Crisis Readiness Toolkit

Purpose

It's quite likely that charitable foundations like ours could be the next American institution under attack. We must be prepared to defend core freedoms: the freedom to speak, the freedom to give, and the freedom to invest.

This readiness toolkit provides general guidance on steps foundations should take to defend ourselves—both individually and collectively. It can be used to develop your own internal plans, tailored to the needs of your specific institution.

We've compiled general best practices to guide and inform the individual responses and decisions each foundation will need to stake out for themselves. The more prepared each one of us is for what's to come, the stronger we'll be when we stand together as a sector—and vice versa.

1. Expedite crisis planning and response.

As a sector, we in philanthropy do our best to give thoughtful deliberation to every decision we make. However, this is an instance where the time we typically take to make major decisions is a luxury we cannot afford. Every institution should develop a crisis plan in short order and be prepared to deploy it with less data and input than we're accustomed to. We must fast-track our efforts by streamlining and simplifying the processes we already have in place. The best way to do that is to:

- **Deputize a crisis team.** Assemble an internal crisis team that consists of a small group of leaders who will be involved in all major decision-making, including communications, legal, and finance. Identify this group now so they're ready to act quickly.
    - Clearly define the roles of each person on that crisis team so that everyone understands what they're accountable for.
    - Develop or refine your crisis protocols so that you have an established and simple decision tree for approvals. Make sure this includes your board procedures as well.

- **Engage in scenario planning.** Identifying areas of exposure and anticipating and developing some preliminary responsive messaging and tactics in advance. As part of this, consider:
    - Which committees, agencies, and states have jurisdiction over you and what actions could they take?
    - Are there politically sensitive activities, issues, individuals, or organizations that you're associated with?
    - Have your DEI practices and policies been updated to comply with recent changes in the law?
    - Are there any internal cultural vulnerabilities, such as low employee morale, disgruntled former employees, or grantees who might pose a risk?
- **Facilitate regular information sharing and crisis assessments.** Unfortunately, scenario planning is never really "done." It requires regular modifications and additions, which requires us to stay on top of the changing landscape.
    - Calendar regular "war room" meetings to share progress updates, intel, and develop a shared assessment of the situation.
    - Keep an open line of communication with your staff and grantees, encouraging them to flag any developments on the ground.

2. Get your house in order.

It's time for all of us to prepare for the worst, whether it's a government investigation designed to cripple our finances or an executive order blocking our spending or freezing our assets. There are a few basic steps all of us can be taking to mitigate potential fallout:

- **Lawyer up.** Make sure your inside and outside counsel are coordinating with a diverse set of experts, including lawyers who are accumulating experience in dealing with the administration's attacks.
- **Prepare a rainy day fund.** The rainy day we all worry about is in the forecast. We all need to have an emergency fund that's ready to tap—either to support ourselves against an attack, or even to come to the aid of a sister organization that can no longer fulfill commitments to employees or grantees. This may be within regular funds or placed elsewhere, depending on needs and opportunity.
- **Tighten your security.** Assess all the security threats you might face and take measures to protect the institution and its staff.
    - Communications: Employees should be instructed to make their personal social media platforms private. Explore alternative and more secure ways of

communicating like signal, zoom, and phone that account for the increasing risks of leaks, cyber attacks, and legal inquiries.
    - Physical Security: Make sure you are mindful of risks to your physical security, including having increased measures to protect your office and the personal addresses of your employees—this is important for all staff, but particularly those who are more visible and therefore may be more likely to be the focus of attacks.
- **Audit your policies.** Pay special attention to the wording and implementing of your policies to make sure it is all legally compliant, particularly:
    - Hiring practices
    - Grantee criteria
    - DEI policies
    - Data collection
- **Identify vulnerable grantees.** identify grantees, current or past, who may be particularly at risk of being targeted with false accusations or smears based on their work, particular employees, etc. This may include grantees focused on issues of DEI and/or that serve specific identity groups. In addition, think about grantees who work on issues areas the Administration has identified as targets (e.g. climate change, immigration, reproductive health), issues related to Israel and Gaza, or grantees engaged in advocacy or litigation. Reach out to them to ask about their needs, share resources or advice, and encourage them to prepare as well.

