

# SECURITY GUIDELINES

2021

## General

1. Every comrade who is part of our organization should know of the heavy attack the U.S. government launched against us. This attack included the FBI raids and grand jury subpoenas of 2010. For many years after, these events defined how our organization practiced security. The lessons learned in that time must never be forgotten. We must also remember that the danger these attacks represent is not over.
2. Our organization has been successful in repelling the enemy's attacks so far. This success comes from the strength of our comrades, our place in the people's movements, and our security members. After summing up many lessons learned during the previous period, it is clear that we must update our methods to reflect the current situation. This document outlines how we should practice security moving forward.
3. There is a contradiction between evaluating our mass work, developing our internal life, and security. That said, *we must never allow a process of spontaneously "drifting" back to the "way things were" before the events of September 24, 2010 took place.* For example, we were relaxed about electronic communications.
4. We are a legal organization and these guidelines should not cause unnecessary alarm. We are building a well-functioning communist organization. In our current environment, security is part of that.

## Compartmentalization and the Need to Know

5. We operate under the principle of democratic centralism. Following the 2010 attacks, our organization became highly centralized in our decision-making. Later, we consciously restored many democratic functions, such as the election of a Central Committee and encouraging commissions to function at higher levels.
6. We carried out a partial compartmentalization of our organization. We have confined the dissemination of some information to the bodies (e.g. the Standing Committee, relevant District Committees) that need to have information to make decisions relevant to their work. This is particularly the case with information related to legal matters.
7. We did not carry out a full compartmentalization—which would mean that unit members would only have contact with (and know the names of) people in their own units or on the leadership bodies they are a part of. We have not done this because it would greatly limit the internal political life of our organization, make consolidation much more difficult, and would limit our ability to have viable national projects.
8. So the question comes up: what information should be on a need-to-know basis?

9. You do not need to know the names of comrades in other cities (red or otherwise) that you are not working with. Unless you are involved with communication issues, you do not need to know how documents, reports from the Center, etc., are being handled. Unless you are directly concerned, or a part of a body responsible for our defense—you do not need to know the details of our legal work. Any finance questions that there may be are, again, on a need-to-know basis. Finally, our international relations are on a need-to-know basis.

### ***Secure Communications and the Protection of Networks***

10. There was a time from 2020-2021 when meeting in-person was not possible due to the COVID-19 Pandemic. During that period, our organization relaxed certain protocols regarding electronic communication. Specifically, this meant comrades held modified meetings through video conferences or over the phone.

11. After the development of a vaccine and as society began to recover, our organization began to practice in-person meetings again, which were held outdoors and with comrades' safety in mind. In-person meetings are much more secure than electronic meetings, and comrades should avoid meeting online or over the phone unless it is absolutely necessary. Our organization is moving forward, and we must raise our standards and practices to a more secure level.

12. Members of our organization should use the most secure method available if electronic communication is necessary. For example, it is much better to use security-oriented apps like Signal than to use a phone's default text messaging application.

13. We have to presume that the phones and email communications of members of our organization are monitored by the enemy. We need to follow the aforementioned *need-to-know* policy when talking on the phone or using email.

14. We are using regular snail mail for some communication, with the exception that comrades who receive documents in this manner will make copies and get them to the comrades they are intended for. We do not see this as a particularly secure method of communication. We see it as a good way to partially protect our networks, i.e., there is not an electronic trail that goes from the center to the entire membership.

15. On a local level we need to be careful about this as well. We should not have communications that go out to the membership of a District Committee, a District as a whole, or even all members of a Unit, that makes it clear to everyone who is receiving said communication is a member of our organization.

16. In the current situation, we need to rely on verbal communication for work that we want to be confidential and to protect our networks. This method is being used nationally and should be used locally too.

17. We should avoid talking about future meeting places by phone or email.

18. **2024 Addendum—General Guidelines for the use of Signal:**

· The title of Signal chat groups should avoid the use of the following: FRSO, Freedom Road, District, Unit, Commission, etc.—anything which

identifies the chat and those who are on it as members of FRSO should be avoided.

- While Signal (and similar end-to-end encrypted communication channels) are more secure than regular telephone calls or SMS text messaging, we should not treat it as a "secure channel." If there is confidential or sensitive information that needs to be shared, it should be done in-person. The content of messages in the chat should not mention FRSO, Freedom Road, or particular component parts of our organization.

- All comrades should enable the "disappearing messages" function for all chats that are related to our political work. Messages should be kept for no longer than 4 weeks.

## **The Enemy Has Big Ears**

19. Comrades must not bring their cell phones or electronics to meetings. Leave them at home or in the car. It is not good enough to turn them off. Faraday bags are useful at times. At important meetings, all comrades and their bags/purses/backpacks should be searched to make sure no one is carrying a cell phone, laptop, Bluetooth device, smart watch, or wearing a wire. This applies to everyone attending the meeting. We should also ensure that our meeting spaces cannot be used against us—smart TVs, landline phones, or Alexa-type devices should be removed or disabled. If we are going to search people, we should pick a meeting location where the search will not seem weird, i.e., where others will not see it.

