**COMPANION GUIDE TO ONLINE TRAINING**

Requires Patreon subscription — use alongside the online lessons at fortunefavorsthepreparedcom/sec-02-landing/

# SEC-02: KNOW WHAT YOU'RE SHOWING STUDENT COMPANION GUIDE

**The Operator's Field Reference**

OPSEC Fundamentals · Critical Information List · Threat Analysis
Indicators · Vulnerability Analysis · Risk Assessment · Countermeasures

**Edition v1.0 · 2026**

**Semper Paratus, Semper Gumby**

https://fortunefavorsthepreparedcom/
Nick Meacher

# SEC-02: KNOW WHAT YOU'RE SHOWING — STUDENT COMPANION GUIDE

Companion Guide to Online Training



Published by Fortune Favors the Prepared
Thomasville, Pennsylvania
fortunefavorsthepreparedcom
Edition v1.0 | 2026

> This companion guide requires an active Patreon subscription. It is designed to be used alongside the SEC-02 Know What You're Showing online training series at fortunefavorsthepreparedcom/sec-02-landing/. The online lessons are the instruction. This guide contains condensed reference summaries, key terms, and blank worksheets only — it does not contain the instructional content. It cannot be used as a standalone document.

## ONLINE TRAINING ACCESS

The seven online lessons are available to Patreon subscribers at the Operator tier or above:

**patreoncom/fortunefavorsthepreparedcom**

## INSTRUCTOR-LED GROUP TRAINING

Group sessions and facilitated training are available. Contact:
fortunefavorsthepreparedcom

## How to Use This Companion Guide

**THIS GUIDE IS A COMPANION TO PATREON-GATED ONLINE TRAINING**

This companion guide requires an active Patreon subscription. It is designed to be used alongside the SEC-02 Know What You're Showing online training series — the online lessons are the instruction. This guide contains condensed reference summaries, key terms, and blank worksheets only. It is not a standalone document.

**Subscribe for online training access:** patreon.com/fortunefavorsthеprepared

**Online curriculum:** fortunefavorsthеprepared.com/sec-02-landing/

### What this guide contains

For each of the seven online lessons: a condensed reference summary covering only the key terms, frameworks, and decision rules — not the instruction. The five-step process reference table, CIL format rules, threat assessment matrix, vulnerability analysis framework, risk scoring worksheet, and countermeasure selection guide are included as working tools. The OPSEC cycle worksheet is in the Worksheets section. The instruction is delivered online — this guide is what you use in the field.

### Required workflow — online lessons BEFORE using this guide

**ORDER MATTERS**

Do not open any section of this guide until the corresponding online lesson has been completed. The condensed summaries here are reference material, not instruction. The sequence below is required, not suggested.

- Step 1 — Subscribe at patreon.com/fortunefavorsthеprepared (Operator tier or above)
- Step 2 — Access the online lessons at fortunefavorsthеprepared.com/sec-02-landing/
- Step 3 — Complete all seven lessons including knowledge checks
- Step 4 — Use this guide for field reference and OPSEC cycle worksheets

**THIS GUIDE IS NOT STANDALONE**

The instruction for each lesson is delivered through the online training series. This guide contains condensed reference tables and blank worksheets only. If you have not completed the online lessons, this guide will not teach you the material — it will give you tables whose meaning you do not yet understand.

## Guide Map — What to Reference When

| When you need… | Turn to… |
|---|---|
| The definition of OPSEC and what distinguishes it from privacy tools | Part I, Chapter 1 |
| The five steps in sequence with output for each step | Part I, Chapter 2 |
| CIL format rules and the adversary-first method | Part I, Chapter 3 |
| The three-part threat test and collection methods table | Part I, Chapter 4 |
| The intersection test and indicator categories | Part I, Chapter 5 |
| The risk formula and scoring guidance | Part I, Chapter 6 |
| Countermeasure categories and the matching principle | Part I, Chapter 7 |
| A blank CIL worksheet to fill in | Part II — CIL Worksheet |
| A blank threat assessment worksheet | Part II — Threat Assessment Worksheet |
| A blank vulnerability and risk scoring worksheet | Part II — Risk Scoring Worksheet |
| A blank countermeasure plan worksheet | Part II — Countermeasure Plan Worksheet |

# PART I — REFERENCE SUMMARIES

## Chapter 1: What OPSEC Actually Is

OPSEC is the systematic analytical process of identifying critical information, determining what observable indicators your activities produce, assessing which adversaries can collect those indicators, and selecting measures to reduce that exposure to an acceptable level. Understanding the process before the tools is the foundation the entire method rests on.

