



De-Risking the Physical Red Team

A Safety Primer for Physical Red Teams

Physical Red Teaming is the safest and most effective way to test whether security controls work. Like most activities, it can also introduce risk to an organization if not done with care. This primer was developed to capture some of the key information physical red teams, and others conducting physical penetration testing, need to know before diving into testing.

If you have questions, additions, or suggestions, please don't hesitate to reach out to us at info@pinerisk.com.



Content

03

Legal Implications of
PhySec Red
Teaming: An
Introduction

06

Legal Implications of
PhySec Red
Teaming: De-
Risking the Red
Team

13

The Proposal: Will
you Red Team Me?

16

Letters of
Authorization

25

Laws that Red
Teamers Should
Know

Legal Implications of PhySec Red Teaming: An Introduction

Committing Condoned Crimes: Avoiding legal liabilities while Red Teaming.

Definitions

- **End User:** The target of the red team assessment and recipient of the red team report. For a consultant, this is your client. For an in-house red team, this is your security team.

Overview

A red team emulates (copies) criminals, spies, and competitors who target your organization by committing crimes of fraud, breaking & entering, burglary, theft, cyber and computer crimes, counterfeiting, impersonation, destruction of property, forgery, theft of trade secrets, and more. So, what is the difference between these bad actors and a red team?

Authorization

A red team is authorized, by individuals who are in positions to provide authorization, to conduct tests of security. You cannot commit theft if you are authorized to take documents, and you cannot break and enter into a building that you have authorization to access. It is very possible to de-risk red teaming by paying attention to details, developing a safety and risk management plan, and ensuring all red teamers follow the scope and guiderails of the assessment.

De-Risking the Physical Red Team

First, let's define the types of legal liabilities and involved parties.

There are three primary risk categories for red teamers to review:

- **Risk of Crime:** The risk of committing a crime
- **Risk of Lawsuit:** The risk of being sued
- **Regulatory Risk:** The risk of violating regulatory requirements, or causing an incident that provokes regulatory action

There are multiple parties that may be affected by your actions. These include:

- **Law Enforcement:** May arrest you for committing a crime, or if they perceive that you committed a crime.
- **Prosecutors:** May choose to prosecute you (or not) for criminal activity based on authorization, motives, and actions.
- **Company Employees:** May be victims of social engineering or theft of property.
- **Co-Tenant Employees:** May be victims of social engineering or witnesses to breaking and entering attempts.
- **Vendors:** May be victims of impersonation or social engineering.
- **Vendor Employees:** May be victims of impersonation or social engineering.
- **The Public:** May be witnesses of stressful situations, victims of impersonation or social engineering.
- **The Company:** May be victim of a multitude of crimes if authorization is not addressed properly.
- **The Landlord:** May be a victim of social engineering, impersonation, or property damage if the right precautions are not taken.
- **Equipment Owners:** If you are targeting leased equipment, you must understand the lease language to know whether the owner or lessee can provide authorization for certain types of attacks.
- **Hiring Team:** If a red team practices outside of its authorized scope, the hiring party may seek legal recourse for the actions taken.

De-risking your red team takes effort, expertise, and ethics.

We will dive into nuance and complexity in this article (and its part deux), but ultimately if you act ethically - with the best interest of your client, the law, and the public in mind - all other details will fall in line behind it. This stands in stark contrast to what we in the industry call "Cowboy Shit", which involves red team operators going off the rails and outside the scope for ego, excitement, or adrenaline:

- **Ego:** Doing something to stoke your ego, show off, or prove a personal point - instead of serving the client and their organization.
- **Excitement:** Prioritizing exciting attacks, instead of realistic, probable, and accurate ones is selfish and can risk the outcome of your red team while trying to make one of the most interesting jobs in the world slightly more exciting.
- **Adrenaline:** Red teaming creates adrenaline through detection apprehension, duper's delight, or by other means. Thinking straight and sticking to the scope while in the midst of an adrenaline rush can be difficult but is necessary to ensure the end user gets the best results from your assessment.

Effectively de-risking the red team operation preemptively accounts and prepares for major risks, defines what is and is not within scope of the assessments, and creates the necessary guardrails around the operation that enable the red teamers to have fun while pursuing the mission... without the operation's lead sprouting grey hairs due to the team seeking additional adrenaline - at the expense of the team cohesion and business mission.

Legal Implications of PhySec Red Teaming: De-Risking the Red Team

A "boring" prerequisite for successful operations.

De-Risking the Red Team

How can you move forward with confidence that your red team mitigates exponentially more risk than it creates? By taking the following steps, red team leaders and operators can proactively identify and manage the most significant legal risks while conducting operations.



De-Risking the Physical Red Team

Step 1: Scope the Engagement

A clear and detailed scope proactively addresses legal risks before the engagement begins. Whether you are an in-house red team or a third-party consultant, having clearly defined scope is your primary document providing authorization for the assessment. This may be in the form of a Statement of Work (SOW) for consultants or Red Team Proposal for in-house teams. Scope should include targets, actions, goals, points of contact, locations, systems, tactics, and more.

