What if ... your organization is subject to a search warrant?

JULY 2025

This primer is not meant to, and does not, offer legal advice, including on any specific facts or circumstances. It is intended for general information and educational purposes only. The distribution of this primer is not intended to create, and receipt of it does not constitute, an attorney-client relationship with protect democracy.

Protect Democracy

Understanding search warrants

What is a search warrant?

A **search warrant** is an official document, issued by a judge or magistrate, that allows law enforcement agents to search a person, place, or entity for evidence related to criminal activity. Organizations can view an example of a federal search and seizure warrant here.

With limited exceptions, government officials cannot enter an organization's private spaces (those spaces not generally open to the public) to conduct a search or seizure without a valid warrant. This is because the Fourth Amendment to the U.S. Constitution protects a reasonable expectation of privacy that extends to private property.

Search warrants are often the beginning of a longer process. They can be used to gather evidence as part of an ongoing investigation and likely signal that an organization should expect further inquiries from federal or state government entities.

(This resource includes additional information on the difference between administrative and judicial warrants in the immigration context.)

Do organizations have to comply with search warrants?

Non-compliance (or obstruction of an authorized search) can result in arrest or criminal charges against organizations and/or their staff.

How are search warrants executed?

Both state and federal governments can task their respective law enforcement agents with conducting searches pursuant to warrants. The rules for executing search warrants may differ somewhat by jurisdiction. Federal agents, for example, generally are required to execute a search warrant within 14 days of a judge issuing it. *See, e.g.,* Fed. R. Cr. P. 41(e)(2)(A)(i). Agents generally are authorized to conduct searches during the "daytime" (defined by federal rules as between the hours of 6:00 a.m. and 10:00 p.m. local time), and searches outside of these hours must be expressly authorized by a judge based on a showing of good cause. With some exceptions, search warrants must be issued by a court with jurisdiction over the place to be searched. (Some federal agencies also have their own additional rules governing applications for and execution of search warrants. *See, e.g.,* IRS Internal Revenue Manual 9.4.9.)

Will organizations know when a search is being executed?

In most cases, search warrants are executed without prior notice, which means organizations usually do not know in advance that the government has been authorized to conduct a search of their premises and/or property.

Agents executing a search warrant can (and often do) conduct visits without warning. However, with limited exceptions, they are generally required to announce and/or identify themselves at the location of the search before carrying out the search itself. There are certain kinds of search warrants, sometimes called "no-knock" or "delayed-notice" search warrants, that specifically permit law enforcement officers to enter a premises without the need to identify themselves or their purpose for being there. The Supreme Court has also held that officers are not required to announce themselves if they have "reasonable suspicion" that doing so would be "dangerous" or "inhibit the … investigation."

Can organizations see what is covered by a government's search warrant?

Yes. Agents are supposed to show a copy of their warrant, which will include a description of the premises they are authorized to search and the material they are allowed to seize. *See, e.g.*, Fed. R. Cr. P. 41(f)(1)(C).

Best practices

Planning ahead

There is broad agreement that the most important thing organizations can do to prepare for the possibility of a search warrant is develop **a plan in advance and in consultation with legal counsel**. Organizations should also ensure that all staff who may interact with government agents are aware of the plan and their individual roles.

In addition to federal rules, state rules and procedures governing search warrants vary, and legal counsel can help ensure that any plan an organization develops is consistent with state and federal practice.

Designating staff for specific roles

In developing a response strategy, organizations should designate specific staff to interact with government agents. Ideally, an organization's attorney (if available) and/or supervisor(s) should handle the majority of interactions with government agents conducting a search. Organizations can also task specific staff to help escort agents throughout the organization's office when they search its premises. Without interfering with the search, these "**designated escorts**" should take notes of ALL activities during the search so that there is a contemporary record of what was searched and/or seized, the organization's compliance with the search, and any incident or conduct that the organization might want to address with legal counsel, the agency, or a court after the search. Escorts can also take pictures throughout a search, as long as their actions are not interfering with agents' activities.

Most search warrants now include electronic data (among other things), so organizations should consider designating an IT supervisor and/or technology expert at the organization to handle searches that seek information stored in computers, servers, devices, the cloud, etc.

Note: Agents executing a warrant may seize and copy phones, laptops, and servers, which may contain personal, privileged, or unrelated data. The seizure of devices with end-to-end encryption and password protection raises complicated questions, including whether agents can compel staff to unlock a device or provide a password during the search. Circumstances may depend on the type of lock (a memorized passcode versus a biometric fingerprint or face scan) and/or relevant state law. **As a general matter, staff should not unlock devices or share passwords without first consulting counsel, and organizations should flag any device or encryption issues for legal counsel early**. For general background, see the Electronic Frontier Foundation's Surveillance Self-Defense guide and the ACLU's resources on electronic device searches.

Getting a lawyer

For organizations subject to a search warrant, **involving legal counsel as soon as possible is critical to determining the organization's options and to protecting confidential and privileged information as much as possible.**

If an organization has in-house counsel, that should be the first call. If not, organizations should have a list of outside lawyers ready ahead of time so someone can be reached immediately.

