

What if ... your organization is subject to politicized executive actions?

JULY 2025

Why target civil society? 1

What to do (and not do)
if you're targeted 2

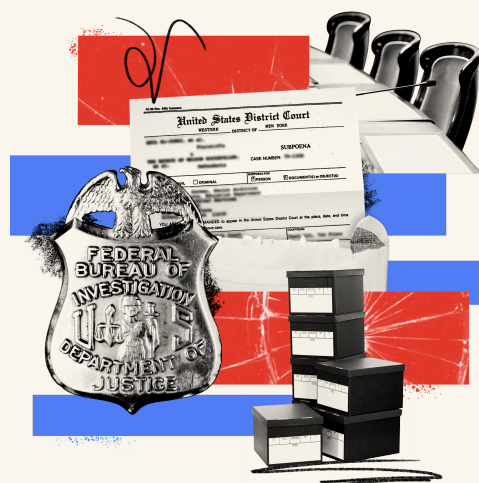
General operating 3

Internal communications 4

Public communications 5

Security 5

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.



Why target civil society?

Understanding politicized executive actions in context

A healthy democracy protects space for people to debate ideas, organize to contest or advocate for policies, share information, and serve as a check on the government. American civil society — composed mostly of nonprofit organizations — is a key component of that civic space. We provide critical services to local communities; feed, house, and clothe the poor; support veterans; advocate for access to healthcare; protect children and the elderly; offer religious services; fight for clean air and water; and defend civil liberties and other core freedoms. And, importantly, we hold our leaders in government to account when they abuse their power.

That's precisely why the current administration — like autocratic regimes around the world — has targeted, and has indicated that they will continue to target, civil society through unlawful executive actions. The goal is to silence critics and sideline any organization that might serve as a check on executive branch power. The administration has already targeted civil servants, the legal profession, and universities. It's all part of the [authoritarian playbook](#).

It's important not to lose sight of this bigger picture:

- These attacks are about censoring political opponents and critics of the government.
- They are also a power grab meant to eliminate checks on abuses of government power.
- The intention is to disrupt nonprofits from carrying out their lawful and mission-critical work.
- Targeting nonprofits hurts our communities and impedes the ability of nonpartisan organizations to provide much-needed services to the American people.

The [path forward](#) lies in organizations across the ideological spectrum calling these tactics out for what they are, forcefully pushing back, [standing up collectively](#), and continuing their everyday, mission-oriented work. The concrete actions outlined below offer important insights on responding to these politicized actions, so you can feel more confident if you are targeted and continue to focus on meeting your mission.

What to do (and not do) if you're targeted

What if you are specifically targeted by a politicized executive action (including an executive order, federal agency investigation, etc.), think you may be covered by its terms, or are worried about becoming a target?

First, try not to panic!

Remaining calm is critical to making good decisions. Actions borne out of panic risk creating more problems for your organization.

Contact an attorney.

Second, it's important to involve legal counsel as soon as possible to establish attorney-client privilege around communications and protect confidential information. If your organization has in-house counsel, they should be your first call. If not, contact an outside lawyer as soon as possible. It will be important to proceed carefully in any response to current or potential threats.

Continue your work.

Third, do not make major changes to how you operate — or cease operating altogether — unless and until you have a comprehensive plan.

Stay vigilant.

Finally, your response to politicized attacks by the executive branch should include protecting your organization against additional threats. If you are publicly targeted, your organization may also be the subject of malicious actors seeking to take advantage of perceived vulnerability to attempt phishing or other cyber attacks, as well as tactics like surreptitious recording of conversations or meetings.

General operating

- ✓ **Do involve legal counsel** as soon as possible. An attorney's expertise will be crucial in determining your organization's options and protecting confidential information.
- ✓ **Do ensure that your staff is aware** of all relevant guidance for what they should and should not do throughout this process. In frightening times, communication is critically important.
- ✓ **Do continue your mission-based work** to the extent practicable. It may be tempting to pause or shut down operations, but this is usually not necessary and may even be counterproductive.
- ✓ **Do ensure your front-line staff know what to do** if they receive a call or in-person visit from someone claiming to be a government official, including how to verify the official's identity and your protocol for accepting service of process on behalf of the organization.
- ✗ **Do not panic.** Remaining level-headed will help ensure good decision-making and avoid disrupting your core work.
- ✗ **Do not rush to adopt new policies** or make significant changes to your operations in this moment of crisis – it is important to take time to consider your options, make smart plans, and consult with legal counsel.
- ✗ **Do not forget to stay up-to-date on all required filings** and registrations. Even as you address this situation, it is important that you continue to meet your routine administrative and legal obligations.
- ✓ **Do communicate with funders and partners**, but pay careful attention to and observe any guidance about such communications from legal counsel. It's important not to hide or retreat in moments like these — civil society is stronger together.
- ✓ **Do evaluate whether to inform your insurance carriers** of the situation, if you have insurance. Your carrier may have resources to help you navigate a crisis.

Internal communications and document retention

- ✓ **Do continue to follow your organization's document retention policies** and consult with legal counsel about whether there is any need to create exceptions to those policies as a result of a politicized executive action.
- ✓ **Do assume that anything in writing** could be disclosed or discoverable. Emails and text messages, even on platforms that promise encryption, DO qualify as discoverable documents.
- ✓ **Do remember that jokes and sarcasm often do not translate** out of context, especially in writing, and can easily be misunderstood or misconstrued. Your staff should use extra caution.
- ✗ **Do not delete documents** in response to an executive action. Make sure your staff is aware that they should continue to follow your regular document retention policies unless told otherwise based on advice from legal counsel.
- ✓ **Do be cautious about sending written messages about any executive action targeting your organization.** It's natural to want to send a flurry of communications following something like this, but it's important to remember that anything in writing could be discoverable. Ideally, all communications should include legal counsel. (This may be particularly critical if you hear from others indirectly, and without verification, that your organization may soon become a target. In such a scenario, remind staff of your communications and document retention protocols and refrain from spreading rumors or engaging in speculation.)

Public communications

- ✓ **Do consider engaging a crisis communications** professional to help, depending on the severity of the situation. Engaging with a professional early may be useful in getting ahead of things.
- ✓ **Do be prepared to share** compelling information about the important work your organization does, and how that work positively affects peoples' lives.
- ✓ **Do ensure you have a clear process** in place for preparing and approving public statements.
- ✗ **Do not engage without a strategy** in place first. Importantly, do not engage in personal public criticism of government officials or post on social media while panicked or triggered.
- ✓ **Do temporarily limit public communications**, especially about a specific politicized executive action, until you've had a chance to consult with legal counsel. This includes speaking with the press, responding to social media posts, or even communicating with friends.

Security

- ✓ **Do retrain staff on cybersecurity best practices** and be alert for increased phishing and cyber attacks.
- ✓ **Do implement online threat monitoring** for your organization and staff. Monitoring can help you know if the organization is being discussed or threatened online and needs to take additional security measures.
- ✓ **Do encourage staff to be vigilant** about online and data privacy. Consider signing up for an online data scrubbing or internet data privacy service and adopting measures like multi-factor authentication.
- ✗ **Do not overlook basic security protocols** even as your organization is moving quickly. Take the time to double check the "To" field of messages, use proper privacy settings, vet participants in group chats and calls, and encourage staff to be cognizant of their physical security.
- ✓ **Do review your physical security protocols.** Make sure your staff knows what resources you have available and who to call if they receive or perceive a threat (including calling 9-1-1 if they sense immediate danger).



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

protectdemocracy.org