penalties in the event of a violation.

Cons of the E-Verify System:

- Not a substitute for Form I-9 completion.
- Will not stave off an audit or workplace inspection.
- Does not constitute a safe harbor.
- Allows DHS and SSA to audit an employer's data.
- Not available during a government shutdown.[51]

G. Employment Verification "Red Flags"

Some practices that may trigger cause for additional investigation and/or sanctions against the employer are the following:

- Form I-9s with no boxes checked or multiple boxes checked;

---

[49] https://www.e-verify.gov/employers/verification-process.
[50] *See id.*
[51] *See* Peck, Amy, *The Pros and Cons of Registering for E-Verify*, SHRM (June 10, 2019), https://www.shrm.org/topics-tools/news/talent-acquisition/pros-cons-registering-e-verify; *see also* Martinez, Alonzo, *https://www.forbes.com/sites/alonzomartinez/2025/10/02/government-shutdown-freezes-e-verify-what-employers-must-do-now/* (Oct. 2. 2025).

- Form I-9s with missing signatures;
- Incorrect verification documents provided;
- Not completing the Form I-9s timely;
- Clearly falsified or missing documentation; and/or
- Social security number mismatches; to name a few.

Additionally, using labor subcontractors to avoid direct hiring liability can also be red flag for agencies.[52] Employers should keep in mind that agencies may pursue anonymous tips from whistleblowers or immigration "vigilantes." Finally, a history of non-compliance is cause for further investigation or enforcement. All of these may lead to more than just a Warning Notice, including sanctions, criminal prosecution and debarment are available enforcement tools.[53]

H. State and Local Mandates

States vary regarding the requirement of employers to utilize E-Verify for employment verification. Some states impose mandatory E-Verify participation through the Federal electronic employment eligibility verification system, such as Arizona.[54] Other states, like California[55], have established various sanctuary provisions limiting cooperation with federal immigration enforcement. Some states, like Virginia, only require use of the E-Verify system for public employees and government contractors of a certain size,[56] while other states, like Maryland, have no legislation either way, which means that an employer's participation in the program is completely voluntary.

In evaluating what obligations a particular community association may have in this area, practitioners may be required to navigate a complex patchwork of state-specific employment verification requirements. These jurisdictional variations create significant compliance challenges for management companies and attorneys who serve associations across multiple states. As a result, associations must understand their specific state requirements rather than assuming a one-size-fits-all approach to compliance.[57]

---

[52] *See* 8 C.F.R. § 274a.5. ("[a]ny person or entity who uses a contract, subcontract, or exchange entered into, renegotiated, or extended after November 6, 1986 . . . to obtain the labor or services of an alien in the United States knowing that the alien is an unauthorized alien with respect to performing such labor or services, shall be considered to have hired the alien for employment in the United States in violation . . . of the Act").
[53] "Debarment" is an administrative process that renders an individual or entity ineligible to participate in or receive governing contracts, loans, grants, and assistance programs.
[54] Ariz. Rev. Stat. § 23-214 (2025).
[55] Cal. Lab. Code § 28-11-2814 (2025).
[56] Va. Code § 2.2-4308.2 (2025).
[57] A state-by-state compendium of E-Verify requirements is included in the Appendix.

I. Summing It All Up: Implications for Associations and Management Companies Establishing a Compliance Process.

Community associations with on-site employees, whether its own hires or employees of their management agent, should establish a compliance process for employment verification of such employees. The process should include the following:

- **Designating the appropriate person** to conduct the employment verification process and sign the Form I-9s. This could be a general manager, portfolio manager, or management company human resource professional. *Board members should not be involved in this process due to the sensitivity of the task and the personal information being collected and maintained.*

- **Establishing protocols** for the storage of employment verification records that meets federal requirements for security and retrieval, whether in paper or electronic form. Community associations need to determine who is the custodian of these records, who has access to the records, and the process for retrieval in the event the community association receives a Notice of Inspection. It is recommended that Form I-9s be kept separate from personnel files for easier retrieval and to protect other employment information from accidental disclosure.

- **Understanding management's process** of storing and retrieval of documents, the location of the documents and who the association can contact at management for assistance in the event the association receives Notice of Inspection.

- **Confer with legal counsel** on next steps if a Notice of Inspection is received.

Recognizing a Workplace Audit/Inspection. While typically the Notice of Inspection letter is mailed to the employer, there are recent reported instances of immigration officials visiting employers at physical workplaces with the Notices of Inspection in-hand and demanding access to employment records on the spot[58] even though the applicable statutory provisions give employers 3 business days to respond. DHS regulations do allow immigration officials to conduct workplace inspections at the employer's place of business;[59] however, the 3 business days' notice is still required. Either way, such an occurrence can be very jarring for managers, desk attendants, concierge staff, and other personnel who are not regularly involved in the employment verification process.

[58] Smith, Jilliam, *ICE says 'workplace inspections' conducted at 100 DC restaurants* (May 7, 2025), https://www.fox5dc.com/news/ice-says-workplace-inspections-conducted-100-dc-restaurants.
[59] *See* 8 C.F.R. 287.8(f).

The reality is that such "front line," resident-facing personnel are not able to and should be prohibited from complying with such a demand. It is likely that employment records are either kept in a locked file cabinet or secured area that only certain supervisory personnel have access to, or the records are stored electronically with management or a human resources compliance company.

When faced with a workplace audit visit, staff should remain calm, accept receipt of the Notice of Inspection, and document the visit. From there, association legal counsel should be contacted immediately to coordinate the record retrieval process to ensure timely response and to ensure that the immigration officials are acting with appropriate authority. Employment verification records should never be provided on the spot without an actual judicial warrant, which is discussed and distinguished in these materials. Employers are permitted to request more time to provide the verification documentation and that request should be made through legal counsel.

Site staff should also be aware that a "workplace inspection" conducted for specific employment verification document is not the same as an "ICE raid." An "ICE raid" specifically targets unauthorized workers for enforcement for immigration laws of persons who entered the country illegally or have otherwise breached terms of entry, as discussed more in these materials.

Understanding Management's Recruiting and Hiring Practices. When engaging a management agent and negotiating management contracts, community associations should inquire as to whether management has outsourced human resources functions to an affiliate or third-party compliance company. Community associations should also ensure that management has adequate insurance coverage to protect against claims of unauthorized disclosure of personnel employment records. Please note that the IRCA's employment verification process applies not only when hiring but also recruiting as well.[60]

Final Thoughts. Workplace audits can pose legal and operational challenges for community associations, especially those that employ staff or contract with vendors who may be subject to immigration enforcement. While associations may not be the direct target of audits, they have a responsibility to ensure compliance with employment verification laws, including proper completion and maintenance of Form I-9s. A proactive approach, such as reviewing hiring practices, working only with reputable vendors, and consulting legal counsel when necessary, can help mitigate risk and avoid costly penalties. Ultimately, preparedness and

[60] *See* 8 U.S.C. § 1324a.

transparency are key to navigating workplace audits while maintaining the integrity and legal standing of the association.

V. Discrimination, Fair Housing & Liability

A. Immigration Status and Citizenship: Protected Classes Under the Fair Housing Act?

The federal Fair Housing Act ("FHA") prohibits housing providers from discriminatory practices based on one's race, color, religion, sex, national origin, familial status, and disability.[61]

Does this include "immigration status" or "citizenship?

The answer is no. While some may argue that "national origin" relates to one's immigration or citizenship status, courts have held that "national origin" as a protected class does not specifically extend protections based on citizenship or immigration status.[62] "National origin" usually refers to the "country where a person was born, or, more broadly, the country from which his or her ancestors came."[63] But, the protection does not specifically extend beyond that.

However, that does not necessarily mean that a fair housing claim cannot go forward if other protected classes are implicated, like race and national origin. The case of *Reyes v. Waples Mobile Home Park Limited Partnership*, 903 F.3d 415 (4th Cir. 2018),[64] which continues to be in active litigation, highlights this type of interplay between fair housing and immigration laws.

B. A Case Study: *Reyes v. Waples Mobile Home Park Limited Partnership*

Four Latino couples living at Waples Mobile Home Park in Fairfax County, Virginia challenged the mobile home park's policy requiring all occupants to provide documentation evidencing legal status in the U.S. in order to renew their leases.[65] The plaintiffs contended that the policy violated FHA because it disproportionately ousted Latinos from residing in the mobile home park, as compared to non-Latinos, on the basis of race and national origin.[66] The

---

[61] *See* 42 U.S.C. § 3604.