### OPSEC Is — and Is Not

| OPSEC IS | OPSEC IS NOT |
|---|---|
| An analytical process run deliberately and repeatedly | A collection of privacy tools or security products |
| A method for identifying what to protect and from whom | Secrecy maximalism — hiding everything from everyone |
| Risk management targeting an acceptable level of exposure | Risk elimination or a guarantee of invisibility |
| A continuous cycle that restarts as conditions change | A one-time training, policy, or checklist event |

> **HISTORICAL ORIGIN**
> OPSEC was formalized after the PURPLE DRAGON study found that the North Vietnamese were not breaking American codes — they were reading American operational patterns. The enemy needed predictability, not secrets. That finding produced the entire discipline.

### Three Words in the Definition That Do the Work

| WORD | WHAT IT MEANS |
|---|---|
| Process | Deliberate, repeatable, with inputs and outputs. Not a posture, not a feeling — something you run. |
| Indicators | Observable traces that activities produce, separate from the underlying information. The adversary collects indicators, not secrets. |
| Acceptable level | A risk management phrase. OPSEC does not promise invisibility. It promises a rational, prioritized reduction in exposure. |

## Chapter 2: The Five-Step Process

The five steps must be run in sequence. Each step depends on the output of the one before it. Skipping or reversing steps does not save time — it produces countermeasures aimed at the wrong targets.

### The Five Steps and Their Outputs

| STEP | NAME | OUTPUT |
|---|---|---|
| 1 | Identify Critical Information | Critical Information List (CIL) — specific facts an adversary needs to disrupt your plans |
| 2 | Analyze the Threat | Threat Assessment — named adversaries with capability and intent assessment for each CIL item |
| 3 | Analyze Vulnerabilities | Vulnerability List — indicators your specific adversaries can actually collect and use |
| 4 | Assess Risk | Risk-Ranked Priority List — scored by probability, impact, and timeliness |
| 5 | Apply Countermeasures | Countermeasure Plan — matched to specific vulnerabilities and adversary collection methods |

### Why the Sequence Is Non-Negotiable

You cannot identify vulnerabilities (Step 3) without knowing your adversary's collection capability (Step 2). You cannot analyze the threat (Step 2) without knowing what information they would need (Step 1). You cannot prioritize risk (Step 4) without a vulnerability list (Step 3). You cannot select countermeasures (Step 5) without a prioritized risk assessment (Step 4).

> **COMMON ERROR**
> Most people jump directly to Step 5 — they buy the encrypted app, switch to cash, use a VPN — without completing Steps 1 through 4. The result is real countermeasures applied to imagined threats, while actual vulnerabilities remain open.

# Chapter 3: Building Your Critical Information List

A Critical Information List is a short, specific, prioritized list of concrete facts that would give an adversary operational advantage if obtained. It is built by thinking from the adversary's perspective first — asking what information they need, not what you value.

## Definition

Critical information: specific facts about your intentions, capabilities, activities, or limitations that, if obtained by an adversary in time to act, would allow them to interfere with your plans or cause harm.

> **SENSITIVE vs. CRITICAL**
>
> Sensitive information is information you prefer to keep private. It becomes critical information only when a specific adversary could act on it in time to matter. Not all sensitive information belongs on your CIL.

## The Adversary-First Method

"If I were my adversary, what specific information would I need to harm or disrupt this person or group?" Work through these adversary question categories:

| ADVERSARY QUESTION CATEGORY | WHAT YOU ARE PROTECTING |
|---|---|
| Plans and intentions | Where you are going, what you are preparing for, when you will act |
| Capabilities and resources | Equipment, personnel count, medical or technical skills, logistics |
| Limitations and vulnerabilities | What you cannot do, where you are exposed, what would stop you |
| Locations and patterns | Where you are, where you go, at what intervals, with whom |

## CIL Entry Format Rules

| FORMAT | EXAMPLE |
|---|---|
| **WRONG — Category** | "Communications security" |
| **CORRECT — Specific fact** | "Our primary comms frequency is 462.625 MHz with CTCSS 100.0" |
| **WRONG — Category** | "Personnel information" |
| **CORRECT — Specific fact** | "The identities of the two members with current EMT certification" |
| **WRONG — Category** | "Schedules and timing" |

| | |
|---|---|
| **CORRECT — Specific fact** | "Our standing meeting occurs the second Saturday of each month at the eastern property" |

### CIL SIZE GUIDANCE

A good CIL has 8 to 12 specific entries. Longer is not better — if everything is critical, nothing is. A CIL you cannot manage actively is not protecting anything. Revisit and update quarterly or whenever your operational situation changes.

## Chapter 4: Threat Analysis

A threat requires a specific adversary with documented capability AND credible intent to collect your critical information and act on it. If any element is missing, the threat is eliminated for planning purposes. Threat inflation wastes countermeasure resources and makes the process feel unworkable.

