Operational Security for Coalitions

An overview of best practices

June 2026

Protect Democracy

Table of Contents

Protect Democracy

Introduction

Coalitions play multiple, and often essential, roles in maintaining a robust civil society and protecting our democracy. Effective coalitions can create conditions for better information-sharing, coordinated advocacy, and greater collective impact. However, coalition activity also can draw negative attention from bad-faith actors.

To continue critical, mission-driven work, coalitions should prioritize building resilience, understanding their risk profiles, and cultivating a **security culture** — a set of security-related norms, values, and attitudes shared by members that inform behaviors and expectations within the coalition — that meets the privacy and security needs of their members. This guide helps orient coalitions to best practices and resources that can help meet these needs. It includes sections on digital security, vetting members, managing listservs, securing meetings and communications, navigating engagement with the media, and responding to politicized investigations. These practices can be a helpful starting place for coalitions looking to think more critically about operational security and should not be treated as a checklist or one-size-fits-all resource.

It is important to remember that the security practices detailed below are only effective if coalitions cultivate a robust, ongoing security culture. These practices should be supplemented by other preparation measures and open conversations about security and privacy. **All members play a role in protecting and maintaining the resilience of a coalition, including by following coalition security guidelines, behaving responsibly, and reinforcing security norms and practices.**

Internal communications: tools, settings & protocols

Training your coalition members to use communication tools with optimized settings is a crucial aspect of keeping your coalition and its members' communications private and secure.

Messaging Services

Signal is a free, open-source, encrypted messaging service that is widely used for secure direct messaging, group messages, video, and audio calls. While the following guidance is aimed primarily at Signal, it is widely applicable to other secure end-to-end encrypted messaging services (such as Threema or Wire). **Keep in mind that anyone admitted into groups and 1:1 chats can take notes or screenshots of communications, even on platforms with end-to-end encryption, so coalition members should continue to practice operational security (OPSEC)**.

- **Enable Disappearing Messages**: Signal does not enable disappearing messages by default, so groups seeking this functionality will need to set it manually for both group chats and DMs. Disappearing messages can be set to time periods as short as minutes or hours, as well as days or weeks. You should consider the settings for both group chats and DMs that best balance your group's need for security, privacy, and information retention.
    - **Message & Call Data**: Note that Signal's disappearing messages feature removes the content of communications, but does not remove the underlying data indicating that communications between parties took place. Similarly, Signal also keeps records of voice and video calls. If this is a concern, one option to consider is deleting groups and chats, not just the messages themselves, in line with your organization's document retention policies. You may also want to consider regular deletion of chats and call history.
    - **Signal and iPhone Call Integration**: On iPhones, Signal has the ability to integrate its call history with the iPhone's native call history, which can compromise the privacy of your Signal calls. This can be disabled on Signal on iOS by navigating to Settings, choosing Privacy, and disabling "Show Calls in Recents."
    - **Signal Contacts Integration**: You may also consider disabling settings like "Share Contacts with iOS" and "Use Phone Contact Photos" on iPhone, as well as "Use address book photos" on Android devices, if you are concerned about Signal recognizing or using your contact names or other information. Each of these settings can be found by selecting the Settings menu, then selecting Chats.

- **Use Usernames, Not Phone Numbers**: Signal allows you to set a unique username, which can be a useful way to share your contact information without directly exposing your phone number.

- **Update Your Devices to Ensure Message Security**: Even if Signal messages are deleted from your device, there is a chance they can be recovered through your phone's notifications system. In order to prevent this, you should be sure you are using the latest version of iOS. To do this, you can navigate to your device settings, choose "General" and then "Software Update."

- **Limit Group Chat Administrators:** Set up Signal chats so that only a limited number of administrators (admins) can vet and approve new members. Having too many admins increases exposure of a chat's history and membership to unauthorized users (e.g., an admin accidentally admits a bad actor, or an admin's account is compromised). Administrators should introduce each new member of the chat to the broader group.