[62] *See Corwin v. B'Nai B'Rith Senior Citizen Housing, Inc*., 489 F.Supp.2d 405 (D. Del. 2007).

[63] *Espinoza v. Farah Mfg. Co.,* 414 U.S. 86, 88 (1973) (superseded by statute). *Espinoza* involved a Title VII challenge alleging that an employer's policy of not hiring aliens amounted to discrimination against the plaintiff in that case because of her national origin of Mexico.

[64] Citations to this case either note the named plaintiff as "*Reyes"* or "*de Reyes"* due to the long procedural history and because the plaintiffs are related to each other.

[65] *See de Reyes v. Waples Mobile Home Park Limited Partnership,* 251 F.Supp.3d 1006 (E.D. Va. 2017).

[66] The tenants were given 21 days to provide an original social security card, an original passport, U.S. visa, and original arrival/departure Form I-94 or I-94W. If they could not produce the documentation, they had 30 days to vacate.

plaintiffs in the case were all non-citizen Latinos of Salvadorian or Bolivian national origin. The four male plaintiffs had a social security number and have provided documentation to satisfy the mobile home park's policy, but the four female plaintiffs could not satisfy the policy because each female plaintiff was an illegal immigrant. Notably, the ten children living with plaintiffs were all U.S. citizens.

The plaintiffs alleged that the policy violated FHA because it disproportionately ousted Hispanic and Latino families from their homes and denied them residence in one of the only affordable housing options in the local area. To support their argument, the plaintiffs provided statistical evidence of the strong link between the undocumented immigrant population and the Latino population to demonstrate that any policy that adversely affects the undocumented immigrant population will likewise have a significant disproportionate impact on the Latino population. The data included statistics that Latinos constituted 64.6% of the total undocumented immigrant population in Virginia at the time of the case and that Latinos are 10 times more likely than non-Latinos to be adversely affected by the mobile home park's policy, as undocumented immigrants constituted 36.4% of the Latino population in Virginia compared with only 3.6% of the non-Latino population. The plaintiffs submitted evidence that Latinos are nearly twice as likely to be undocumented compared to Asians, and twenty times more likely to be undocumented than other groups. They also submitted evidence that 60% of the tenants within the mobile home park were Latino, and that 11 of the 12, or 91.7% of the tenants at the park who were not in compliance with the policy as of May 2016 were Latino.

The district court dismissed the disparate impact claim under Rule 12(b)(6) on the basis that the plaintiffs failed to show a robust causal connection between the defendant's challenged policy and disparate impact on a protected class because the policy at issue was targeted towards race or national origin under FHA. The district court also granted summary judgement in favor of the mobile home park on disparate treatment claim because 60% of the park was Latino and the male plaintiffs were allowed to remain on the premises, thus negating any direct disparate treatment.[67]

On appeal, the 4th Circuit determined that the plaintiffs had actually sufficiently alleged a *prima facie* case of disparate impact due to the statistical evidence that was produced and should have been allowed to pursue that cause of action further. It determined that the lower court erred in dismissing that claim at a preliminary stage. The appeals court also vacated the summary judgement ruling on the disparate treatment claim.

Specifically, the 4th Circuit found that the lower court made a "grievous error" in concluding that the female plaintiffs' immigration status precluded them from making a *prima*

[67] *See de Reyes at* 1021.

facie showing of disparate impact.[68] The appeals court reasoned that the district court attempted to distinguish a claim of disparate impact based on immigration status, as opposed to race or national origin, but there was evidence that the policy disproportionately targeted the plaintiffs based on race and national origin anyway. The 4th Circuit was persuaded by dicta from U.S. Supreme Court in *Espinoza v. Farah Mfg. Co.* when it stated "[c]ertainly Tit. VII prohibits discrimination on the basis of citizenship whenever it has the purpose or effect of discriminating on the basis of national origin.… The Act proscribes not only overt discrimination but also practices that are fair in form, but discriminatory in operation."[69]

But *Reyes* does not stop there. The 4th Circuit remanded the case, in which the plaintiffs then pursued only a disparate-impact theory for their FHA claim. Both sides filed motions for summary judgement, which were both denied. As the parties were preparing for trial, the case was reassigned to a new district court judge who reversed course and granted summary judgment in favor of the mobile home park.[70] The park had argued that it met its burden under the *Inclusive Communities* analysis[71] at summary judgment because the policy of requiring evidence of residents' legal status was necessary to serve several valid interests under IRCA's anti-harboring statute, such as verifying identity, conducting criminal background checks, avoiding loss from eviction, and avoiding further liability.[72] IRCA's anti-harboring statute makes it a criminal offense to knowingly or recklessly assist an undocumented immigrant from entering or remaining in the U.S. illegally, such as providing shelter, transportation, or other similar assistance, with certain exceptions.

The families countered that summary judgment was improper because there were triable issues of fact as to whether the park could satisfy the second step of *Inclusive Communities* framework; specifically, whether the policy served a valid interest, and, if so, whether such an interest could be served through less discriminatory means by applying the policy only to leaseholders as opposed to all tenants in residence.[73] However, the district court found that

---

[68] *Reyes v. Waples Mobile Home Park Limited Partnership,* 903 F.3d 415, 429 (4th Cir. 2018), *rehearing en banc denied* (Dec. 19, 2018)), *cert. denied*, 87 U.S. 987 (May 13, 2019).
[69] *See Espinoza* at 92 (citing *Griggs v. Duke Power Co.,* 401 U.S. 424, 431 (1974)).
[70] *See de Reyes v. Waples Mobile Home Park Limited Partnership,* 602 F.Supp.3d 890 (E.D. Va. 2022).
[71] *Texas Department of Housing and Community Affairs v. Inclusive Communities Project, Inc.,* 576 U.S. 519 (2015). Under *Inclusive Communities* framework, the plaintiff bears the initial burden of establishing a prima facie case of disparate impact by showing a robust causal connection between the defendant's challenged policy and the disparate impact on the protected class. If satisfied, the burden shifts to the defendant to show that the discriminatory policy was necessary to achieve a legitimate non-discriminatory interest. If the defendant does so, the burden shifts back to the plaintiff to show that the interest could be served through less discriminatory means.
[72] *See Reyes* at 898 *(referring to* 8 U.S.C. § 1324(a)).
[73] *See id.*

the park met its burden because "implementing a policy to avoid increased criminal liability under the anti-harboring statute is a valid and necessary interest."[74]

The families appealed again, and the 4th Circuit considered the case *de novo.*[75] The appeals court noted that while employers are required to vet the immigration status of their employees or face civil and criminal sanctions under the employment verification requirements of IRCA, no such requirement exists for housing providers.[76] The lease agreement alone is too attenuated to establish "harboring." The appeals court recognized that such a policy of discouraging or prohibiting housing for any undocumented person could lead to an unsustainable level of homelessness. The appeals court also noted that Congress could modify its approach to housing policy at any time it so desires.[77]

The 4th Circuit also noted that the park's policy did not serve a business necessity under the *Inclusive Communities* framework.[78] The appeals court noted that plaintiffs had been residing at the mobile park for years before the park started enforcing the policy, negating the park's claim that it was concerned about anti-harboring under IRCA. Accordingly, the 4th Circuit found that the grant of summary judgement in favor of the mobile home park was improper and remanded the case back to the lower court once again.[79]

> ***Practitioner's Note:*** *This case is one that legal practitioners should monitor closely, as the interplay between federal fair housing laws and immigration laws is well-highlighted in the court's analysis. A final resolution of the case can have wide implications for community associations.*

C. Application of HUD "Hostile Environment" Regulations

For community association attorneys, the fair housing concern may present itself in the form of a resident's claim of hostile environment under the Department of Housing and Urban Developments (HUD) regulations on the basis of the resident's immigration status or citizenship, masking as discrimination based on race or national origin.[80] Hostile environment harassment is defined as "unwelcome conduct that is sufficiently severe or pervasive as to interfere with "the availability, sale, rental, or use or enjoyment of a dwelling; the terms, conditions, or privileges of the sale or rental, or the provision or enjoyment of services or

---

[74] *See id.* at 899.
[75] *Reyes v. Waples Mobile Home Park Limited Partnership,* 91 F.4th 270 (4th Cir. 2024), *cert. denied,* 145 S. Ct. 172 (Oct. 07, 2024).
[76] *See id.* at 278.
[77] *See id.*
[78] *See id.* at 279.
[79] *See id* at. 280.
[80] *See* 24 C.F.R. § 100.600(a)(2).

facilities in connection therewith; or the availability, terms, or conditions of a residential real estate-related transaction. Hostile environment harassment does not require a change in the economic benefits, terms, or conditions of the dwelling or housing-related services or facilities, or of the residential real-estate transaction."[81]

For example, a Board member or another resident of a community may make assumptions about a resident's immigration status based on their race or national origin and may target them on that basis through threats, intimidation, or other actions meant to interfere with the resident's use and enjoyment of the premises. In those cases, the association likely has a duty to address the conduct and take corrective action under the direct or vicarious liability requirements of the regulations.[82]

The issue is further highlighted in the context of an ICE warrant. A Board member or resident may feel compelled to cooperate with ICE officers in the execution of an ICE warrant in identifying or locating a particular resident, which can lead to claims of discrimination, especially the hostile environment provisions of the HUD regulations.