Step 2: Determine Attack Types

Actions create risk. Determine the actions you are permitted to and prohibited from taking during the assessment and document them. There will always be gray areas, yet over-structuring a red team engagement runs counter to the red team ethos. Initial conversations with red team operations and the end-user about tactics will create a mutual understanding of the approach. There must also be a clear and quick approval flow for operators seeking to use tactics that were not defined as approved/prohibited in the initial review. This may be as simple as a group chat or text chain; however, it should be in timestamped and in writing.

Step 3: Determine Property Ownership

The majority of red team assessments will fall into one of the below categories. Though this may seem complicated, the easiest way of addressing this risk is to review the relevant lease agreement for any language that would allow or prohibit your red team activities.

De-Risking the Physical Red Team

If that is not possible (it often is not), then steps 1, 2, and 4 are especially relevant.

- Fully Owned/Operated: The end-user owns and is the sole occupant of the building.
 - Action: This is the easiest and most ideal scenario. There is no special action needed.
- Owned & Co-Leased: The end-user is the landlord and also one of multiple tenants of the building.
 - Action: Since the landlord is the owner and the end-user, you simply need to avoid any actions to disrupt or break the lease agreement with other tenants. Leases often include the process for which landlord employees (you) can enter tenant space, so make note that you avoid spaces leased to other organizations.
- Sole-Lease: The end-user is the sole lessor of the site.
 - Action: Depending on the landlord's day-to-day involvement, this is often a simple scenario where you only need to understand the delineation of responsibilities for security, locks, and more. If you break a window to a landlord space that is outside of your leased area, you may create additional liabilities. Be prepared to smooth things over with the landlord after the assessment, and to quickly pay for fixes of any damage. Make sure you are compliant with any damage clause language included in your agreement, as some may prohibit any intentional damage to their property.
- Lease with Co-Tenants: The end-user leases part of a building or property with other organizations leasing other parts of the same site.
 - Action: The same as "sole lease" with two caveats. 1) Do not disrupt other co-tenants or access their spaces, and 2) take extra care to not destroy any co-tenant property. The end-user is a tenant paying the landlord so typically there is some good-will; however, this is not the case with co-tenants.
- Subleasing: The end-user subleases part of a property.
 - Action: Find the correct situation above and follow instructions. Review the lease and sublease if possible.

De-Risking the Physical Red Team

- Guest or Vendor: The end-user is not a legal tenant of the site to be assessed.
 - Action: This can be complicated and risky, if not approached correctly. Breaking into a space where the end-user is not the landlord or tenant requires additional authorization by the landlord, tenant, or both. This may occur if a security services company hires an outside consultant to test their personnel or systems.

Government Property: Government property will typically fall into one of the above categories, but may also have additional complications including various departments, which may be standalone entities, managing different aspects of maintenance, security, law enforcement, IT, and others.

Equipment Ownership: Review any equipment that you plan to manipulate, damage, disrupt, hack, circumvent, or otherwise impact during the assessment. Does the end-user have permission from the owner of this equipment to authorize these tests? For example, if Bank of America has an ATM in your end-user's lobby, and your goal is to test the security in and around that lobby - you must determine whether you can open, hack, steal from, or place a skimmer on that ATM. Typically the answer is no; however, it's important to review any significant leased equipment and what the scope of actions involve.

“
The red team is there for a week. The office is there indefinitely. Do not harm their relationship with the landlord or co-tenants.”

Step 4: Safety & Risk Plan

Each red team assessment should have a Safety and Risk Plan. Creating, training to, and following this plan ensures that the operators remain safe, and that a wide array of risks is reviewed and addressed prior to the assessment beginning. The Safety & Risk Plan should include reviews of EH&S risks, armed responder risks, privacy risks, law enforcement risks, and more.

Specific attention should be paid to any regulations the business operates under and any certifications it maintains, such as:

- **Regulatory Risk:** Banks, casinos, hospitals, and other entities have specific information and physical security regulations that govern their approach to security, their actions during an incident, or the consequences of a breach. Understanding these regulations has two benefits:
- **Compliance:** It allows you to understand their security goals and assess their compliance with the regulations, ensuring the end user has actionable and relevant information.
- **Non-Compliance Avoidance:** It allows you to avoid taking action that would place the end-user out of compliance with the regulations.
- **Certifications:** Some certifications, such as PCI (Payment Card Industry), define the actions to take and consequences of a breach. Understanding the specific certifications that the end-user has (or is pursuing) is important to providing them with relevant and actionable information. It also allows you to avoid actions that would put those certifications at risk. It is important to note that most organizations define a breach as unauthorized access of information. As we will see next, red team access of sensitive information must always be authorized.

The safety plan must clearly identify target spaces and any co-tenant or landlord spaces, along with defining what actions may be taken in each space. To avoid the potential for civil or privacy violations, any video recording should often be conducted without sound enabled and detailed discussions should take place as to what actions can be conducted with employees or the public present.