- **Use a Group Link to Add New Members**: Through Signal, you can create a shareable URL or QR code that allows coalition members to request access to a group chat, rather than being added manually or providing a phone number. The link should be configured to require administrator approval before a new member can access the content of the chat.

- **Set a Signal Pin:** Setting a PIN lowers the risk of unauthorized access to a Signal account and the potential consequences (e.g. impersonating coalition members, accessing data, and disrupting internal coalition communications). Even if an unauthorized user gains control of a phone number, they cannot re-register the Signal account associated with that phone number on a new device without entering the associated Signal PIN.

- **Vetting and Adding New Coalition Members:** Vetting is the process of conducting a background check of a potential coalition member before granting them access to sensitive information or internal coalition communications. Most vetting processes involve verifying the identity, intentions, and track record of an individual or group.

    - Adding new members to a coalition will depend on the needs of the coalition. It is recommended to speak with at least one current coalition member as a sort of reference check before adding new members. Having a video conversation with potential new coalition members to go over the coalition community and safety rules and norms (your "code of conduct"), and to confirm contact information, is also a crucial best practice.

- **Regularly Vet/Maintain Existing Group Chats:** Vetting existing group chats on a regular basis can be as simple as comparing the chat's current membership against your current coalition membership list. If you are unsure about the identity of a user, or believe they may have joined or been added in error or for malicious purposes (or they should be removed for some other reason), you can remove and block them from the chat.

- **Remove Former Members Promptly:** It is generally a good practice to promptly remove members who leave the coalition, either of their own accord or because they have violated confidentiality or security rules or norms.

- **Embrace OPSEC Culture:** The most resilient coalitions have a strong security culture, where coalition leaders/admins are empowered and trusted to exercise OPSEC practices, such as denying membership and group chat requests, introducing new accounts into coalition group chats, etc.

- **Additional Internal Messaging Resources:** Consider sharing these messaging resources from trusted experts with your coalition members:

    - Activist Checklist: Signal Security Checklist
    - Security in-a-box: Protect Yourself and Your Communications When Using Signal
    - Surveillance Self-Defense: Tips, Tools, and How-Tos for Safer Online Communications

Email Groups/Listservs

Many of the best practices that apply to Signal and other encrypted messaging services also apply to email groups or listservs, including: limiting the number of admins; vetting new and existing members; onboarding members with a "code of conduct" that outlines norms and expectations; removing people when they present a potential risk or leave the coalition, or they violate the code of conduct; and generally embracing OPSEC culture. **That said, email generally does not offer the same security options as encrypted messaging**. If your coalition had decided that, on balance, it is helpful to use an email group or listserv, consider these additional best practices:

- **Take Pride in Authorship:** Remind coalition members that what they share via the listserv will be published to the coalition, and while you may take measures to ensure privacy, everyone should post only what they would be comfortable having shared widely (think of the "newspaper" rule: if you wouldn't want it printed, don't write it).

- **Prevent Spoofing:** Coalitions with large listservs may be susceptible to impersonation by bad actors, or "spoofing." Spoofing strategies include spamming listservs, requesting sensitive information from recipients, and sharing malicious content via attachments or phishing links. Steps to minimize the risk of spoofing, include:

    - Enforcing multi-factor authentication for admin accounts (and setting the expectation that members will do the same for their accounts).
    - Setting up domain/email authentication protocols.
    - Using only professional/work email addresses whenever possible for admins and members/subscribers.
    - Conducting regular listserv administrative access audits.

- Encouraging members to notify admins as soon as they become aware of compromised emails within the group or listserv (and admins should likewise notify the group/listserv of compromised emails to prevent escalating and cascading hacks/phishing).