3. Know what you're going to say before you say it.

Now is not the time to bite our tongues. When one of us gets attacked, we all need to be prepared to speak up in defense of ourselves and one another. Our lawyers will handle the legal filings, but foundation leaders will be the ones appearing in the court of public opinion. We need to prepare our opening argument.

- **Nail your messaging.** As part of your scenario planning, decide what you're going to say to push back. Then craft a narrative that is designed to meet the moment. That means being ready to talk about the important role that philanthropy plays in addressing the pressing economic concerns of everyday people, not abstract principles or wonky policy terms. It also requires identifying hostile government actions as what they are: an intentional attack on our fundamental freedoms. Know what the story is you want to tell and how you will convey it.
- **Prep your best messengers.** Identify and prepare the messengers within your organizations and boards who are best positioned to speak to some of the audiences we will need to reach: moderates, conservatives, businesspeople, and

working Americans. Ideally, try to include some grantees as spokespeople for the work that's happening on the ground.

- **Collect your receipts.** Compile all of the data, case studies, and proof points to show the important role we both individually and collectively play in America's economy and in local communities. Dismantling charitable giving is not a partisan issue – it harms people in every corner of the nation. We should be paying special attention to how attacks on our funding endanger constituencies that MAGA supporters care about, particularly rural communities, veterans, working families, and people in red and purple states.
- **Prepare for high-pressure settings.** We will deploy our messaging and spokespeople in speaking publicly (to press, public events, etc.) in order to communicate our story. But some of us may also need to prepare to communicate effectively in more directly hostile settings (investigations, hearings, etc.). Identify and tap into resources and expertise (communications, legal, etc.) that will help you prepare effectively for this if needed.

4. Work in coalition and make new friends.

Anyone who has been following the news has seen how silence and inaction in other sectors has only provoked more fear and uncertainty. It also hasn't done anything to tame the attacks against civil society. There is power, impact, and security in collective action. When one or more of us are targeted, as foundations we should:

- **Speak up.** We can speak together through sign-on letters, shared statements, and other collective communications vehicles, or independently through press quotes, media interviews, social media, and opinion pieces.
- **Make allies.** Fortify your networks with local voices and unlikely bedfellows – and think beyond the philanthropic and nonprofit world! Rally civic leaders in your communities to join in public statements, speak out in the media, or otherwise express support. Join forces with faith leaders, libertarians, business leaders, and others who share concerns around government overreach.
- **Share intel.** Be generous with what we know by sharing information and intelligence around current and potential threats to ourselves, each other, and adjacent fields.
- **Don't cut off the nose to save the face.** At the very least, don't speak out against one another publicly. We will not allow fear and chaos to divide us because that would allow them to achieve their goal of weakening us.

5. Lean in.

While it may be tempting to hunker down, lay low, and guard our resources—the moment calls for us to lean in. It's not just the philanthropic sector that is in midst of a crisis. The charities we fund, the people they serve, the institutions we rely on to thrive are all under attack. Foundations need to act accordingly. For those of us who can afford to increase our giving to address increasing needs, let's do it. The stakes are existential, and the price of inaction is our democracy.

Additional Resources

- Council on Foundations – Crises: A Practitioner Playbook for Corporate Responsibility and Philanthropy
- Mellon Foundation – Information Resources for Nonprofits (Code: Visionaries1969)
- Democracy Funders Network – The Authoritarian Threat: Preparing for the Repression of U.S. Philanthropy & Civil Society
- National Council for Nonprofits – Cybersecurity for Nonprofits
- Democracy Protection Network – Readiness and Resilience Building Resources
- Democracy Protection Network – Protecting Civic Space – A Primer