Any actual or perceived bias in handling residents, especially in response to law enforcement or ICE inquiries, can expose associations to civil rights violations and HUD complaints. This highlights the importance for community associations to designate a person with authority to interact with immigration officials on behalf of the association, such as a manager or legal counsel. A Code of Conduct for Board members is a valuable tool to stave off actions taken by Board members outside of their authority.

D. State and Local Fair Housing Laws: Immigration Status and Citizenship as Protected Classes and Expanded Protections

Community association legal practitioners also should keep in mind the application of state and local level fair housing protections. At this time, most states do not extend fair housing protections to persons based on immigration status or citizenship. Only California and Illinois have expanded state fair housing laws to protect persons from discrimination in housing based on citizenship and immigration status:

- **California (AB 291, Civil Code § 1940.3)**: Prohibits landlords, HOAs, and housing providers from inquiring about or using immigration status in any housing decision, including data sharing or enforcement.[83]

---

[81] *Id.*

[82] *See* 24 C.F.R. § 100.7.

[83] *See* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB291 (CA Tenant Protection Act, AB 291 (chaptered Oct. 5, 2017).

- **Illinois (775 ILSC 5/3-101 (2025)):** Illinois amended its Human Rights Act in 2024 to prohibit discrimination in any housing-related dealings based on an individual's immigration status, which is defined as "a person's actual or perceived *citizenship* or *immigration status*."

Municipal and local level jurisdictions within states may be more robust in extending fair housing protections to persons based on their immigration status and/or citizenship. Here are some examples:

- **New York City - T**he New York City Human Rights Law makes it illegal to be denied a housing opportunity because of one's immigration or citizenship status, which is defined as the immigration status or citizenship of any person who is not a citizen or national of the United States - N.Y.C. Admin. Code 8-107.5(a).
- **Prince George's County, Maryland –** The County incorporates immigration status as a protected class in its human rights statute - Prince George's Co., Md., Subtit. 2, Div. 12, Sec. 2-210 (2025).

Training Tip. *Know your state and local jurisdiction's full list of protected classes and train staff accordingly, especially when handling data requests, complaints, or enforcement.*

E. Immigration Status as a Protected Class in Employment

When undergoing the employment verification requirements, employers need to be careful not to run afoul of employment discrimination laws during the recruiting and hiring process. Under the Immigration and Nationality Act, employers with 4 or more employees cannot discriminate when hiring, firing, or recruiting because of someone's citizenship or immigration status.[84] Citizenship or immigration status discrimination occurs when an employer treats someone di erently en irin , firin , or recruitin ecause of t e person s real or perceived citizenship or immigration status.

Some practical tips to stave off claims of immigration-related employment discrimination in hiring are:

- Make sure job announcements and descriptions are clear about the position being advertised.
- Include a statement of equal opportunity on job listings.
- Prepare interview questions that are related to the role. Do not delve into the applicant's family life, religious practices, or background.

[84] *See* 8 U.S.C. § 1324b.

- Select interviewers from a cross-section of the employer.
- Avoid unconscious biases – confirm the pronunciation of the applicant's name and preferred pronouns.
- Limit humor to reduce the risk of making an off-putting comment.
- Document all stages of the hiring process.

F. Fair Housing Liability Traps: Over-Compliance, Improper Refusal, and Discriminatory Practices

Community associations can face significant civil or even criminal exposure if procedures are not carefully followed. Common traps include:

Over-Compliance. Voluntarily handing over surveillance footage, license plate logs, or resident info without proper legal compulsion (*e.g.*, subpoena or warrant). Even well-meaning cooperation can lead to claims of privacy invasion or discrimination.

Improper Refusal. Denying a data or enforcement request without proper documentation or process can appear arbitrary or retaliatory, especially if the person involved is a protected class member.

Disparate or Discriminatory Treatment. Unequal enforcement of rules, differential responses to similar complaints, or selective cooperation with law enforcement can be interpreted as discriminatory intent. Selective enforcement presents a particular danger. Associations that appear to target specific ethnic groups or that apply different standards based on perceived immigration status invite costly litigation and potential damages. Even well-intentioned policies can create liability if they have disparate impacts on protected groups.

Boards should be given clear guidance so they can avoid becoming unofficial enforcement proxies; a role which they're neither authorized nor equipped to perform. Well-meaning, but legally uninformed boards might implement unauthorized verification requirements, establish reporting mechanisms, or create policies that inappropriately monitor residents based on perceived immigration status. Counsel needs to help boards understand where their responsibilities end and where they might inadvertently cross into unauthorized enforcement activities. This guidance should include protocols for responding to government information requests without overstepping into proactive enforcement.

G. Importance of Neutral, Documented Procedures to Mitigate Exposure.

Whether a resident who may be subject to an ICE investigation would feel comfortable filing a claim of discrimination with a local, state, or federal human rights office is unclear.

Nevertheless, community associations can take steps to ward off Fair Housing violations in the context of ICE activity, as follows:

- Never ask about a resident's immigration status or national origin during occupancy, enforcement, or compliance resolution.
- Keep responses to community questions about ICE activity neutral and the subject of the ICE activity confidential.
- Advise residents not to interfere with ICE activities or attempt to take matters into their own hands.
- Assure the community that unit and lot files, which are likely to contain contact and vehicle information for residents, are kept confidential and will not be disclosed to officials unless subject to a judicial subpoena or warrant. Maintain strict privacy protocols for all surveillance or resident data.
- Train staff on implicit bias and housing discrimination laws, especially regarding language, national origin, and perceived immigration status.
- Adopt an anti-discrimination policy.
- Bring in a trusted speaker to explain local ICE activity in general terms (community resource officer, local elected official, etc.).

VI. Conclusion

Community associations sit at a volatile intersection of private governance, public enforcement, and rapidly evolving expectations around privacy and discrimination, and counsel can no longer afford to treat ICE encounters or law-enforcement data demands as "edge cases." The practical charge for community association lawyers is to convert the legal principles outlined in this manuscript into clear, repeatable playbooks: training boards and staff to distinguish warrant types, to control access to private areas and data, to channel all interactions through designated points of contact, and to apply neutral, documented procedures that avoid turning the association into a de facto immigration-enforcement arm.

That same discipline should also extend to vendor contracts, employment practices, surveillance technologies, and fair housing compliance, so that each potential point of exposure is backed by thoughtful drafting and consistent implementation rather than improvisation at the front desk. By building that infrastructure now, practitioners help their clients respect legitimate law-enforcement objectives while honoring constitutional protections, state and local privacy regimes, and anti-discrimination obligations. In short, the goal is not to stop ICE "at the gate," but to ensure that when enforcement does arrive, the association responds in a way that is lawful, defensible, and aligned with its duties to the community it serves.

VII. Appendix and Additional Resources

A. Appendix of Exhibits

i. Sample ICE Warrant

ii. Sample U.S. District Court Judicial Warrant

iii. Surveillance Camera Policy Samples

iv. Standard Form I-9 Employment Verification

v. Sample Notice of Inspection to Employer

vi. Multi-State Sample of E-Verify Requirements

vii. Sample Policy: Response to ICE Inquiries (CA Specific)

B. Recommended Resources

i. CAI National, Guidance for Community Associations Handling ICE Requests (authored by Leslie Brown, Esq. and J. David Ramsey, Esq, CCAL; released March 5, 2025).

ii. Eric Finke, CMCA, AMS, PCAM, *Closing Out the Year Strong: How Montebello's Partnership with Law Enforcement Helped Solve a Homicide*, Quorum Magazine, CAI-CAWM, Dec. 2025 (www.quorum-digital.com/cawm/december_2025/).