- **Configure Default Privacy Settings:** Tailoring a listserv's default privacy settings can help mitigate risk. Privacy menus will vary by platform, but most listserv systems should have the following settings (or similar) that admins can enable:

    - Ensure "review members" or "subscriber list" options are *only visible to admins* so that coalition membership list information isn't exposed.
    - Moderate or limit posting in listservs to help prevent compromised accounts from sending emails to the whole coalition listserv.
    - Disable external image auto-loading to prevent third parties from identifying IP addresses.
    - Set configurations to automatically strip sender IP addresses from email headers.

- **Minimize Data Collection:** When possible, listserv admins should only collect and store personally identifiable information (PII) about members/subscribers that is absolutely necessary for coalition activity.

- **For Sensitive Information, Prioritize Encryption:** If your coalition frequently exchanges sensitive information, consider specialized listserv platforms that provide more robust privacy options. Whatever platform you use, it may be helpful to establish a norm of posters specifying if/how others should engage on the topic (e.g., "reply directly to me only").

- **Use Confidential/Restricted Email Send Options:** Sending sensitive information to email groups or listservs may not be ideal, but when necessary, coalition admins sending such information over email should consider using confidential/restricted email send modes. Major email platforms like Gmail, Microsoft Outlook, Zoho Mail, and Proton Mail have options for restricting recipients from forwarding, copying, printing, and downloading email text and attachments. Gmail, Outlook, and Zoho Mail also have settings for automatic expiration, revocation of access, and password protection of emailed content. Of course, these settings are not a substitute for a strong OPSEC culture, as they do not necessarily prevent screenshots and other high- and low-tech workarounds.

- **Minimize Archiving:** Set email archives to "auto-delete" on a timeframe in accordance with the coalition's record retention policy, or absent a policy, no longer than necessary to provide relevant context/history, e.g. 90 days to 6 months.

- **Email Group/Listserv Resources:** Consider sharing these email group/listserv resources with your coalition members and admins:

    - PEN America: Your Email Safety Toolbox

- The Global Cyber Alliance Cybersecurity Toolkit: Protect Your Email and Reputation

Virtual meetings: security protocol guidance

Virtual meetings are a crucial tool for organizations and individuals working in coalition with one another. The standard method for hosting a virtual meeting can often vary between organizations and groups based on a variety of factors, but there are some basic protocols that help elevate the level of security and privacy for participants:

Vet video call/meeting participants

Regardless of the platform you are using to host your meeting, there are best practices you can follow to ensure video meetings are not compromised. For a meeting that will have public or semi-public sign-ups, be sure to use a registration form to collect relevant info, such as each participant's full name and email address. Asking people to submit their organization name also can help to speed up your vetting process.

Limit information included in calendar invites

When creating a calendar invite for a coalition meeting, it is a good idea to disable invitees' ability to invite other participants, and to disable the ability of invitees to see the full participant list. This ensures that if the calendar invite ends up in the wrong hands, it does not compromise your security.

Designate more than one meeting host

In addition to the personal or organizational account hosting the meeting, at least one more person should be designated as a host and given administrative privileges. This allows other staff members to address issues like vetting participants and removing bad or unwanted actors from the call without compromising the content of the meeting.

- When setting up a Google Meet call in Google calendar, click the settings (gear) icon next to the video call information. Enable "Host controls" and then navigate to the "Guests" tab in the lefthand sidebar. You can add co-hosts by inputting their email address into the co-hosts section of the page.

- In Zoom, start your meeting as the host. In the toolbar, click the participants icon. In the participants panel on the right side of the meeting window, hover over the participant's name you would like to make a co-host and click "More." Then click "Make co-host" and click confirm.

- In Microsoft Teams, join the call as the organizer. Click the icon for "More" (three dots) and navigate to "Meeting options." This will allow you to choose a co-organizer by searching through the list of participants.

Coalition members should familiarize themselves with this process *beforehand* so they can respond quickly if they need to remove users during a live meeting.