Step 5: Authorization

The red team must receive authorization, in writing, from a party authorized to authorize the engagement - or an Authorized Signatory (AS). In other words, if a nurse tells you that you can conduct a surgery, that doesn't mean you are authorized to do so. Many steps need to be taken prior to you being authorized to conduct a red team assessment, the last of which is a Letter of Authorization from an Authorized Signatory. As the red teamers at Coalfire discovered, this should be from both the entities that control the space being tested and the organization that oversees security for that space. Often these are the same entity, so someone in leadership with security, operations, or finance can provide that authorization. However, for government buildings, sites with contract security, or leased sites, identifying the right AS and ensuring that they sign off on the operation is absolutely critical to mitigating your legal liabilities.

Step 6: Notifications

The most frequent cause of legal liabilities is miscommunication. The following proactive notifications should be considered as part of the red team engagement. Each should be balanced with the need for secrecy to maintain the integrity and authenticity of the operation:

- **Law Enforcement:** For any action with a 5% or greater chance of law enforcement being present or called should likely have proactive notifications to law enforcement. Often, security teams or consultants will have a relationship with local law enforcement and can do this informally through their network. Typically, dispatch will notify a patrol Sargeant that security testing is taking place at a specific site and that is sufficient to help de-escalate most situations.
- **Landlord:** Depending on the scope of the engagement, it is often worthwhile to notify landlord leadership that a test is being conducted. This may help head off any issues that arise during the engagement.
- **Co-Tenants:** At times, it is relevant to notify co-tenant security that a test is taking place, especially if they are good at detecting and responding to suspicious behavior in shared spaces.

Step 7: STOPOP

The red team leader must monitor for any legal risks and be prepared to stop all operations (STOPOP) if they feel that the engagement is becoming too risky. All engagements have diminishing returns over time, and a good leader should determine when continuing an assessment may create more risk than it helps to mitigate. Having clear protocols for when and how to initiate, communicate, and follow-through on the STOPOP notification is essential. If the red team leader, analyst, or safety liaison identifies an armed law enforcement response, a real-world incident unfolding, operational disruptions, or inappropriate security response to the red team's actions, they can quickly initiate a STOPOP and all activities will cease. I have used this many times as armed response officers respond to my operators climbing fences, or as co-tenant security begins to a significant response to a breach of their neighbor's space, not knowing it was a test.

Perception vs. Reality

When law enforcement, security, or the public arrive, they may not understand or appreciate the nuance of the situation, and they may not care that you claim to be, or have a flimsy piece of paper that states you are authorized to be committing what appear to be crimes.



The Proposal: Will you Red Team Me?

What is a proposal and why write one? Learn how to proactively address detractors, gather buy-in, ensure safety, and get CYA approvals.

- /// **Perspective:** This post is written from the perspective of in-house red teams; however, consultants can use this information to:
 - Enhance your business proposals.
 - Assist the team who hired you with selling the assessment to your leadership and peers.

What is a Red Team Proposal

The Red Team Proposal (“proposal”) is a document that sets the foundations, context, goals, and safeguards for conducting an effective red team. It should be viewed by a select few leaders and security peers who are read-in to the operation, along with the entire team of operators and analysts who will be involved with the test. For those who have worked in the Project Management field, think of this as a Project Management Plan - heavily modified to meet the needs of a red team and the security organization. In fact, if the red team wants to take a more authoritative approach, the proposal may be called a “plan” if approvals of others are not required to proceed.



Pondering whether to Prepare a Proposal?

Proposals are important for red teams to:

- **Gain Buy In:** Get leadership and peer buy-in as to the tactics, context, importance, planning, and safeguards in place for you to conduct this assessment.
- **Be on the Same Page:** The entire team involved in the assessment should aid in preparation of or at least thoroughly read and sign-off on the red team proposal.
- **Cover Your A\$\$:** If something were to go awry during the assessment, you have early documentation that showcases your planning and safeguards. If you send the document to leadership and peers, and especially if you get their approval to proceed, you have top cover of approvals and notifications outside of your team.
- **Legal Safeguards:** If your legal team is involved in your review or approval process, they can review and provide feedback on the proposal. The proposal should include a specific section that identifies legal risks associated with the operation and the steps the team will take to address those risks. The legal team can be a great partner to help draft or review this section.
- **Get Approval:** This is the best opportunity to get approval from leadership or legal teams: you have a professional document that includes the context, safeguards, and all relevant details for the assessment. You show leadership that this is thoroughly planned, well thought through, and will be expertly executed - increasing your likelihood for approval.
- **Showcase Professionalism:** Having worked in and consulted across a wide array of security environments, I am confident that a well-prepared red team proposal will put you ahead of nearly all your peer security teams in terms of forethought, documentation, planning, risk management, and strategic thinking. This is an excellent opportunity to showcase your individual and team professionalism to your leadership.

What's in a Proposal?

