ADLER & COLVIN
A Law Corporation

135 MAIN STREET - 20TH FLOOR - SAN FRANCISCO, CALIFORNIA 94105
TEL: (415) 421-7555 - WWW.ADLERCOLVIN.COM

Hardening the Target: Nonprofits Under Fire

SEPTEMBER 2017

We are increasingly being asked by U.S. nonprofit organizations and their funders what they can do to be prepared for heightened scrutiny or even attacks due to taking positions at odds with policies of the government in power. Here is a summary of our thoughts. The discussion focuses on charities with tax exemption under Section 501(c)(3) of the Internal Revenue Code, although much of the advice is also relevant for other types of nonprofit and tax-exempt organizations.

Legal compliance. Be ready for close scrutiny by the IRS or a state charity regulator (such as, in some states, the state Attorney General) by making sure your organization is on solid legal footing generally. Some law firms (including ours) offer legal compliance audits that could encompass any subset of the following, depending on the areas of greatest concern:

- Filings with federal, state, and local regulatory agencies, as applicable (typically at least IRS, state-level taxing agency, Secretary of State, and Attorney General)
- Governance (review of Articles of Incorporation, Bylaws, and corporate minute books; compliance with governing documents and best practices; membership issues)
- Corporate policies (including conflicts of interest, document retention, whistleblowers, etc.)
- Solicitations (compliance with registration requirements, terms of solicitations, donor acknowledgements and disclosures, restricted fund accounting as needed)
- Financial practices, controls, and audits
- Insurance policies appropriate to activities
- Compliance with tax-exempt status requirements, public support tests (if applicable)
- Compliance with legislative lobbying limits and prohibition on intervening in candidate elections for public office
- Compliance with the private inurement prohibition, and executive compensation practices
- Unrelated business activities and taxes
- Appropriate legal separation from, and transactions with, and documentation for, any affiliates or fiscally sponsored projects
- Employment law compliance (hiring practices, personnel policy, classification of employees versus independent contractors, payroll tax issues)
- Volunteer management practices (including recruitment and screening procedures, supervision, waivers and releases)
- Internal trainings of board and staff on legal compliance

If your organization does in fact get contacted by the IRS or a state charity regulator for an audit, contact a knowledgeable attorney or accountant for advice on how to respond, if at all possible before any substantive communications with the IRS or state charity regulator occur. If you do find yourself responding to the IRS or state charity regulator with information, focus on written submissions to establish a clear written record of information provided, and make sure to keep complete and exact copies of every document provided.

Physical security. Muslim and Jewish organizations are on the cutting edge of increased security needs for offices, facilities, events, and even individual leadership, but such concerns are not new. Other organizations with positions or activities

generating controversy have been dealing with these problems for years. Consider whether your profile and activities merit greater attention to security than in the past: build relationships with local police (an officer may be able to give you a walk-through security assessment); use a P.O. box instead of your physical address; lock doors and windows at night and on weekends; control access during working hours; install/set alarm systems; have an emergency evacuation plan, and know who's in charge in an emergency; apply to FEMA's Nonprofit Security Grant Program if you're eligible. At the same time, you may not want to create a fortress: your organization will have to decide how much is enough for you.

Cyber security. Build basic security measures into websites and donor and client databases — install anti-virus software, and back up essential data regularly, off site. Some organizations may want to implement heightened verification on websites, where users have a password and must also receive a text each time they access an account. As with physical security, there's a trade-off between security and ease of use, so you choose your position on the spectrum.

Stranger (and other) danger. More than one nonprofit has been caught by being too trusting of strangers, or by being undisciplined when among apparent friends. Be alert for signs that you've been the target of opposition research by private actors; beware sting or entrapment operations where someone poses as a reporter or a client. Don't assume that someone new to you is who they say they are: make sure you know before you allow them into your confidence. This includes new staff hires. And unfortunately, this can even apply to coalition partners or others you have some reason to trust. Take care saying anything that could be recorded and taken out of context, or leaked, that reflects badly on your organization. Staff should strive always to represent the organization in the best possible light, even in "closed" environments, and should assume that anything they say or do could become public.

Lobbying. As a public charity exempt under Section 501(c)(3), you are limited in the amount of legislative lobbying you can do. Don't be scared off, though — your voice may be more crucial now than ever to represent your constituents. Instead, have someone in your organization learn the rules, and track and report your lobbying properly. Consider making the election to have your lobbying expenditures governed by Section 501(h). We have lots of useful information available, and can advise if you need it. In addition to tax law rules arising from your 501(c)(3) status, certain lobbying activities require registration and reporting to federal, state, or local agencies; consult a political lawyer for more information.

Ballot measures. Many groups are currently engaged on ballot measures at the state and local level. Ballot measures are a form of legislation, and you can weigh in on ballot measures within your lobbying limits (see preceding item). If you raise money for ballot measure work, or give money to a ballot measure committee, or coordinate your activities with a ballot measure committee, you may trigger extensive reporting obligations under campaign finance laws and therefore may require specialized campaign finance counsel. Also, ballot measure campaigns are expensive, so a charity considering a major role in one must consider the impact on the charity's lobbying limit. It usually makes sense to establish a separate non-charity for this purpose.