Enable a waiting room

Enabling a waiting room for your meeting is one of the most important steps towards properly vetting the participants in a virtual meeting. Waiting rooms are an optional, administrative option on most platforms. The waiting room option should be selected when scheduling a virtual meeting. You can compare the names in the waiting room to your event sign-ups or coalition membership list. For anyone not in the event sign-ups or expected to attend, be sure to vet them before granting access to the meeting. Ideally you will choose a dedicated screener prior to the start of the meeting, who may need to conduct online searches to verify the identity of a participant.

Include a disclaimer

Starting each meeting with a disclaimer helps to both set expectations around shared security practices and make coalition members feel more secure. Here is sample language that can be repurposed for a variety of meetings:

Welcome to the [Coalition Name] [insert month] meeting. Please note the following security protocols: This meeting is confidential and intended for vetted members only. Participants are prohibited from taking screenshots or using AI notetakers and transcribers. We ask that you do not record verbatim notes or attribute specific comments to individuals. If you need to revisit information shared in the chat after the meeting, please contact the [Host] team directly. By remaining in the meeting, you agree to these guidelines.

Depending on the platform, the disclaimer may be best shared with participants via the chat function at the beginning of the meeting. If using Zoom, however, admins have the option of setting a custom message (including disclaimer text and links) that participants must acknowledge before they are permitted to join the meeting.

Disable continuous chat

While virtual meeting chats can be a useful tool for facilitating discussion and community, you should take steps to ensure that the content of those chats does not fall into the hands of malicious actors seeking to compromise your coalition. “Continuous Meeting Chat” is a feature that makes the chat function in a meeting ongoing and accessible at any time (including outside of a designated meeting time). Disabling continuous meeting chats is a key security measure to maintaining confidentiality and security.

- In Google Calendar, open “Video call options” and turn “continuous meeting chat” to “off” (note: this must be done before the meeting starts).
- In Zoom, open meeting settings and toggle “Enable continuous meeting chat” to “off.”

- In Teams, navigate to “Meeting Settings” and disable the chat functionality.

Remove unwanted/unknown participants

One meeting host should be tasked with monitoring the attendees and chat, and removing unwanted participants.

- In Google Meet, click “show everyone,” select the three-dot menu next to the unwanted participant, and click “remove from the call.”
- In Zoom, open the participants list, hover over the unwanted participant, click more, and then click “remove.” **Tip:** Make sure that “allow removed participants to rejoin” is disabled in your account settings.
- In Teams, open the “Participants” pane, find the unwanted participant, select the three-dot menu, and click “remove from meeting.”

Also, ensure in advance that your admins have the ability (and know how) to “mute” all chat messages instantly, or freeze the ability of non-admins from posting if a participant begins spamming a virtual meeting.

Lock meetings in progress

You can “lock” your meeting once everyone you are expecting has arrived, so that unauthorized access is not possible.

- In Google Meet, click the host controls (padlock) icon in the bottom right corner of your screen. Under meeting access, change from “Trusted” to “Restricted.”
- In Zoom, click “Host Tools” on the toolbar at the bottom of your screen, and then select “Lock Meeting.”
- In Teams, click the “people” icon at the top of your screen, and then click the three dot icon in the participants panel. Select “Lock the meeting.”

Virtual meeting security resources

Consider these security resources from the Democracy Security Project to help orient your coalition members towards best practices on meeting security:

- Explainer on Zoom Bomb Threats
- Infiltration & Traps
- Vetting & Verification

Information-sharing: protocols & precautions

Sharing information is one of the greatest values of a coalition, but the protocols and precautions you take are crucial to ensuring that sensitive information is safeguarded without compromising the ability of your coalition to continue its mission-critical work. Here are some guidelines to consider:

Note-taking

Concise and actionable notes are the best way to preserve information without creating unnecessary backlogs of documents and risk exposure if the notes are leaked or accessed by third parties.