Each proposal should contain the following components:

- **Introduction:** A paragraph description of who the red team is, what your goals are and, most importantly, how your team supports the wider goals of your security organization and the business.
- **Prioritization:** Why conduct this assessment, against these assets, and why now?
- **Context:** Further details about the origin of this proposal and any contributing factors - within the industry, intelligence relating to it, or the company.
- **Intelligence & Analysis:** Operationalized, tactical analysis of intelligence surrounding the business, the assets, or the industry - from threat intelligence to geopolitical risk assessments to OSINT: intelligence makes the red team world go round.
 - If this assessment stems from a threat model or a Poison Circle, relevant pieces would be included in this section. (Hint: if it does not stem from one of the above, well, it should.)
- **Target (including floors and sites in and out of scope):** This is particularly relevant for multi-tenant and shared spaces where other parties are not part of or subject to the red team.
- **Timeline (dates, reporting, etc.):** Breaking down the phases of a red team - Planning, Intelligence-Gathering, Rehearsal, Execution, Reporting - helps properly allocate resources in a timely manner and set proper expectations with the in-the-know parties and leadership.
- **Expected Tools, Tactics, Procedures (TTPs):** The intelligence section of the proposal will indicate the likely threat actor, and this section will detail how the red team intends to emulate their tactics. Often this section will outline both the tools and the ethics of the methods the team intends to test in the field.
- **List of Participating Red Team Members:** In-field operators are required to carry a valid government-issued ID on them - ensure the name on the ID matches the name on the proposal (and the get-out-of-jail-free letter).

De-Risking the Physical Red Team

- **List of Individuals Read-In to the Operation:** For the authenticity of the red team findings, this should be a very small group of higher-level leadership, and these stakeholders should be documented in writing.
- **Communication Plan:** Who knows about the operation and how much? Who will be receiving live action updates, and who invited to the post-op debrief? How is the communication conducted: between team leadership and operators, team leadership and peers, team leadership and their superiors? Are radios being used or Signal? Who is responsible for sending STARTOP and STOPOP notifications? What happens if a situation in the field escalates? The detailed answers to these questions are contained within this section of the proposal.
- **Safety Plan (EHS, Armed Personnel, Law Enforcement, Legal, Privacy, Public Awareness [will the public notice?], Reputational, etc.):** This one is pretty straightforward for those of us who have been in the field - things will go wrong, and no one likes a bad surprise. Key here is to brainstorm and prepare, make a plan, check your assumptions, and train the whole red team to said plan. Certain things might become leadership calls if situation does not go as planned, but if, as a team, you prepare for the worst and account for Lessons Learned from previous assessments, the number of those calls will diminish significantly.

This may feel like a significant amount of work - and the first time likely will be. However, each time will get easier and, with time, it is significantly easier to update specific sections, with a typical proposal requiring only 50% update of the whole document. The immeasurable benefit of this upfront work is that completing the proposal process often results in a much more robust red team and more risks being proactively addressed.

In Summary

Only you can determine the best approach for your red team. If you want to set a new high bar for professionalism and safeguard the sanctity of the red team (jobs, reputation, and even lives) then preparing a proposal will serve you well.

Letters of Authorization

You finally get caught by security (or the police!)... Now what?

What is the tangible thing that separates a red teamer from a criminal? Being told you are authorized is great, but it is intangible and may be inadmissible. The best proof of that authorization takes the form of a Letter of Authorization (LoA). The LoA is the single most essential tool for red teamers to carry during an operation. It is an excellent de-escalation tool and can keep you out of jail or other serious trouble. Having a valid, serious, and professional LoA that meets the below criteria has saved me when detained by security personnel, where a police helicopter was dispatched to search for me, and when police officers ran towards me with long guns pointed at my chest (more on that in a future post). There are many more benign instances of using LoAs as well, but they make for less exciting stories.



De-Risking the Physical Red Team

Your likelihood of using an LoA depends on your operation's strategy and objectives.

Broadly stated, there are two types of ends to red team operation:

- **Capture the Flag:** You achieve specific objectives (e.g., stealing passwords from a safe or gaining persistent access to the network via a server room) and leave the premises, often without being detected.
 - You test security's Deterrence, Prevention, and Detection capabilities. Response is only tested if detection capabilities are high (which is rare).
- **Escalate Until Caught:** You achieve specific objectives and then continue to escalate the obviousness of your suspicious behavior until you are detected by security and/or other personnel and reported. This allows you to determine the detection threshold while documenting the strengths and weaknesses in security team's response.
 - You test security's Deterrence, Prevention, Detection, and Response capabilities.

From experience, I have used LoAs less than 10% of the time during Capture the Flag operations, and around 80% of the time during Escalate Until Caught assessments. I have carried an LoA on 100% of the tests I have conducted.



What is a Letter of Authorization?

