# Being Prepared: Emerging Threats to Health Philanthropy

As part of a January 2025 executive order aimed at rolling back DEI initiatives, the Trump Administration has asked every federal agency to identify up to nine organizations—including companies, universities, nonprofits and foundations with assets of $500 million or more—each believes is in violation of federal civil rights or contracting rules because of DEI-related practices. These lists are due to the White House by **May 21, 2025**, and are expected to inform future investigations, funding decisions, and public enforcement. With 440 agencies listed in the Federal Register, the directive could result in up to 3,960 organizations being named.

## The Splash Effect: Philanthropies of Every Size Should be Ready

The reputational and regulatory risks of this process extend beyond the organizations directly targeted. When a high-profile institution within a sector faces scrutiny—such as a university challenged on its tax-exempt status or academic governance—peer organizations quickly recognize that the underlying precedent or rationale may be applied more broadly. This "splash effect" means that entities not named in official actions nevertheless feel the impact, as the boundaries of regulatory enforcement and political critique expand. This activity has prompted preemptive internal reviews, shifts in public positioning, or changes to external partnerships. For example, when the federal government questions Harvard's tax status, it sends a clear signal to other universities that their own status could be subject to review under similar criteria. Organizations in many other sectors are also reevaluating their own risk exposure.

While many Grantmakers In Health Funding Partners are much smaller than the $500 million threshold to be included in the federal exercise, we expect that state and local governments—and social media influencers—that share the Trump Administration's priorities may use this federal exercise as an impetus to call attention to organizations within their jurisdictions as well. Given the focus of many GIH partners on health equity, and ongoing attacks on philanthropy and non-profits generally, partners should be aware this may happen and be prepared if it does.

## Knowledge is Power: Basic Monitoring

The first step in detecting a brewing threat to your organization is monitoring, and there are a variety of free and paid tools you can use to get this started.

- **Google Alerts:** Set up free Google Alerts to track website, blog, news, and other web content for mentions of your organization; any relevant acronyms or nicknames; the names of your CEO, influential board members, and other key leaders; a selection of your grantees; and key terms in your space. We recommend setting up alerts to be delivered on a daily basis for regular monitoring, or you can receive notification emails as they happen in crisis moments or for specific terms. While Google Alerts are helpful for tracking mentions in the news and on web pages, they do not track social media platforms.
- **Social Media:** Established channels like Facebook, Instagram, X, and Truth Social are places where conversation and chatter can quickly turn into a risk for your organization.
    - For platforms on which you already engage: You can manually search for keywords on the social media platform's search bar or set up private lists of

accounts or search terms to monitor.  Closely monitor your own handles, as they will be notified if you are tagged in a post. On X, it may be advisable to sign up to the platform using a neutral username that is not affiliated with your organization or team in any way and use it to monitor a private list of accounts.

  - Alternatively, there are fee-based social monitoring tools like X Pro (formerly TweetDeck, specific to X and relatively inexpensive), as well as more expensive (and expansive) tools such as Meltwater, Hootsuite, Sprout Social, Brandwatch, or Critical Mention. They will monitor and provide timely alerts across multiple platforms and search terms, although platforms without open APIs, such as META, LinkedIn, and Truth Social may still require some manual monitoring.

**Case Study: Turning Public Information into a Threat**

Recently, a regional health foundation was highlighted on social media by an account that described itself as being "inspired by DOGE." The specific areas this account raised for critique were taken from publicly available information, including the organization's 990 Form and its website, and included:

- That the Foundation had received taxpayer funds for its activities in the form of government grants and contracts;
- That the Foundation partnered with a 501c4 for the purposes of undertaking permitted (and disclosed) lobbying activities, including on progressive causes;
- That resources were dedicated to people and communities of color and LGBTQIA+ communities; and
- The salary of Foundation leadership and other aspects of its budget.

Given the availability of similar information for practically every GIH partner, it is smart to be prepared in case your organization is targeted in the coming days and weeks. Some key principles and steps to guide your response are:

- **Monitor:** Begin with monitoring the account that posted the material, any other accounts they tagged in their post, and engagement on the post from other users. This particular post tagged MAGA influencers in the state, but the account itself had a small number of followers and there was not much engagement with the post early on. If engagement stays low, and it is not picked up by other users, there is low risk to your organization.
- **Reach out to GIH:** This will allow GIH to identify any trends affecting the broader health philanthropy community as they emerge and ensure others can be ready.
- **Do Not Take the Bait:** Engaging with a post, particularly one with low engagement from others, will just amplify their message and prolong the lifespan of the post. Do not engage.

**Instead, use the time to:**

- **Prepare a Holding Statement:** This is a short statement that you would feel comfortable providing to the media if you were asked about the post. A holding statement will be succinct—not a point-by-point rebuttal to the poster's points. And the message should be simple, such as, "We are proud to serve our community and to work to improve health for all."

- **Prepare a Fact Sheet/Backgrounder:** This would address any false claims made by the post and could be provided to the media "on background" if you are asked for information. Avoid repeating false allegations in the fact sheet; instead, focus on presenting true statements and information.
- **Consider Communication with Other Stakeholders:** If one post turns into many, or if you feel the initial criticism is gaining momentum, you will want to consider communicating with stakeholders, including staff, board members, grantees, donors, and community leaders. Using the backgrounder, prepare appropriate communications for each priority audience ensuring they know you are monitoring the situation, explaining how you are responding, and, in the case of your Board and Staff, reminding them that all media inquiries should be routed through your organization's communications lead.
- **Develop a Press List:** In case you do eventually need to conduct proactive outreach, have a list of media outlets and reporters that could amplify the truth about your organization. Start with reporters or outlets with whom you already have a good relationship and consider the outlets you turn to for news in your community.
- **Only Engage with Media "If-Asked":** Unless the post goes viral, no proactive press outreach is necessary; the holding statement and fact sheet can be used as needed if media reach out, on a case-by-case basis. You do not have to respond to every inquiry.
- **Monitor and Reassess:** Assign an incident lead in your organization—most likely the communications officer—to monitor the situation and provide regular reports to organizational leadership. Is the original post getting engagement? Have local leaders picked up the thread or repeated the allegations? Periodically reassess if the level of risk to the organization has escalated, or if initial chatter is dying down on its own.