U.S. DEPARTMENT OF HOMELAND SECURITY **Warrant for Arrest of Alien**

File No. _____

Date: _____

To: Any immigration officer authorized pursuant to sections 236 and 287 of the Immigration and Nationality Act and part 287 of title 8, Code of Federal Regulations, to serve warrants of arrest for immigration violations

I have determined that there is probable cause to believe that _____ is removable from the United States. This determination is based upon:

☐ the execution of a charging document to initiate removal proceedings against the subject;

☐ the pendency of ongoing removal proceedings against the subject;

☐ the failure to establish admissibility subsequent to deferred inspection;

☐ biometric confirmation of the subject's identity and a records check of federal databases that affirmatively indicate, by themselves or in addition to other reliable information, that the subject either lacks immigration status or notwithstanding such status is removable under U.S. immigration law; and/or

☐ statements made voluntarily by the subject to an immigration officer and/or other reliable evidence that affirmatively indicate the subject either lacks immigration status or notwithstanding such status is removable under U.S. immigration law.

YOU ARE COMMANDED to arrest and take into custody for removal proceedings under the Immigration and Nationality Act, the above-named alien.

_____
(Signature of Authorized Immigration Officer)

_____
(Printed Name and Title of Authorized Immigration Officer)

Certificate of Service

I hereby certify that the Warrant for Arrest of Alien was served by me at _____
(Location)

on _____ on _____, and the contents of this
(Name of Alien) (Date of Service)

notice were read to him or her in the _____ language.
(Language)

_____ _____
Name and Signature of Officer Name or Number of Interpreter (if applicable)

UNITED STATES DISTRICT COURT

for the

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)))))))	Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: _____ _____
Judge's signature

City and state: _____ _____
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Print Save As... Reset

ASSOCIATION

POLICY RESOLUTION NO. 20-_____

(Policy for Access, Viewing and Liability Limitations of Security Camera Footage)

WHEREAS, Article III, Section 3.04 of the Declaration of Covenants, Conditions, Restrictions and Reservation of Easements ("Declaration") provides that the business and affairs of the Association ("Association") shall be managed by a Board of Directors ("Board"); and

WHEREAS, Article II, Section 2.01(a) of the Declaration provides the Board with the right to adopt, promulgate, enforce, and, from time to time, amend reasonable rules and regulations pertaining to the use of the Community Facilities which shall enhance the preservation of such facilities and the safety and convenience of the users; and

WHEREAS, Article IV, Section 4.01 of the Bylaws authorizes the Board to adopt and publish rules and regulations governing the use of the Common Area and the personal conduct of the Members and their guests thereon; and

WHEREAS, Article III, Section 3.06 of the Declaration states that the Association shall not be liable to any Members for loss or damage, by theft or otherwise, of articles which may be stored upon the Common Area or its facilities; and

WHEREAS, the Board has taken measures to install security features on Association property, to include, but not be limited to, security camera(s) on Common Area and Community Facilities; and

WHEREAS, the Board deems it in the best interest of the Association to establish and publish such rules relating to the access to and limitations of security camera footage given the possibly private and/or sensitive nature of the footage.

NOW THEREFORE, BE IT RESOLVED that the Board adopts the following policies and procedures regarding security camera recordings:

A. Access to and viewing of the security camera footage shall be limited to the members of the Board of Directors and management for the Association as camera data may include sensitive information.

B. Security camera data will generally only be used to extent necessary to protect the Association's property, but data gathered may be used in the enforcement of the Association's Rules and Regulations, at the discretion of the Board of Directors.

C. Member Access to the security camera recordings/footage shall be limited to the extent available at law under the POA Act or other applicable local, state or federal laws. Requests to view the security footage shall be made in accordance with the applicable requirements under the law. Since camera data can include sensitive information about

the comings and goings of residents of the community and their guests, in most cases requests by a Member to examine camera footage will need to be accompanied by evidence of a subpoena for the records or to further an active police investigation unless otherwise required by law.

D. Requests from law enforcement to review the footage will be determined on a case by case basis at the discretion of the Board of Directors. Since camera data can include sensitive information about the comings and goings of residents of the community and their guests, in most cases requests by law enforcement to examine camera footage will need to be accompanied by evidence of a subpoena for the records or to further an active police investigation unless otherwise required by law.

E. The Association assumes no liability or responsibility for any malfunction or failure of the security cameras, or the scope of footage obtained by the camera(s).

F. No Member or Resident shall rely on the security cameras for protection, defense from theft or damage to their person or Lot, or for evidence otherwise. The Association assumes no liability for any damage or harm to a Member, Resident or their property that may occur in areas where there are or are not security camera(s).

G. Security cameras will not be actively monitored, but instead, the footage will be reviewed retrospectively as circumstances require. No Member or Resident shall assume that the security cameras are being actively monitored or will provide active assistance in the event a Member or Resident is injured or in other need of active assistance by medical personnel, law enforcement, or otherwise.

H. Generally, recordings that are made by the security cameras shall be kept for a maximum of 48 hours before being deleted. The Board of Directors and management may decide to keep the recordings for a longer period of time if they determine in their sole discretion to do so.

I. While the Association's policy is to keep recordings for at least 48 hours, the Association assumes no liability for failure to do so.

This Resolution shall be effective upon its adoption and shall supersede and replace any previous Resolution or rules governing the recording of meetings.

ALTERNATIVE LANGUAGE (if applicable):

NOW THEREFORE, BE IT RESOLVED that the Board adopts the following policies and procedures regarding security camera recordings:

I. REQUESTS TO REVIEW/COPY RECORDED INFORMATION

A. Generally, recordings that are made by the security cameras shall be kept for a maximum of 48 hours before being recorded over. The Board of Directors and management may

decide to keep the recordings for a longer period of time if they determine in their sole discretion to do so.

B. If a Unit Owner would like to review and/or copy a recording, the Unit Owner must submit a written request to management by the next business day after the recording was made and such request must include:

1. The purpose for which the recorded footage is being requested,

2. The location of the specific camera that is of interest to the requestor,

3. The date and time when the footage was believed to have been recorded, and

4. Whether the requestor would like a copy of the footage or simply the opportunity to review it.

D. Requests to review or copy the recordings will be denied by the Board of Directors if they are not for a proper purpose (i.e. are for pecuniary gain, for harassment, or similar purposes) and the requestor shall be notified in writing that the request has been denied and the reason for the denial shall be provided. Management shall have the right to approve such requests only if the request includes a subpoena for the records or proof of an active police investigation. Otherwise, such request shall be reviewed by the Board.

E. Review of Recording.

1. If the request to review is approved, and the recording is controlled by a third party (e.g. a security company) and the Council must pay to save and make the footage accessible, the requestor must pay the charge assessed by such third party for the footage before management will schedule a time for the requestor to review the recording.

2. Within twenty-one (21) days of the date of the request, management shall schedule a time for the footage to be reviewed.

3. A reasonable charge shall be assessed for the staff's time to assist the requestor in reviewing the footage. Such charge shall be based on the length of time required to review the recording and an estimated total cost will be provided to the requestor. The requestor must pay that estimate prior to being given the opportunity to review the footage. Any overage paid to the Council after determining the actual expense will be promptly refunded.

G. Copy of Recording. If the request for a copy is approved, and the recording is controlled by a third party (e.g. a security company) and the Council must pay to save and make the footage accessible, the requestor must pay the charge assessed by such third party for the footage and the duplication of the same before management will provide the requestor with a copy of the recording.

H. The Council shall have the discretion to release video footage to the policy and/or any other authorities in the event that an alleged crime is discovered on the surveillance footage and/or if such footage is requested by the authorities.

II. LIMITATIONS

A. The Council assumes no liability for any malfunction or failure of the security cameras.

B. The Council shall have no responsibility and/or lability for the security of owners, residents, tenants or guests and/or the assets of such persons. The installation of cameras shall in no way warrant protection to any owners, resident, tenants, guests or property.

C. While the Council's policy is to keep recordings for at least 48 hours, the Association assumes no liability for failure to do so.

D. If a Unit Owner submits a written request for a recording, it is the Unit Owner's obligation to follow up with management to ensure that the request was received, and the recording has been preserved.

E. Unit Owners are prohibited from posting the recording online without the Council's permission, including websites and all forms of social media.

SURVEILLANCE CAMERA POLICY

Adopted _____

After careful consideration, the Association has determined that use of devices capable of video surveillance and/or recording ("Surveillance Cameras") is important in efforts to enforce the Association's Governing Documents, as well as attempts to deter vandalism or other acts that may damage property in the Association Surveillance Areas (defined below).

Accordingly, in light of these purposes and in compliance with privacy laws governing the collection of personal information, the Association has adopted this Surveillance Camera Policy.