A LoA is (unsurprisingly) a letter that states you are authorized to be conducting the activities that you are conducting. All LoAs must be provided and signed by someone who has undisputed dominion to authorize you to conduct an assessment on the property. All effective LoAs generally have the same components and features:

- **Professionalism:** During a high-stress situation, the LoA has to make a strong impression within seconds to a security officer, building manager, or law enforcement. LoAs should maintain a professional appearance.
- **Letterhead:** LoAs should be on client letterhead.
- **Statement of Fact:** A one or two sentence explanation of what the letter is. Something along the lines of "The holder of this letter is authorized by CLIENTNAME to conduct X activities."
- **Detainment Statement:** "The holder of this letter should not be detained any longer than it takes to substantiate the information listed within this letter."
- **Name:** The full legal first and last name of the red teamer.
- **Dates of Validity:** The date range within which the letter is valid.
- **Location (Optional):** The sites or locations for which the LoA is valid.
- **ID Check Statement (Encouraged):** A statement that says the holder of the letter must be carrying government ID that matches the name on this letter.
- **Compliance Statement (Optional):** For certain sites - that only allow individuals with hard hats or those who have complete certain types of training - the LoA may state that the red teamer has met all requirements for being at the site (assuming they actually have). This is to avoid situations where your red teaming activity is confirmed, but angry site personnel seek to use your lack of training completion, safety equipment, or other requirements against you or the security department.

De-Risking the Physical Red Team

- **First Call:** The client points of contact who authorized the operation. This should include their full name, title, work phone number, and personal cell number (yes, really)
 - Note, you are asking these individuals to call a random phone number you provided to validate what would otherwise be criminal behavior. They are likely to be suspicious of the phone numbers you provide, and rightfully so. Encourage them to use internal messaging or work systems to call the individual. Bonus points if you include screenshots of these internal profiles on the LoA, or use internal language that provides an air of authenticity.
- **Second Call:** A backup point of contact on the client team who is aware of the assessment. This is often the manager of the individual listed in the first call. This should include full name, title, and work and personal phone numbers.
- **Third Call:** A backup to the backup that can get you out of trouble if your primary and secondary points of contact are not answering their phone. This has come in handy for me only once but when I needed it, I really needed it.

Optional Authentication

Option 1: Some organizations can publish internal posts, Wikis, or other announcements that the security team can view with a certain code. Once they enter the code or find a secret internal URL/page, they can view the names, photos, dates of engagement, and locations for the red team assessment. This provides quick and easy authentication on an internal system.

Option 2: For more advanced or mistrustful organizations, the LoAs can include bilateral authentication phrases. I rarely recommend this, but it can be helpful to ward off questions about fake LoAs or concerns regarding authenticity of the phone numbers. For option 2, follow these steps:

- Print a unique authentication phrase on the LoA, something like “Charlie-Zulu-Delta-Xray.”
- Print a counter-authentication letter and provide a sealed copy to the first call (GSOC, security director, or similar) which includes the same phrase.

De-Risking the Physical Red Team

- If you present the LoA, the person you give the LoA to can ask the GSOC, director, or other individual who authorized the assessment for a specific authentication code. When they provide the right one, there is an additional sense that the letter is valid.
 - **Additional note for Option 2:** Ensure your escalation contacts are trained to this protocol and have complete understanding of what is expected of them.

Option 3: For organizations with frequent tests, there can be a phrase of the day/week/month that security officers are told during each shift brief. That phrase is to be used only by testers to prove their authenticity when caught.