Electioneering. While you're speaking out on your issues, be careful to avoid actions or statements that could be construed as supporting or opposing candidates for public office. Nonpartisan issues advocacy, voter registration, and get-out-the-vote campaigns are fine, but the nonpartisan line can sometimes be hard to draw. Remember that President Trump is already a candidate for 2020, and most politicians are candidates all the time under IRS rules, so stick to critiques of specific policies and urging specific actions, rather than attacking character or commenting on overall fitness for office. Be especially careful if your communication refers, directly or indirectly, to future elections or voting.

Insurance and indemnification. Review the coverage you have with a knowledgeable insurance agent, and consider whether it's adequate in light of any changes in your risk profiles. Most organizations need general liability insurance, directors' and officers' liability insurance, and employment practices coverage. Other types of insurance depend on your operations, such as auto insurance, volunteer coverage, and special events riders. Some organizations should consider cyber liability coverage for hacking, virus transmission, and disclosure of third-party confidential information. Your directors, officers, and staff may also have questions about their personal liability exposure. Directors and officers insurance typically covers individuals acting as

agents on behalf of an organization. In addition, organization bylaws and policies and laws applicable to the organization typically address when an organization will or can indemnify its agents, including directors, officers, and employees, if they are sued or otherwise exposed to claims due to actions taken on behalf of the organization, so it is helpful to have clarity on the indemnification provisions applicable to your organization.

Social media. Social media is powerful, but also unpredictable and changes fast. Control your social media accounts, and have policies on how employees use personal accounts for work and represent their affiliation with you when speaking personally. Monitor social media for early warning of any lies about or attacks on your organization or your constituencies. And don't "feed the trolls."

Staff and Board trainings. Great organizational policies and procedures are no use unless your people know about them and follow them. Create a culture of legal compliance and crisis preparedness from the top: show that you take these concerns seriously by taking the time to develop the policies and train people to follow them, with refreshers as needed. Staff should understand that protecting the organization from risk is a job performance obligation; the organization will typically be responsible for actions of employees done in the scope of their employment. Directors should embrace these considerations as part of their fiduciary duties. And every organization should have policies to clearly distinguish what employees do personally from what is in the scope of their employment, to avoid attribution to the organization of personal activities that may be inconsistent with the organization's exemption.

Donors. Consider making your donors aware of any brewing controversy — large individual donors as well as foundations and institutional funders. If they get blindsided, consider a plan for bringing them up to speed quickly. And if you have new funding needs tied to changes in the political environment for your work, they may be able to help. Also consider whether and how to protect donor confidentiality.

Crisis planning. Think about your organization's worst-case scenarios and where, based on your specific activities and plans, you're vulnerable, and consider whether you need a generic crisis plan, or plans for specific contingencies. The crisis could involve your organization alone, specific constituencies, or types of programs.

- *Crisis consultants:* Depending on your risk profile, you may want to identify in advance public relations or communication strategy firms experienced in crisis communications, and lawyers with appropriate expertise, so that you're not scrambling if a crisis arises.
- *Crisis communications:* Whether you hire a consultant or not, try to anticipate and be prepared. For example, consider drafting social media responses to possible media stories, whether in traditional publications or in tweets or other social media postings, or setting up phone trees to expedite communications with major donors. Consider what tone you want to take in response to an attack; have fact sheets ready on your organization and your issues; decide who will speak for the organization on what topics, and make sure everyone in the organization knows.

Relationships with legislators. At every level of government, make sure your legislators know who you are, what you do, and how you help their constituents or improve the world. It's much harder to develop credibility once you're the subject of an attack. And these relationships will be useful to advance your mission anyway. (Don't forget to track and report any legislative lobbying, though — see above.)

Relationships with the media. As with legislators, having a pre-existing relationship with reporters who cover your work is a good precaution, and can also be useful to advance your mission. Contact them when you have good news!

Relationships with allies. Share some of the burden of preparing for the new political environment by networking with other organizations with similar concerns. Join your local, state, and national nonprofit trade associations.

Antiterrorism. If you have foreign activities or expenditures, or if you support other organizations that do, or if you support organizations that could be associated with domestic terrorism, you should be aware of the antiterrorism financing rules under federal law, and take appropriate steps to manage that risk. We have a separate memorandum on these issues.

Potentially illegal activities. If you anticipate engaging in activities that may be illegal under state or federal law (such as trespassing in corporate headquarters, or perhaps providing assistance to undocumented immigrants), or that create a risk of illegal activities occurring in conjunction with your activity (such as protest marches, rallies, or sit-ins), you should understand the risks, and take steps to protect your tax-exempt status. In addition, some states have passed legislation to increase penalties on protestors, and in some cases to impose sanctions on organizations that "conspire" with the protestors to cause damage. For example, Oklahoma passed a bill in April 2017 (Bill No. 1123) that imposes significant penalties on organizations that are found to be conspirators in the willful trespass or damage to "critical infrastructure facilities." It is important to be informed as to possible legislation and enforcement activities in a state in which you may be considering getting involved in a protest or similar action.