Association's Use of Surveillance Cameras

1. The Association may install, or has installed, Surveillance Cameras in and around the Project, including, but not limited to the entrance and pool areas. Additional cameras may be installed in other Common Property areas as deemed necessary by the Board in the future ("Association Surveillance Areas").

2. The Board elected to install Surveillance Cameras to monitor certain Association Surveillance Areas because of the increased potential for non-compliance with the Governing Documents or other instances of vandalism or destruction of property.

3. The Association will ensure that signs identifying the presence of Surveillance Cameras are clearly posted within the pool area.

4. The Surveillance Cameras will not be directed or set to view or record the bathrooms of the pool area or inside any of the Residences or other areas deemed under the law to have a reasonable expectation of privacy.

5. The Association intends for the Surveillance Cameras to be used for passive recording purposes. The Surveillance Cameras include digital video recording equipment, which will record images, which will then be viewed only in the event that any of the Association Surveillance Areas are vandalized or when the Association is made aware of violations of the Governing Documents or potential criminal activity in the Association Surveillance Areas.

6. Live feeds of the Surveillance Cameras may occasionally be viewed in the event the Association Surveillance Areas are being vandalized or when the Association has been made aware that violations of the Governing Documents or other criminal activity is taking place in the Association Surveillance Areas.

7. The individuals permitted to view live or recorded images from the Surveillance Cameras include the Association's community manager or any patrol personnel retained by the Association. Members of the Board are not authorized to view live or recorded images from the Surveillance Cameras unless circumstances require (such as when necessary due to emergency or provided for review as evidence related to a violation hearing).

8. Although the primary use of the Surveillance Cameras is to attempt to deter vandalism or other damage to property in the Association Surveillance Areas, the Association makes

no warranty, express or implied, as to the safety of persons residing in or entering the Project or to their personal or real property.

9. Pertinent footage of an event which has occurred, including but not limited to, vandalism, property damage, litigation evidence, criminal activity, insurance investigation and suspicious activity or specific issues of concern may be released by the Association for the purpose of identifying the individuals involved or notifying the residents of such activity.

10. If access to video surveillance is requested for the purpose of law enforcement investigation due to criminal activity or potential criminal activity, pertinent footage related to the investigation may be provided to law enforcement officials upon approval by the Board.

11. To protect the privacy of the individuals within the Association, no recordings, photos, images, or any other information obtained through the recording process will be made available to requesting Members or residents absent receipt of a valid court order or subpoena.

All Owners are responsible to ensure that their family members, employees, visitors, guests, tenants, agents, and invitees observe and comply with all Association Governing Documents, including those Rules and Regulations adopted by the Board of Directors.

SURVEILLANCE CAMERA POLICY

MEMBER INCIDENT PRESERVATION REQUEST

For Owners to request that the Association preserve potentially relevant footage within the standard retention period.

Instructions: Submit by email to _____ or via the owner portal within 15 days of the subject incident, sooner if possible. Please note that incomplete or overbroad requests may delay processing and could result in the Association being unable to facilitate the request.

A. Requestor Information

- Member Name: _____
- Property Address / Unit No.: _____
- Mailing Address (if different): _____
- Phone: _____ Email: _____

B. Subject Incident Details

- Date of subject incident: _____
- Approximate time window (max. 1 hour, absent Board approval based on good cause): _____
- Location (check one or more):

  ☐ [ ] main entry/exit gate

  ☐ [ ] entry/exit gate

  ☐ Other common area (describe): _____
- Brief description of incident (facts only; attach any photos/documents):

C. Law Enforcement (if applicable)

- Police agency notified: _____
- Report/Case/Incident No.: _____
- Officer/Contact (if known): _____

D. Acknowledgments (initial each)

____ I understand this request is for **preservation only**; it does **not** guarantee that footage exists, is usable, or will be captured within the field of view.

____ I understand the Association **does not provide copies** of surveillance footage to Members or Residents. The Association may release footage **to law enforcement** with a case/incident number or **pursuant to a valid subpoena/court order**.

____ I understand footage may be unavailable due to retention limits, technical malfunctions, power/network outages, or vendor issues. I agree the Association will not be held responsible for any inability or failure to record or retain the requested footage.

____ I agree to pay **actual costs** incurred by the Association as a result of any extraordinary searches/exports/redactions that I have requested, which are approved by the Board, including any necessary advanced deposit. Unused deposits will be refunded; any deficits will be billed to the requesting party. The following are examples of circumstances which may require deposit or reimbursement:

1. Exports requiring redaction or compilation across multiple cameras or days.
2. Vendor time to retrieve, convert, or securely transmit large files.
3. Non-routine searches beyond a one-hour window or without precise timestamps.
4. Storage of preserved footage beyond 60 days at third-party rates.

I certify that the above information is true and correct and that I have a good-faith basis for this request.

Signature: _____ Date: _____

Printed Name: _____

For Association Use Only (to be completed by Management)

- Date/Time Received: _____ Received by: _____
- Review result: ☐ Footage preserved ☐ None found ☐ Not available
- Costs/deposit requested: ☐ Yes $_____ ☐ No
- Disposition/notes: _____

Employment Eligibility Verification

Department of Homeland Security

U.S. Citizenship and Immigration Services

USCIS Form I-9

OMB No.1615-0047

Expires 05/31/2027

START HERE: Employers must ensure the form instructions are available to employees when completing this form. Employers are liable for failing to comply with the requirements for completing this form. See below and the Instructions.

ANTI-DISCRIMINATION NOTICE: All employees can choose which acceptable documentation to present for Form I-9. Employers cannot ask employees for documentation to verify information in **Section 1**, or specify which acceptable documentation employees must present for **Section 2** or Supplement B, Reverification and Rehire. Treating employees differently based on their citizenship, immigration status, or national origin may be illegal.

Section 1. Employee Information and Attestation: Employees must complete and sign Section 1 of Form I-9 no later than the first day of employment, but not before accepting a job offer.

Last Name (Family Name)	First Name (Given Name)	Middle Initial (if any)	Other Last Names Used (if any)

Address (Street Number and Name)	Apt. Number (if any)	City or Town	State	ZIP Code

Date of Birth (mm/dd/yyyy)	U.S. Social Security Number	Employee's Email Address	Employee's Telephone Number

I am aware that federal law provides for imprisonment and/or fines for false statements, or the use of false documents, in connection with the completion of this form. I attest, under penalty of perjury, that this information, including my selection of the box attesting to my citizenship or immigration status, is true and correct.

Check one of the following boxes to attest to your citizenship or immigration status (See page 2 and 3 of the instructions.):

- ☐ 1. A citizen of the United States
- ☐ 2. A noncitizen national of the United States (See Instructions.)
- ☐ 3. A lawful permanent resident (Enter USCIS or A-Number.) _____
- ☐ 4. An alien authorized to work until _____ (exp. date, if any)

If you check **Item Number 4.**, enter one of these:

USCIS A-Number	OR	Form I-94 Admission Number	OR	Foreign Passport Number and Country of Issuance

Signature of Employee	Today's Date (mm/dd/yyyy)

If a preparer and/or translator assisted you in completing Section 1, that person MUST complete the Preparer and/or Translator Certification on Page 3.

Section 2. Employer Review and Verification: Employers or their authorized representative must complete and sign Section 2 within three business days after the employee's first day of employment, and must physically examine, or examine consistent with an alternative procedure authorized by the Secretary of DHS, documentation from List A OR a combination of documentation from List B and List C. Enter any additional documentation in the Additional Information box; see Instructions.

	List A	OR	List B	AND	List C
Document Title 1					
Issuing Authority					
Document Number (if any)					
Expiration Date (if any)					
Document Title 2 (if any)					
Issuing Authority					
Document Number (if any)					
Expiration Date (if any)					
Document Title 3 (if any)					
Issuing Authority					
Document Number (if any)					
Expiration Date (if any)					

Additional Information

☐ Check here if you used an alternative procedure authorized by DHS to examine documents.

Certification: I attest, under penalty of perjury, that (1) I have examined the documentation presented by the above-named employee, (2) the above-listed documentation appears to be genuine and to relate to the employee named, and (3) to the best of my knowledge, the employee is authorized to work in the United States.

First Day of Employment (mm/dd/yyyy):

Last Name, First Name and Title of Employer or Authorized Representative	Signature of Employer or Authorized Representative	Today's Date (mm/dd/yyyy)

Employer's Business or Organization Name	Employer's Business or Organization Address, City or Town, State, ZIP Code

For reverification or rehire, complete Supplement B, Reverification and Rehire on Page 4.