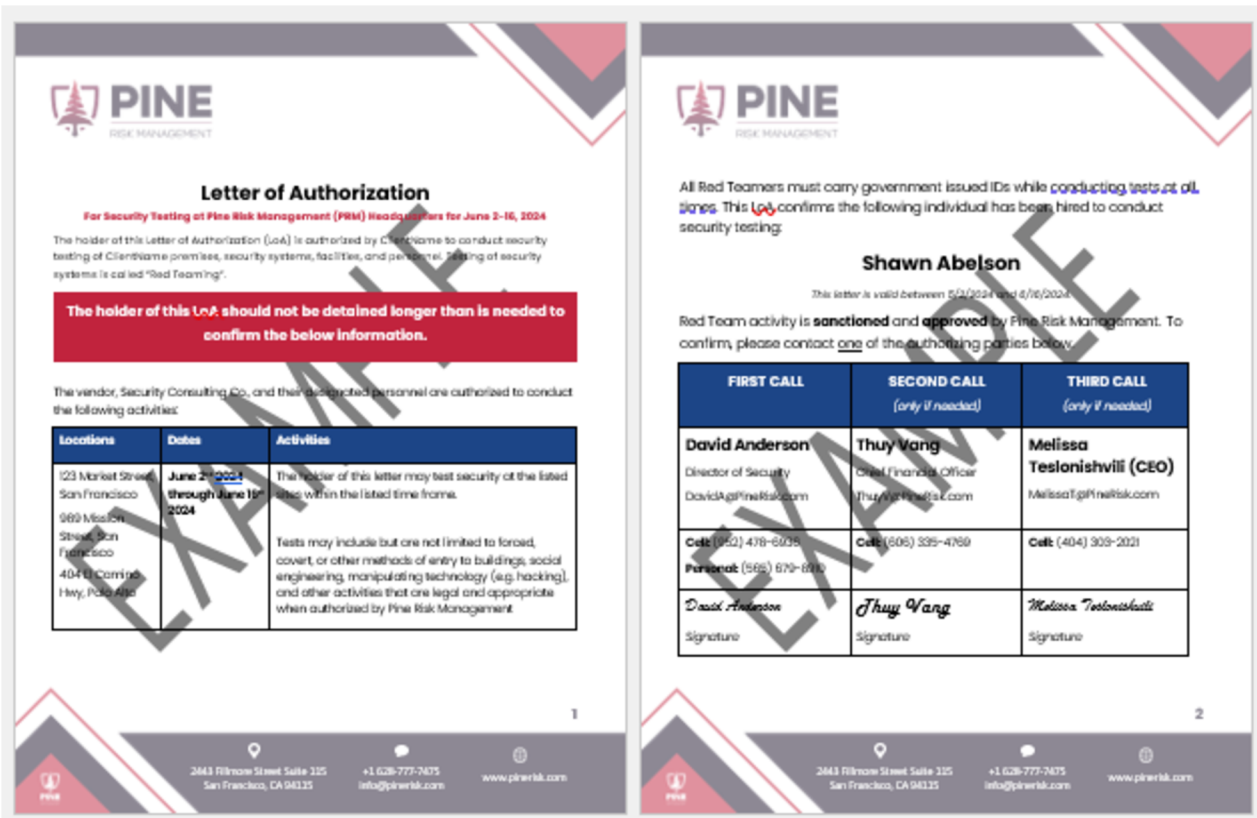
Authorization Caveats

As red teamers, we would be remiss to not learn lessons from our peers. When two Coalfire red teamers were arrested and charged with felonies in Iowa in 2019, a turf war, contract debate, and scope of authority debate ensued between the local Sheriff's office who were entrusted to secure the courthouse and the State Court Administration who oversaw the courthouse and its networks. The boundaries of authority for each party were blurry; however, the fact remains that Coalfire conducted tests of a law enforcement protected space without alerting or collaborating with law enforcement. Here are some key lessons learned:

1. Whoever signs the authorization letter must have the authority to authorize a penetration test.
2. If law enforcement protects a site, you should speak with their leadership and law enforcement leadership should be listed as the first or second calls on the bottom of the LoA.
3. If you are a consultant, check whether the entity hiring you is a building/landowner or tenant of a leased space. Ask them to review their lease to ensure it does not preclude the activity that you are intending to conduct. Understand the landlord (i.e. "base-building" security model, protocols, and policies.)

De-Risking the Physical Red Team

4. If you are part of a company, consider whether you own or lease a space.
 - If you own it, you have significant latitude and greater authority over what occurs in your space. If you are a tenant of a space, review your agreement with the landlord, and ensure your red team tests only your security measures.
 - a. If you have a close relationship and/or rely on landlord security as part of your security model or layers of security, then you should work with your landlord and see if they are comfortable with their security being within the scope of the test. If that is the case, then a landlord leadership should be listed on the LoA as well.



Other Precautions


Two additional caveats come to mind in relation to Letters of Authorization:

1. Ensure the client points of contact listed in the LoA are available and will answer their phones during your test. If you plan a nighttime test, let them know ahead of time and ask them to keep a work or personal phone nearby that night. No matter when you test, it is a best practice to have a group chat (or multiple 1:1 threads) to inform them before activities start and when they end. This will ensure they are available and enable them to relax after the operations are complete.
2. Most red teamers keep their letters in their back pocket, or on the inside of a jacket or shirt. Many security officers are current or former law enforcement. When caught, a red teamer is typically doing something to significantly raise the concern and suspicion of security or law enforcement personnel. These facts combine to create a dangerous situation for the red teamer who may reach for their letter of authorization during the height of an escalated situation with security or law enforcement personnel. Red teamers must ask permission to reach for their LoA prior to reaching into the same place many people carry firearms. Red teamers should explain that they have a letter authorizing them to be there, that it is in their back pocket, and ask permission to show it to the officer.

Letters of Authorization ensure that red teamers are safe and successful in the course of their operations. They can effectively de-escalate situations and keep you out of trouble. Each of the above caveats and suggestions are based on more than a decade of conducting assessments, making mistakes, learning lessons, and improving my approach to ensure my teams are safe and secure.

Resources:

Letters of Authorization (LoA) are sensitive documents as they often provide trained security professionals with approval to do things that are otherwise considered crimes. Templates of LoAs are available to Locks & Leaks paid subscribers for professional use only. Those subscribers may click below to continue.



Locks and Leaks

Risk, resilience, and red teams!
Promoting and supporting the Physical Red Teaming profession, along with...

[Subscribe](#)

Subscribe to Locks and Leaks

Risk, resilience, and red teams! Promoting and supporting the Physical Red Teaming profession, along with articles, tutorials, and stories about physical security, red teaming, and security risk management. Click to...