- Focus on capturing key, distilled takeaways.
- Refrain from creating verbatim notes or transcripts.
- Do not directly attribute quotes/comments to individual speakers.
- Where relevant, include proper context to prevent misunderstandings.

Confidentiality agreements

Consider using non-disclosure agreements (NDAs) or other confidentiality agreements with members when sharing particularly sensitive information and documents.

Document access

Regularly check the sharing permissions of any sensitive documents so they are not improperly accessed. Make sure that document owners monitor all file share requests.

- Verify the identity of anyone you don't know who is requesting document access — and when in doubt, don't share anything.
- Refrain from using the Google Docs sharing permission "anyone with the link can [view/edit/comment]."
- For sharing sensitive folders and files, consider using platforms like Cryptpad that have end-to-end encryption and don't track personal information.

Document retention

Depending on the size and nature of the coalition, consider adopting coalition document retention policies (including policies that apply to electronic communications) that admins and coalition members are comfortable with and agree to follow. Otherwise, ensure that coalition members have individual or org-wide document retention policies of their own.

- Retention periods should be calibrated to the type of document, so a best practice is to work with an attorney to craft a retention schedule that takes into account your coalition's particular needs and obligations.
- Once you have a retention policy, coalition leadership should push periodic reminders to members (e.g. on a quarterly basis) to take whatever steps are necessary to stay within policy.
- If admins or other coalition leaders create or maintain any coalition records (e.g., meeting notes), those records should be retained in accordance with your own organizational policies (assuming there is no coalition-wide policy). If more than one organization runs or leads the coalition, you should agree on a retention schedule that works best for your organizations and the coalition.

Information-sharing resources

Consider sharing these resources with your coalition members:

- Digital Defense Fund: Google Workspace Admin Security Guide
- National Council of Nonprofits: Document Retention Policies for Nonprofits

Device security: protocols & precautions

When a single coalition member's device is compromised, it can create a "weak link" that jeopardizes the collective privacy and security of the full coalition. Bad actors often use tactics like phishing, smishing, vishing, and spear phishing to take control of a device or even steal confidential information that disrupts a coalition's work. Maintaining digital hygiene and a healthy security culture are first-line defenses against unauthorized access to private coalition data. By implementing these security measures, coalition members can protect their personal devices and information and avoid compromising the coalition.

- **Software and Application Updates:** Encourage coalition members to install software and application updates to ensure that security patches are current. These updates often address security vulnerabilities that could jeopardize the entire group.
- **Password Complexity**: For coalition documents that are password-protected, use either a passphrase (six unique unrelated words strung together) or a complex and unique password of at least 16 characters in length that includes a mix of uppercase letters, lowercase letters, numbers, and symbols. Never use the same password for more than one document or account.
- **Password Management:** For coalition leaders/admins, using a dedicated password manager, such as 1Password, can help you securely store and keep track of different coalition logins.
- **VPN Usage:** Use a Virtual Private Network (VPN) on computers and mobile devices to encrypt your online activity and mask your digital footprint.
- **Authentication Methods:** Always enable 2-Factor Authentication (2FA) and use a minimum 9 digit passcode to sign in to your devices over biometric options like facial recognition or fingerprints.
- **Emergency Biometric Lock**: On an iPhone, to quickly disable facial or fingerprint login settings, click the power button five times.
- **Device Security and IT Training**: Consider sharing these security resources and training opportunities from trusted experts with your coalition members:
    - CyberPeace Institute: CyberPeace Academy
    - Digital Defense Fund: Learn
    - Democracy Security Project: Cyber resources
    - Surveillance Self-Defense: What Should I Know About Encryption?

Security protocols while traveling

Traveling introduces additional risks for coalitions, especially in airports where data can more easily be intercepted and accessed. To ensure your work remains confidential while in transit, we recommend that coalition members take these additional steps.