LISTS OF ACCEPTABLE DOCUMENTS

All documents containing an expiration date must be unexpired.
* Documents extended by the issuing authority are considered unexpired.
Employees may present one selection from List A or a
combination of one selection from List B and one selection from List C.
Examples of many of these documents appear in the Handbook for Employers (M-274).

LIST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Identity	AND	LIST C Documents that Establish Employment Authorization
1. U.S. Passport or U.S. Passport Card		**1.** Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, sex, height, eye color, and address		**1.** A Social Security Account Number card, unless the card includes one of the following restrictions: **(1)** NOT VALID FOR EMPLOYMENT **(2)** VALID FOR WORK ONLY WITH INS AUTHORIZATION **(3)** VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		**2.** ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, sex, height, eye color, and address		**2.** Certification of report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		**3.** School ID card with a photograph		**3.** Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
4. Employment Authorization Document that contains a photograph (Form I-766)		**4.** Voter's registration card		**4.** Native American tribal document
5. For an individual temporarily authorized to work for a specific employer because of his or her status or parole: **a.** Foreign passport; and **b.** Form I-94 or Form I-94A that has the following: **(1)** The same name as the passport; and **(2)** An endorsement of the individual's status or parole as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.		**5.** U.S. Military card or draft record		**5.** U.S. Citizen ID Card (Form I-197)
		6. Military dependent's ID card		**6.** Identification Card for Use of Resident Citizen in the United States (Form I-179)
		7. U.S. Coast Guard Merchant Mariner Card		**7.** Employment authorization document issued by the Department of Homeland Security For examples, see **Section 7** and **Section 13** of the M-274 on **uscis.gov/i-9-central**. The Form I-766, Employment Authorization Document, is a List A, **Item Number 4.** document, not a List C document.
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI		**8.** Native American tribal document		
		9. Driver's license issued by a Canadian government authority		
		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		

Acceptable Receipts

May be presented in lieu of a document listed above for a temporary period.
For receipt validity dates, see the M-274.

• Receipt for a replacement of a lost, stolen, or damaged List A document. • Form I-94 issued to a lawful permanent resident that contains an I-551 stamp and a photograph of the individual. • Form I-94 with “RE” notation or refugee stamp issued to a refugee.	**OR**	Receipt for a replacement of a lost, stolen, or damaged List B document.	Receipt for a replacement of a lost, stolen, or damaged List C document.

*Refer to the Employment Authorization Extensions page on **I-9 Central** for more information.

Supplement A,
Preparer and/or Translator Certification for Section 1

Department of Homeland Security
U.S. Citizenship and Immigration Services

USCIS
Form I-9
Supplement A
OMB No. 1615-0047
Expires 05/31/2027

Last Name *(Family Name)* from **Section 1.**	First Name *(Given Name)* from **Section 1.**	Middle initial (if any) from **Section 1.**

Instructions: This supplement must be completed by any preparer and/or translator who assists an employee in completing Section 1 of Form I-9. The preparer and/or translator must enter the employee's name in the spaces provided above. Each preparer or translator must complete, sign, and date a separate certification area. Employers must retain completed supplement sheets with the employee's completed Form I-9.

I attest, under penalty of perjury, that I have assisted in the completion of Section 1 of this form and that to the best of my knowledge the information is true and correct.

Signature of Preparer or Translator			Date *(mm/dd/yyyy)*
Last Name *(Family Name)*	First Name *(Given Name)*		Middle Initial *(if any)*
Address *(Street Number and Name)*	City or Town	State	ZIP Code

I attest, under penalty of perjury, that I have assisted in the completion of Section 1 of this form and that to the best of my knowledge the information is true and correct.

Signature of Preparer or Translator			Date *(mm/dd/yyyy)*
Last Name *(Family Name)*	First Name *(Given Name)*		Middle Initial *(if any)*
Address *(Street Number and Name)*	City or Town	State	ZIP Code

I attest, under penalty of perjury, that I have assisted in the completion of Section 1 of this form and that to the best of my knowledge the information is true and correct.

Signature of Preparer or Translator			Date *(mm/dd/yyyy)*
Last Name *(Family Name)*	First Name *(Given Name)*		Middle Initial *(if any)*
Address *(Street Number and Name)*	City or Town	State	ZIP Code

I attest, under penalty of perjury, that I have assisted in the completion of Section 1 of this form and that to the best of my knowledge the information is true and correct.

Signature of Preparer or Translator			Date *(mm/dd/yyyy)*
Last Name *(Family Name)*	First Name *(Given Name)*		Middle Initial *(if any)*
Address *(Street Number and Name)*	City or Town	State	ZIP Code

Supplement B,

Reverification and Rehire (formerly Section 3)

Department of Homeland Security

U.S. Citizenship and Immigration Services

USCIS
Form I-9
Supplement B
OMB No. 1615-0047
Expires 05/31/2027

Last Name *(Family Name)* from **Section 1.**	First Name *(Given Name)* from **Section 1.**	Middle initial (if any) from **Section 1.**

Instructions: This supplement replaces Section 3 on the previous version of Form I-9. Only use this page if your employee requires reverification, is rehired within three years of the date the original Form I-9 was completed, or provides proof of a legal name change. Enter the employee's name in the fields above. Use a new section for each reverification or rehire. Review the Form I-9 instructions before completing this page. Keep this page as part of the employee's Form I-9 record. Additional guidance can be found in the Handbook for Employers: Guidance for Completing Form I-9 (M-274)

Date of Rehire *(if applicable)*	New Name *(if applicable)*		
Date *(mm/dd/yyyy)*	Last Name (Family Name)	First Name (Given Name)	Middle Initial

Reverification: If the employee requires reverification, your employee can choose to present any acceptable List A or List C documentation to show continued employment authorization. Enter the document information in the spaces below.

Document Title	Document Number (if any)	Expiration Date (if any) (mm/dd/yyyy)

I attest, under penalty of perjury, that to the best of my knowledge, this employee is authorized to work in the United States, and if the employee presented documentation, the documentation I examined appears to be genuine and to relate to the individual who presented it.

Name of Employer or Authorized Representative	Signature of Employer or Authorized Representative	Today's Date *(mm/dd/yyyy)*

Additional Information (Initial and date each notation.)

☐ Check here if you used an alternative procedure authorized by DHS to examine documents.

Date of Rehire *(if applicable)*	New Name *(if applicable)*		
Date *(mm/dd/yyyy)*	Last Name (Family Name)	First Name (Given Name)	Middle Initial

Reverification: If the employee requires reverification, your employee can choose to present any acceptable List A or List C documentation to show continued employment authorization. Enter the document information in the spaces below.

Document Title	Document Number (if any)	Expiration Date (if any) (mm/dd/yyyy)

I attest, under penalty of perjury, that to the best of my knowledge, this employee is authorized to work in the United States, and if the employee presented documentation, the documentation I examined appears to be genuine and to relate to the individual who presented it.

Name of Employer or Authorized Representative	Signature of Employer or Authorized Representative	Today's Date *(mm/dd/yyyy)*

Additional Information (Initial and date each notation.)

☐ Check here if you used an alternative procedure authorized by DHS to examine documents.

Date of Rehire *(if applicable)*	New Name *(if applicable)*		
Date *(mm/dd/yyyy)*	Last Name (Family Name)	First Name (Given Name)	Middle Initial

Reverification: If the employee requires reverification, your employee can choose to present any acceptable List A or List C documentation to show continued employment authorization. Enter the document information in the spaces below.

Document Title	Document Number (if any)	Expiration Date (if any) (mm/dd/yyyy)

I attest, under penalty of perjury, that to the best of my knowledge, this employee is authorized to work in the United States, and if the employee presented documentation, the documentation I examined appears to be genuine and to relate to the individual who presented it.

Name of Employer or Authorized Representative	Signature of Employer or Authorized Representative	Today's Date *(mm/dd/yyyy)*

Additional Information (Initial and date each notation.)

☐ Check here if you used an alternative procedure authorized by DHS to examine documents.

Homeland Security Investigations
Office of the Special Agent in Charge

U.S. Department of Homeland Security
[redacted]

NOTICE OF INSPECTION

[redacted]

United States

Dear Sir/Madam:

Employers are required under section 274A(b) of the Immigration and Nationality Act (INA), as amended by the Immigration Reform and Control Act of 1986 (IRCA) to verify the identity and employment eligibility of all individuals hired in the United States after November 6, 1986. Federal regulation, 8 C.F.R. Section 274a.2, designates the Employment Eligibility Verification Form I-9 (Form I-9) as the means of documenting this verification.