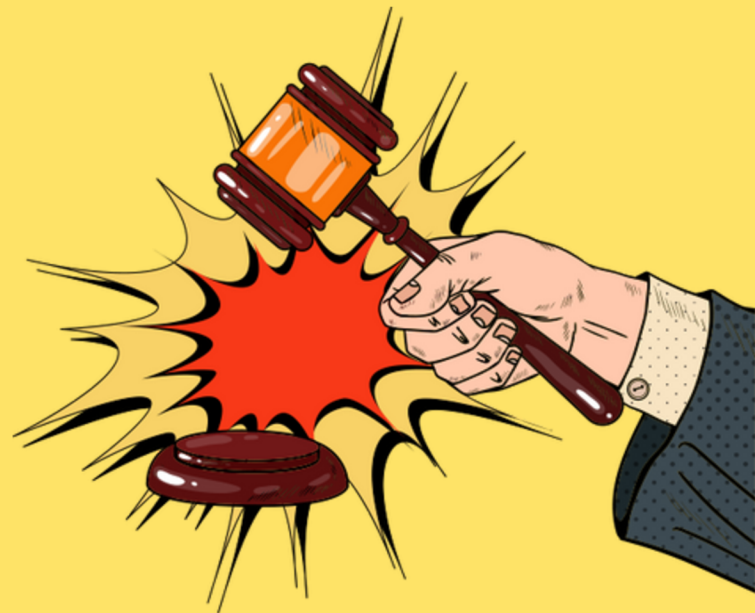
 [substack.com /](https://substack.com/)

Laws that Red Teamers Should Know

What is wiretapping, which states have two-party consent, and are burglary tools illegal without intent to use them illegally?

Laws Around Red Teaming

There is a wide array of laws that physec red teamers should be aware of. It must be noted that laws are broken by conducting unauthorized activities, and the red team is authorized.



De-Risking the Physical Red Team

With that in mind, it is still essential to be familiar with the laws affecting our profession:

- **Burglary**

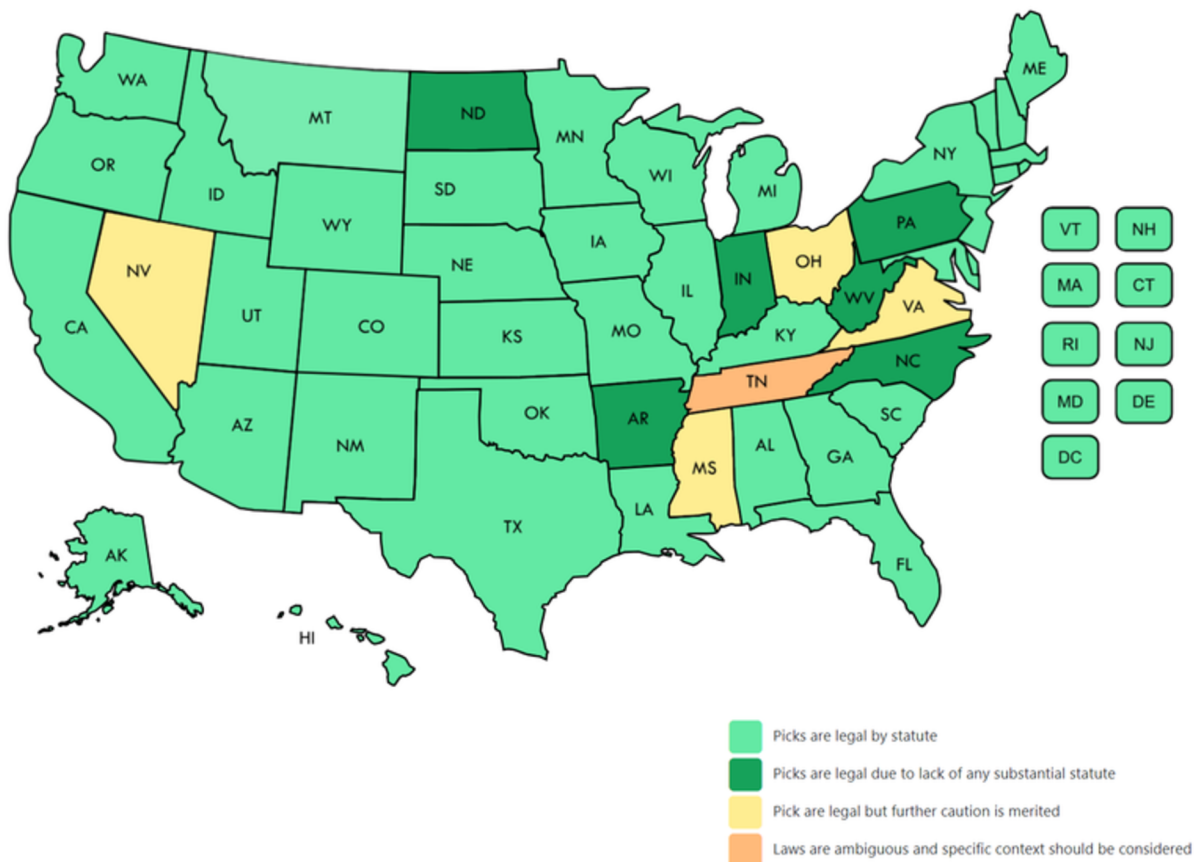
- Varies by state. Intent typically matters less than permission. If you are authorized to be there, then it is not burglary.