- **Charging Safety**: Avoid charging your devices at public USB charging stations, like at airports, to prevent potential "juice jacking." If you need to charge, always use a charging brick instead.
- **Public Wi-Fi Security**: Turn on your VPN before joining airport Wi-Fi networks.
- **Operational Security:** Practice diligent OPSEC by using a laptop privacy screen and staying hyper-aware of what information can be seen or heard by those around you.
- **Audio Privacy**: This may seem obvious, but you should always use headphones and be aware of your own speaking volume when taking calls to ensure work or coalition-related conversations are not overheard.

Media coverage & public communications

A coalition itself might become the subject of media coverage and attention. Having communications practices in place can help coalitions prepare for this and other kinds of situations, as well as any risks associated with engaging the media.

- **Media Inquiry and Communications Practices**: Coalitions should align on what to do if a member is approached by the media about the coalition itself or about other coalition members.

- **External Information-Sharing:** Some coalitions are public-facing, while others work more privately. Ensuring clear, external information-sharing agreements can help define what kinds of information the coalition is or is not comfortable with being shared publicly (and how).

- **Doxxing and Crisis Communications:** Coalitions concerned about the doxxing of members, spreading of misinformation, and other crisis communications scenarios may find these resources helpful to review and share:

    - Activist Checklist: Doxxing Defense Checklist
    - Spitfire Strategies: Spitfire's Guide to Crisis Prep & Management

Preparing for & responding to government investigations

Nonprofit organizations and coalitions may face politicized investigations or other threats intended to disrupt or "chill" their collaborative efforts. A coalition member may be targeted to send a message to others within the coalition, or the field at large, that the risk of continuing their work is too great. These kinds of threats seek to intimidate and drain coalitions' time, resources, and morale so they cease lawful activity. Investigations can also cause organizations and individuals to distance themselves from each other out of self-preservation, resulting in coalitions disbanding altogether.

These strategies are all a part of the authoritarian playbook, and autocrats intentionally use them to consolidate power and quash opposition. However, organizations that work in broad coalitions can combat authoritarianism more successfully than those that self-censor or act alone. Read on to learn more about what coalitions should keep in mind when preparing for and responding to government investigations.

Risk tolerance and preparation: have a plan

Coalitions should take time to think through potential risks and scenarios that could affect the full group and individual members. This includes knowing *what to do if one or more coalition members become the targets of an investigation or enforcement action*, as well as *what to do if the coalition itself faces scrutiny*. Keep in mind that coalition members may have varying levels of risk tolerance, which can affect the group's ability to exchange confidential information and collaborate effectively. Questions to consider include: when and whether it makes sense for a targeted member to remain active in the coalition while, e.g., they are under investigation; what rules should apply to any discussion of the investigation itself; and what additional steps the coalition should take to protect the group, its members, and their shared information.

Having honest, transparent conversations within a coalition *in advance* can help the group continue its mission-based work together without engaging in "anticipatory obedience" and without allowing bad-faith actors to divide and conquer. Also, to the extent possible, these conversations should be guided by advice from legal counsel.

Legal guidance

Coalition members should strictly follow the specific guidance provided by their legal counsel and coalition leadership. Coalitions might also consider whether to retain common counsel for the group, or at least counsel for admins or coalition leadership specifically to advise on matters relevant to the coalition.

Keep calm and carry on

If a coalition member becomes the subject of a government investigation, the most important first step you can take is to remain calm. Continue engaging in your regular coalition work while waiting for additional information and legal guidance.

Data preservation

Do not delete coalition files or communications in a way that deviates from your normal document retention practices without guidance from legal counsel. Doing so could unintentionally introduce legal complications.

Educate coalition membership on investigations and threats

Misinformation and complex procedures can intimidate lawful organizations into unnecessary "compliance." For real-world examples and information that demystifies different kinds of government investigations, consider sharing this resource with coalition members:

- Protect Democracy: Nonprofit Investigations Toolkit

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

protectdemocracy.org