Pursuant to Section 274A of the INA, the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) SAC Boston is serving this Notice of Inspection ("Notice" or "NOI") to commence an inspection of your company's Forms I-9. Federal regulations afford employers **three (3)** business days' notice prior to the start of a Form I-9 inspection. This Notice serves as your advanced notification that HSI has scheduled an inspection of your company's original (wet ink) Forms I-9, or electronically generated with audit trails and/or retained Forms I-9, as applicable, to commence **three (3)** business days from the date of service of this Notice. The Forms I-9 and supporting documents listed in the associated administrative subpoena, if any, must be received by HSI no later than 7/11/2025 5:00 PM . As of the service date of this Notice, do not make any amendments to the existing Forms I-9. Any Forms I-9 that are prepared or completed after the service date of this Notice will not be part of this inspection.

Your company may provide the requested Forms I-9 and any related supporting documents to the address listed at the end of this letter in one of the following ways: certified mail, or by contacting the HSI Special Agent identified in this Notice to schedule a time for these items to be collected by the HSI Special Agent at your company's place of business. Your company may also wish to provide a list of the items it will present to HSI, including the total number of Forms I-9 submitted for inspection. Upon receipt of the original (wet ink) Forms I-9, electronically generated with audit trails and/or retained Forms I-9, as applicable, any related supporting documentation, and/or any property (e.g., CD, external hard drive, etc.) containing such items, as requested, an HSI Special Agent will provide a receipt that documents such items received from your company. Only original (wet ink) Forms I-9, electronically generated with audit trails and/or retained Forms I-9, as applicable, any related supporting documents, and/or any property containing such items (e.g., CD, external hard drive, etc.), as requested in this Notice and/or an administrative subpoena, if any, will be documented on the receipt provided by HSI.

This inspection will cover all your current employees as of the date of service of this Notice, and employees who were terminated within the twelve months prior to the date of service of this NOI. Your company may also wish to provide a list of all covered

employees with hire dates and, if applicable, termination dates. This inspection is for employees employed by the above captioned during the requested time period at the following location(s):

[redacted]

During the inspection, the undersigned will discuss the requirements of the applicable federal laws and regulations with you. In addition to presenting your company's Forms I-9, your company will need to present copies of any identity and/or employment authorization documents copied as part of the employment eligibility verification process. If your company utilizes an electronic system or software product to create electronically generated/modified/stored Forms I-9, you will need to present: the name of the electronic system or software product utilized; the internal business practices/protocols related to the generation of, use of, storage of, security of, and inspection and quality assurance programs for, your electronically generated/modified/stored Forms I-9. In addition, you will need to present: the indexing system identifying how the electronic information contained in the Form I-9 is linked to each employee; documents describing the system used to capture the electronic signature, including the identity and attestation of the individual signing the Form I-9; and the audit trail for each electronically generated/modified/ stored Form I-9. Further, pursuant to 8 C.F.R. Section 274a.2(c)(8)(ii), the undersigned may contact you to schedule a demonstration of the generation of an electronic Form I-9 by the electronic system or software product used by your company.

The purpose of this inspection is to assess your compliance with the federal laws and regulations applicable to employment eligibility verification. HSI will make every effort to conduct the inspection in a timely manner so as not to impede your normal business routine. Failure to provide the requested documents may lead to civil or criminal penalties.

If you have any questions with respect to this inspection and/or wish to discuss other Forms I-9 delivery options, please contact the undersigned.

If this Notice was served in person, you may waive the three-day notice period described above, if you wish to do so, by annotating and signing page three of this Notice and advising this office of your decision.

Sincerely,

[redacted]

[redacted]

Special Agent in Charge - [redacted]

Please send all questions and correspondence to Special Agent [redacted]

For more information on how to properly fill out a Form I-9, please visit:
https://www.uscis.gov/i-9-central/form-i-9-resources/handbook-for-employers-m-274

Digitally Signed by: 'E=Title-IIISupport@ice.dhs.gov, CN=Homeland Security Investigations, O=Homeland Security Invest
Date: 2025.07.08 17:01:08 +00:00

Waiver of the Three-Day Period

I wish to waive the three-day notice to which I am entitled by 8 C.F.R. Section 274a.2(b)(2)(ii).

(Printed Name)	(Signature)	(Date)

Certificate of Service

This Notice of Inspection was served upon the employer by me on 7-8-2025, in the following manner:
(Date of Service)

☑ In person ☐ Electronically ☐ By certified mail, return receipt requested

Electronically served at N/A
(Electronic service address of employer/business representative/attorney served)

Expressed consent for electronic service provided by N/A
(Name and Title of owner/designated business representative/attorney served)

via email on N/A
Date

[redacted] (Printed Name of HSI Special Agent)	[redacted] (Printed Name of Employer if Personally Served)
[redacted] (Signature of HSI Special Agent)	[redacted] (Signature of [redacted]loyer if Personally Served)

MULTI-STATE SAMPLE OF E-VERIFY REQUIREMENTS

State	Employer Types Required to Use E-Verify	Effective*
Alabama	All e'ers (public/pvt)	4/1/12 (HB 56)
Arizona	All e'ers	1/1/08
Florida	Public e'ers & all contractors/subs; Pvt e'ers w/ 25+ e'ees	1/1/21 (statewide)
Georgia	Pvt e'ers w/ 11+ e'ees; all state contractors/subs	1/1/13
Mississippi	All e'ers in state must register	7/1/11 (phased in)
S. Carolina	All e'ers	1/1/12
Utah	Pvt e'ers w/ 150+ e'ees; public e'ers/contractors	(Not specified)
Indiana	All public e'ers; many state contractors/subs	6/30/11 (state agencies)
Louisiana	All e'ers must either use E-Verify or maintain certain ID verification; state contractors/subs mandated	8/15/11 (pvt e'er rule)
Missouri	Public e'ers & contractors on certain sized projects	1/1/09
Nebraska	Public e'ers & contractors	10/1/09
Oklahoma	Public e'ers & contractors/subs	11/1/07 (public e'ers)
Penn.	Public works contractors & certain construction e'ers	1/1/13
Texas	Contractors/subs working w/ state agencies	12/3/14

SAMPLE POLICY:
RESPONSE TO ICE INQUIRIES

Purpose:

This policy outlines procedures for board members, community managers, and other staff in California when approached at the association by U.S. Immigration and Customs Enforcement (ICE) or any other federal immigration agency. It ensures compliance with California law, particularly the Immigrant Worker Protection Act (AB 450; Labor Code §§ 7285.1, 7285.2, 1019.2), while safeguarding the rights and privacy of residents, workers, and contractors.

I. Scope and Application

This policy applies to:
- Board members, Committee members, and Association employees
- Community managers and professional management companies
- On-site staff such as maintenance, security, patrol, and administrative personnel
- Third-party vendors and contractors working on association properties

II. General Principles

1. Respect for Law and Employee Rights:
California enforces strict privacy protections under AB 450 (CA Gov. Code §§ 7285.1 and 7285.2). This law prohibits employers from voluntarily granting ICE access to non-public areas or employee records without a judicial warrant or subpoena. Associations must balance compliance with lawful government actions while also respecting individual rights provided under California law, including the California Constitution, Article I, Section 13 and U.S. Constitution Amendment IV (protecting against unreasonable searches and seizures).

2. Legal Compliance:
Compliance with valid, lawful directives is essential. However, under California Labor Code § 7285.1(a), employers and managers may not voluntarily permit ICE agents to access non-public areas of the workplace or residential community without a judicial warrant signed by a judge. Similarly, under § 7285.2(a), they may not provide employee records without a subpoena or court order, except in very limited cases such as I-9 audits. Administrative warrants (*e.g.*, I-9 audits) are not sufficient for access or data requests without further legal review.

III. Designated Point of Contact

The Board shall appoint a Designated ICE Response Officer (DIRO), typically the general manager or association president. Only this individual is authorized to interact with ICE agents. This person must be trained in the applicable laws and should immediately contact legal counsel upon any ICE interaction. All other personnel must direct agents to this contact without engaging in discussion or providing documents. The DIRO, typically the board president, community manager, or legal counsel, shall be only authorized individual that may interact with ICE agents on behalf of the association.