- **Trespassing**

- Varies by state. Intent often does not matter, but permission does.

- **Burglary Tools**

- Varies by state. Charges typically require possession and intent to use them illegally.
- Check out TOOOL's fantastic map [here](#).



Burglary Tool and Lock Pick Laws by State (Credit: TOOOL.org)

De-Risking the Physical Red Team

- **Hacking**

- Computer Fraud and Abuse Act [CFAA - 18 U.S.C. § 1030]: Prohibits unauthorized access to computers and networks. Even though it's primarily focused on digital access, physical actions that lead to unauthorized digital access can be covered.
- Many states have versions of CFAA.
- Stored Communications Act (SCA) (18 U.S.C. §§ 2701-2712): Part of the Electronic Communications Privacy Act (ECPA), it protects the privacy of stored electronic communications, prohibiting unauthorized access.

- **Theft**

- Varies by state and jurisdiction. 18 U.S.C. §§ 2314-2315 addresses movement of stolen goods across state lines.

- **Theft of Trade Secrets**

- Economic Espionage Act (18 U.S.C. §§ 1831-1839): Prohibits the theft or misappropriation of trade secrets.

- **Impersonation**

- Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028)
- Makes it a federal crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity.
- Federal Law - Impersonating a Federal Officer (18 U.S.C. § 912)
- This statute makes it a federal crime to falsely assume or pretend to be an officer or employee acting under the authority of the United States and, in such a pretended character, demand or obtain any money, paper, document, or thing of value.
- Federal Law - Impersonating a Foreign Diplomat (18 U.S.C. § 915)
- It's illegal to impersonate a foreign diplomat or consular officer with intent to defraud the United States or any individual.
- State Laws
- Each state has its own laws regarding impersonation of state and local law enforcement officers. The specifics vary by state, but generally, it's illegal to falsely represent oneself as a police officer, sheriff, state trooper, or other state or local law enforcement agent. This can include wearing a uniform, displaying a badge, or using equipment (such as flashing lights) that would give others the appearance of being a law enforcement officer.

De-Risking the Physical Red Team

- Many states also have laws against impersonating other types of government officials, such as judges, inspectors, or other regulatory agents.
- Use of Equipment or Vehicles
- In many jurisdictions, it's illegal to use or possess certain equipment, vehicles, or insignia that are reserved for law enforcement or government officials. This can include police lights, sirens, badges, uniforms, and marked vehicles.
- **Recording of Phone Calls & Wiretapping**
 - Federal Wiretap Act (18 U.S.C. §§ 2510-2522): Prohibits the interception of oral, wire, or electronic communications without consent.
 - NOTE: Some states allow one-party consent for recording a phone call or conversation while others require all party consent. Read [here for the US](#), and here for [Global laws](#) around recording.
- **Interception of Information**
 - Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2510-2522): Prohibits unauthorized interception of wire, oral, or electronic communications. This includes wiretapping and eavesdropping.
- **State Privacy Laws**
 - Vary by state, but many states have laws that protect the privacy of individuals, including protection against video surveillance, audio recording, and other forms of monitoring.
- **Drone Laws**
 - Part 107 License for all red team flights. This means that each Red Teamer operating a drone needs to be licensed, and that each drone itself needs to be registered with the [Federal Aviation Administration](#) (FAA).
 - **NOTE:** If flying at night, at or below certain altitudes, or in restricted airspaces, additional requirements will apply.
 - **EXAMPLE:** Check out the crimes you can be charged with for flying your drone over nuclear submarines in restricted airspace without a license: [This Federal Criminal Complaint](#) from January 2024 indicted a Chinese National and University of Minnesota student who flew his drone into a tree while spying on U.S. subs.

Illegal vs. Prosecutable

Welcome to the danger zone. Any time you are exploring the difference between something being illegal and prosecutable, you may want to have a talk with your legal team. With that said, it's always worth considering the intent of the laws listed above. The goal is to protect the public, prevent harm, promote justice, build a strong society, deter bad behavior, and protect the United States. If you are authorized to conduct assessments and your goals align with the ones listed above (protecting, preventing harm, etc.), you have little to worry about. Your goal is to emulate criminals without committing crimes, which is easy to do with authorization. Even so, having knowledge of the relevant laws will help you in your career, and will ensure that you take steps (document these steps!) to avoid violating rules, laws, regulations, or ethical considerations. A red teamer's goal is ultimately to help protect their organization. Part of that protection is ensuring that you do not create any undue risk (physical, financial, reputational, or other) as you seek to uncover vulnerabilities, systemic issues, and gaps in the security posture.



© Locks & Leaks

08 / 09 / 2024

hlocksandleaks.substack.com/