20. The best way to talk without the enemy hearing is to go to a place where it is unlikely that there are listening devices and keep your voice down. If you have to do this, you should consider whether the person really needs to know what you are telling them. We need to be careful about what we say in cars and understand that it is easy to track the movements of comrades via GPS.

## **Agents**

21. There are three types of enemy agents: members of different police forces and intelligence agencies (FBI, JTTF, local law enforcement, etc.), informants working for them, and right-wingers who volunteer their services to the police or reactionary organizations.

22. There are two basic methods to find agents: behavioral and via verification. While behaviors can raise a flag—and where appropriate should lead to an investigation—this is not the main approach.

23. The main approach is verification. By that we mean we want to determine that people are who they say they are. To do that, we need to do background checks. The most important part of a background check is to meet the family of the person who is joining our ranks. The second method is to get the person's life story (where did they go to high school, recent work history, etc.) and check it out. The first method of visiting family and identifying old friends should not preclude the second. The center can give you additional advice about this. People without a verifiable history or ties should **not be recruited**. If you hit a case you think is an exception (e.g., an **undocumented person**), contact the center.

**24.** The second method of observing behaviors is important, but problematic. The person who comes to meetings, takes too many notes, and does not do much work might be an informer—but they might just be comparatively lazy or shy. The same goes for disruptive people, those who call for action that exceeds street fighting, people who ask too many questions about sensitive things, etc. If comrades (or people we work with) raise questions about a comrade or person we work with in the mass organizations, the local body responsible must *consider* an investigation. If considered and agreed upon, all investigations carried out must be reported to the center.

**25.** Entrapment is now a key tool of the enemy, and all comrades need to be careful about this. Everyone should be aware that things like physical threats against certain public officials can be considered a crime.

**26.** No one should ever be publicly accused of being an agent where without overwhelming evidence and the approval of the center. This includes on Facebook, TikTok, Twitter, and other social media platforms.

**27.** If we have proof that someone is an agent, our general approach will be to make it public (press conferences, posters, etc.).

**28.** There are a few additional ways to find agents, but they are the exception to the methods outlined above. For example, say you get documents via the Freedom of Information Act that says you said something to an informant—but you only said that thing to one person. Or you find their police ID. Or they try to turn a comrade they are dating into an informant and that person turns them in. The list goes on and on, and all the above has happened in the real world.

**29.** Still, in the main, we need to rely on the investigation/verification process.

### ***Eleven "Shoulds" and "Should-Nots"***

**1.** All contacts with the FBI, a U.S. Attorney's Office, or any branch of the Justice Department (including "community relations") must be reported to the local organization which will then contact the center. If requested by the center, a detailed written report will be prepared. Any contact with local law enforcement or immigration that might impact our organization must also be reported.

**2.** No communist would ever chose to answer FBI questions. It is well-known that legally all you need to do is confirm your name and say you want to talk with a lawyer. Period. Standard legal advice says it is a bad idea to discuss any topic with federal agents, even if that is directions to the nearest coffee shop. It is well known that any communication with the FBI, even with an attorney present, is hazardous.

**3.** You do not need to and should not let any law enforcement agency into your home or office without a warrant. If they have a warrant, you need to insist on reading it, and if possible challenging it (if it has a wrong address, name, etc.).

**4.** There are many examples of people heroically resisting grand juries and other legal proceedings directed at the revolutionary movements in this country. Those who resist such proceedings are heroes. Those who fail to resist are the opposite. This form of resistance to the enemy's attacks is a fundamental requirement for anyone elected to the leadership at any level in our organization.

5. You should not make any false reports to the organization about security matters (this includes wild exaggerations). All breaches of security must be reported (e.g., left a stack of internal documents in a backpack at the federal building).
6. District and National level bodies do not keep membership lists or financial records with people's real names. Old records must be destroyed.
7. No district level leader or higher should keep a diary or personal journal. Anyone who has such a thing must place it in a secure location or destroy it. Others who have such a thing should not write about the organization or its members. This includes electronic journals.
8. Anyone who travels internationally must not answer questions from Immigration and Customs about our organization, its members, or fraternal parties, or their members. The only questions one legally need to answer concern the following: who you are, what countries you have been to, your contact with farms, and what things you brought back with you that you want to declare.
9. You must not gossip about comrades or business that does not concern you. If you have complaints, go through the correct channels. You can always bring back your concerns to the center if it is important. Gossip about those under direct attack is evil.
10. Comrades must avoid apolitical arrests (e.g., drugs, fighting in bars, etc.). Anyone who is facing any pressure from law enforcement (or social services, etc.) must report it. Responsible comrades will act in such a way as to minimize the embarrassment of those concerned, while enforcing our rules and protecting our collective security.
11. All work with fraternal parties, foreign revolutionary groups, national liberation movements and progressive governments on any level must first be talked about with the center. **There are no exceptions to this.**