Remaining calm

It can be scary to be subject to a government search, especially without notice. Warrants can be executed by an individual law enforcement agent or group of agents who present themselves in a variety of ways. Remember that **remaining calm and level-headed will help ensure good decision-making and avoid disrupting core work.**

Interacting with government agents

When interacting with government agents conducting a search, organizational staff should consider the following:

- ✔ **Staff should remain calm, polite, cooperative, and observant.** Interfering with or trying to prevent the search can result in serious legal consequences.
- ✖ **Agents are there to conduct a search, not an interrogation.** Generally speaking, staff are not required to speak to agents about anything substantive. Direct any questions to legal counsel, and keep any conversation to a minimum, unless the particular staff member has received specific instructions from legal counsel.
- ✖ **Staff generally do not have the authority to consent to anything on behalf of the organization.** If agents make requests such as, "May I see your phone?" or "May I search this area?," staff should generally note that they cannot speak or consent on behalf of the organization and should involve legal counsel as soon as possible.
- ✖ **Destroying, tampering with, removing, or throwing away documents or materials relevant to the search may result in criminal charges.**

For legal advice and additional best practices around interacting with government agents, organizations should consult with legal counsel. For more general resources on how to prepare for interactions with government agents, check out: the Center for Constitutional Rights' guide: If An Agent Knocks and Clear's list of Know Your Rights resources.

Considerations for frontline staff

Employees staffed at an organization's front desk or tasked with answering phone calls need training for how to respond to search warrants.

Staff can ask to see the agents' identification and get their business cards. If staff cannot get identification for all agents, they should generally try to obtain contact information for the lead agent(s) in charge of the search.

Frontline staff should immediately contact the person(s) designated to respond to the situation. This is very likely to be in-house or outside counsel, or potentially a designated supervisor.

When possible, staff should politely request that the agents wait for appropriate personnel who will help them find the areas and information they are authorized to search. Once the organization's designated point person arrives, that person should take over the process.

If an agent wants a staff member's personal possessions, those personal effects should be

listed within the scope of the warrant, and if not, staff can inform agents that their personal property is not covered. If the agent insists, staff should wait for instruction from someone in charge. If that is not possible and staff must surrender items, they can say they object to the seizure and notify the staff member in charge.

Staff should take notes of anything they see, hear, or otherwise notice and give those notes to the staff member in charge after the search.

If the organization receives a phone call from government agents about a search warrant, staff who answer the call should verify the caller's identity, get their contact information, immediately notify a staff member in charge, and take note of anything the agents say over the phone.

Considerations for supervisory staff and on-site counsel

Supervisory employees and/or legal counsel who have been designated to interact with government agents before and during a search of an organization need to plan in advance and regularly train on their roles in responding to a search warrant.

Before a search begins:

Organizations should have a point person (ideally an attorney for the organization) meet the agents as soon as possible.

If an attorney is not present, one should be **called immediately and informed of the search.** If the organization is not able to reach an attorney, it should stick to the plan created in preparation for this scenario.

The point person should ask for a copy of the warrant. If a copy is not provided, they should ask to take a photo of the warrant.

The warrant should clearly state that it is a *search* warrant and **accurately reflect the name and address of the organization**, should be signed by a judge or magistrate, and cannot have expired. If the warrant fails any of these requirements, this should be explicitly noted to the agent in charge.

There may be actions that the warrant does not permit and it's important to make note of those. **Agents are legally permitted to search only rooms and materials that fall within the scope of the warrant** (unless they have probable cause to expand their search or other warrant exceptions are at play). If agents take any action beyond what the warrant permits, the organization's counsel should explicitly object and take contemporaneous notes of what is being done. If staff consent to any actions beyond the scope of the warrant, it will be difficult to object to seizure of those materials after the fact.

The warrant must specify if computers, servers, other devices, or cloud-based information

are within the scope of the search (which will usually be the case). If so, IT professionals should be alerted. Some organizations also choose to make a designated IT staff member available to agents to both cooperate and monitor what is being done. Such a representative (and/or legal counsel) can also work with the agents to obtain what they need without disrupting the continuity of operations (*e.g.* shutting down systems that allow for remote work).

Staff who are present on site should be informed of agents' presence and instructed not to interfere with the search in any way.

Organizations should make sure their pre-designated escorts (if supervisors or in-house counsel are not one of them) **are available** and meet agents in charge of the search. Escorts can and should observe all search and seizure activity and take notes of their actions and items searched for and taken.

Some organizations may choose to send all employees home (except for legal counsel, escorts, and/or necessary IT personnel), and close the office except for the search activity.

When possible, discussions with agents should be limited to legal counsel, so that other staff members do not have to speak to agents during the search. Counsel can inform the agents that they speak on behalf of the organization and request that all conversations go through them.

During a search:

Keep a detailed list of everything that happens throughout the search. What rooms, files, computers, and/or servers were reviewed and/or seized? Were any employees interviewed? Were there any "incidents" (*e.g.*, bad interactions with agents, damaged property)? Contemporaneous notes are critical.

Rules governing audio and video **recordings of government agents** may vary by jurisdiction and circumstance. Organizations should consult with legal counsel about their options as part of advance planning and make sure the plan includes clear instruction for staff.

Protect attorney-client privilege. One reason having legal counsel present is critical is they can notify agents if any material they are reviewing might contain privileged information. Counsel **generally cannot prevent agents from seizing such material**, but can and should ask that it be placed in a sealed box or envelope marked "Potentially Privileged and Confidential."

Ask for and obtain a receipt of anything taken by agents. Organizations subject to search warrants are entitled to this.

Organizations should also be prepared to receive a subpoena. **Agents will often serve a subpoena in addition to conducting a search.** If agents have a subpoena for the organization, the organization should allow legal counsel to handle acceptance of service. (To learn more about responding to subpoenas, read *What if . . . your organization is served with a subpoena*).

Lastly, once the agents depart, organizational representatives should **debrief internally with legal counsel** as soon as possible.

Protect Democracy is a nonpartisan nonprofit organization dedicated to preventing American democracy from declining into a more authoritarian form of government.

protectdemocracy.org