IV. Responding to ICE Agents

Upon being approached by ICE:

1. Request Identification and Documentation:

- Politely ask for the agent's name, badge number, and agency.
- Request a copy of the judicial warrant (signed by a judge), subpoena, or court order that constitutes the legal authority of any warrant or subpoena. Take a photo or copy if possible.
- AB 450 mandates that access to non-public areas requires a judicial warrant (not an administrative warrant). For document requests (*e.g.*, I-9 audits), a subpoena or Notice of Inspection under 8 CFR § 274a.2 must be reviewed by legal counsel.

2. Do Not Consent to Access:

- Do not allow entry to any private or non-public areas without a judicial warrant signed by a judge. Refer to Government Code § 7285.1.
- Do not turn over any documents or records without consulting legal counsel
- Do not grant access to private or non-public areas (*e.g.* management office, residential gates) unless a judicial warrant is provided, as per CA Labor Code § 7285.1.

3. Notify Legal Counsel:

- Immediately contact the association’s legal representative to review the documentation and oversee any response.
- Do not answer questions or sign any documents without legal review.

4. Document the Encounter:

- Record the date, time, and nature of the inquiry in writing.
- Note the names and badge numbers of all agents involved.
- Submit a report to the Board and legal counsel.

5. Verify Legal Authority: ent the Encounter:
- Request to review any subpoena or notice with legal counsel prior to compliance, per Labor Code § 7285.2.

V. Notification and Communication

1. Employee/Resident Notification:
- Under Labor Code § 90.2, if ICE serves a Notice of Inspection (NOI) regarding I-9 forms, the association must notify any affected employees within 72 hours using a prescribed notice format.

2. Community Messaging:
- Do not make public announcements about ICE presence or activity without legal guidance. Managers should avoid disseminating broad alerts that may cause panic and increase legal exposure. Communications should be coordinated with legal counsel to ensure accuracy and compliance.

VI. Prohibition on Retaliation

California Labor Code § 1019.1 prohibits retaliation or discrimination against employees for asserting their immigration status or for asserting rights under state law. Board members, managers, and staff are prohibited from disciplining, threatening, or penalizing any staff or residents who exercise their rights, inquire about legal obligations, or otherwise, question or act under this policy.

VII. Policy Review

This policy shall be reviewed annually by the Board or legal counsel to ensure compliance with updated local, state, or federal immigration laws. Annual training on the rights, responsibilities, and procedures outlined above is recommended so all staff and Board members are informed and equipped to follow procedures correctly.

Approved by: [Board of Directors / Community Management Company]
Effective Date: [Insert Date]
Policy Review Date: [Insert Date]

February 2025

Guidance for Community Associations Handling ICE Requests

community ASSOCIATIONS INSTITUTE

www.caionline.org
#WeAreCAI

Guidance for Community Associations Handling ICE Requests

Released March 5, 2025

Authors:
Leslie Brown, Esq. Rees Broome (Virginia)
J. David Ramsey, Esq. Fellow, CCAL Becker Lawyers, New Jersey

Recent reports indicate U.S. Immigration and Customs Enforcement agents have appeared at community mangers' offices seeking information about owners, residents, and employees. This raises serious issues concerning the legal obligations community managers and associations have regarding immigration status.

Community associations uphold certain duties to protect members and employees' information unless applicable law or proper judicial process require disclosure. As a community association manager or board member, it's important to understand your rights and responsibilities when approached by ICE agents requesting lists of employees or residents to verify immigration status or attempting to execute an ICE warrant on association premises.

Guidance from the American Civil Liberties Union and the National Immigration Law Center outlines best practices for such situations.

1. Understand the Nature of the Request

ICE may seek access to information about association employees such as staff and other personnel or residents for various reasons including:

- **Form I-9 audit**. ICE agents may request association records regarding employees to ensure compliance with employment eligibility verification. Employers must receive at least three business days to produce the I-9 forms requested in the Notice of Inspection.
- **Targeted enforcement**. ICE agents may attempt to locate specific individuals for purposes of making a detention and/or arrest.

2. Verify Legal Authority

Before providing any information such as a membership list or access to the association premises, managers and board members should:

- **Request identification**. Ensure the individual is an ICE agent by asking for official identification, which includes a name and badge number.
- **Ask for a warrant**. ICE agents must present a judicial warrant to access private areas or obtain specific association information.
    - **Judicial warrant**. Issued by a court and signed by a judge or magistrate. It grants permission for entry onto association premises and/or obtain association records and information. The judicial warrant will state with specificity the premises to be searched or the documents to be obtained. Sometimes police will rely on constitutional

exceptions to conduct searches without a warrant such as in the event evidence may be destroyed or other exigent circumstances. That situation would be a very rare exception in the context of community associations.

- **Administrative warrant**. This document issued by ICE and signed by an ICE administrative officer does not grant the same authority as a judicial warrant. It allows ICE agents to arrest noncitizens suspected of committing immigration violations. It does not grant the ICE agent authority to enter nonpublic association areas or obtain information about whether the person works or resides at the association or any other information maintained by the association regarding employment, residency, etc. Without a valid judicial warrant, the association is not legally obligated to provide access to private areas or confidential information. For more details, refer to NILC's *A Guide for Employers: What to Do if Immigration Comes to You?*

3. Protect Resident and Employee Privacy

Unless presented with a judicial warrant or subpoena, association management and boards should protect employment and resident information from disclosure.

- **Confidentiality**. Maintain the confidentiality of all residents and employees.
- **Data sharing**. Do not share personal information such as names, addresses, vehicle information, etc., without proper legal authorization.

4. Develop a Response Plan

Management and boards can prepare in advance by:

- **Designating a point of contact**. Assign a staff member to handle interactions with ICE agents.
- **Training staff**. Ensure all staff members recognize the difference between a judicial warrant or subpoena versus an ICE warrant and staff understand protocols for handling ICE inquiries.
- **Legal consultation**. Consult with association legal counsel to establish procedures that comply with federal and state laws.
- **Remain calm.** Respond respectfully. It is appropriate for association representatives to calmly tell an ICE officer they cannot consent to access or provide information without a valid warrant and provide the name and contact information of association legal counsel for further inquiries.
- **Call local law enforcement.** If the interaction with the ICE agent escalates, it is appropriate to contact local law enforcement for assistance.
- **Never Interfere**. If an ICE officer seeks to enter an area without a proper judicial or administrative warrant, do not attempt to interfere. Other legal remedies are available in such circumstances.

5. Know Your Rights and Responsibilities

- **Access to private areas**. ICE agents cannot enter private areas without a judicial warrant or the explicit consent of an association representative such as the manager or a board member. Absent extraordinary circumstances, access should not be provided.
- **Voluntary interviews**. Association representatives are not obligated to answer questions or allow interviews without legal compulsion or comprehensive information on rights and procedures. While some association representatives may feel compelled to cooperate with ICE officials, they should first consult with association legal counsel. For more information, consult the ACLU's Immigrants' Rights and Resources Hub.

6. Document All Interactions

Keep detailed records of:

- **Agent identifications**. Write down names and badge numbers. Ask for business cards.
- **Presented documents**. Make copies of any warrants or other legal documents.
- **Communication details**. Write down dates, times, and summaries of all interactions.

7. Stay Informed

Immigration policies and enforcement practices can change. Regularly consult authoritative sources to stay updated:

- **National Immigration Law Center**. www.nilc.org](https://www.nilc.org)
- **American Civil Liberties Union**. www.aclu.org](https://www.aclu.org) By adhering to this guidance, you can ensure your actions are lawful and respectful of the rights of community members.
- **Association legal counsel.** Consult with association legal counsel regularly on employment and immigration issues and concerns.

Legal Disclaimer

The information provided in this document is for general informational purposes only and is not intended to constitute legal advice. The Community Associations Institute (CAI) is not a law firm. Nothing in this guidance should be construed as creating an attorney-client relationship or as a substitute for legal advice from a qualified attorney.

Community associations, board members, managers, and other stakeholders should consult with a licensed attorney familiar with local, state, and federal laws before taking any action related to U.S. Immigration and Customs Enforcement (ICE) requests. CAI makes no representations or warranties regarding the accuracy, completeness, or applicability of the information contained herein.

By using this guidance, you acknowledge that CAI, its affiliates, officers, directors, employees, and contributors shall not be liable for any claims, losses, or damages arising from reliance on the information provided.

For legal advice tailored to your specific situation, please consult a qualified attorney.

COMMUNITY ASSOCIATIONS INSTITUTE

6402 Arlington Blvd., Suite 500
Falls Church, VA 22042
(888) 224-4321
www.caionline.org

#WeAreCAI

CAISOCIAL

Community Associations Institute

@CAISocial and @CAIAdvocacy

@CAISocial

community ASSOCIATIONS INSTITUTE