### The Three-Part Test

| ELEMENT | DEFINITION | FAILURE MODE |
|---|---|---|
| Specific Adversary | An identifiable person, group, or organization with operational reason to want your CIL items | "Bad actors" or "the government" — too vague to produce countermeasures |
| Capability | The means, access, and skill to actually collect the information | Assuming all adversaries have all collection capabilities |
| Intent | Active, credible interest in collecting your CIL items for a purpose that would harm you | Confusing capability with motivation — capable does not mean interested |

### Collection Methods

| METHOD | WHAT IT COVERS | COMMON VECTORS |
|---|---|---|
| OSINT | Open source and public records | Social media, property records, voter registration, court filings, web presence, purchase records |
| HUMINT | Human contact and elicitation | Conversations, members talking to family or neighbors, visitors, outsiders asking questions |
| Physical Observation | Surveillance of location and activity patterns | Vehicle patterns, visitor frequency, delivery schedules, lights, access road traffic |
| Technical Collection | Signals, network, electronic | Radio frequency monitoring, network intrusion, device exploitation |

**THREAT GROUNDING**

Start with the most likely and most capable threats, not the most catastrophic imaginable ones. For most preparedness groups, the realistic threat landscape includes OSINT exposure from social media, HUMINT from members' personal networks, and physical observation by local parties — not nation-state surveillance programs.

# Chapter 5: Indicators and Vulnerabilities

An indicator is any observable trace that your activities produce. A vulnerability is an indicator that your specific adversary has the capability to collect and use to infer a specific item on your CIL. These are not the same thing. The intersection test determines which indicators are actual vulnerabilities.

## Indicator Categories

| CATEGORY | DEFINITION | EXAMPLE |
|---|---|---|
| Signatures | Persistent, characteristic patterns that build over time without active collection effort | Monthly supply orders at the same vendor on the same schedule |
| Associations | Who you know and interact with reveals capabilities, affiliations, and intentions | Member publicly listed as a licensed EMT; vendor vehicle in driveway |
| Profiles | Aggregated pictures built from multiple individually innocuous indicators | Vehicle type + neighborhood + purchase pattern + meeting frequency = group picture |

## The Intersection Test

An indicator becomes a vulnerability only when BOTH conditions are simultaneously true:

1. Your identified adversary has the collection capability to observe or obtain this indicator, AND
2. That indicator allows the adversary to infer a specific item on your CIL.

Run the test separately for each adversary. The same indicator may be a vulnerability against Adversary A and irrelevant against Adversary B.

## Vulnerability Analysis Matrix (Example)

| INDICATOR | CIL ITEM REVEALED | ADV. A CAN COLLECT? | VULNERABILITY? |
|---|---|---|---|
| Monthly supply orders, same vendor | Group size and tempo | Yes (OSINT) | **YES** |
| Encrypted radio traffic | Comms frequency | No (no radio capability) | **NO** |
| Vehicle cluster at property monthly | Meeting schedule and location | Yes (physical access) | **YES** |
| Encrypted digital files | Document contents | No (no technical capability) | **NO** |

### PATTERN BEATS CONTENT

An adversary reading your behavioral patterns does not need to intercept your messages. Signatures and profiles built from observable activity can reveal critical information even when each individual piece appears innocuous.

## Chapter 6: Risk Assessment

Risk assessment produces a prioritized action list. Not every vulnerability requires equal countermeasure effort. The risk formula evaluates probability, impact, and timeliness to tell you what to fix first and what to formally accept.

### The Risk Formula

Risk = Probability × Impact × Timeliness. Rate each variable 1 (Low), 2 (Medium), or 3 (High). Multiply. Higher scores = higher priority.

| VARIABLE | DEFINITION | SCORING GUIDE (1–3) |
|---|---|---|
| Probability | Likelihood the adversary will collect this indicator given access and interest | 1=Unlikely 2=Possible 3=Probable or already occurring |
| Impact | Severity of consequence if the adversary collects and acts on the information | 1=Minor disruption 2=Significant disruption 3=Severe harm to safety or plans |
| Timeliness | Adversary's ability to convert collected information into action within the operational window | 1=Cannot act in time 2=Possible with effort 3=Can act immediately |

**TIMELINESS MATTERS**

A vulnerability that scores High on probability and impact but Low on timeliness carries lower operational risk than the formula alone suggests. Critical information has a shelf life. An adversary who learns your resupply route six hours ahead can interdict. One who learns it three months later cannot.

### Risk Responses

| RESPONSE | DEFINITION | WHEN TO USE |
|---|---|---|
| Mitigate | Apply countermeasures to reduce probability, impact, or timeliness to acceptable levels | Most common response — applies to high- and medium-priority vulnerabilities |
| Eliminate | Stop the activity that generates the indicator entirely | High-risk items where mitigation is insufficient; operationally expensive |
| Accept | Document the vulnerability and the deliberate decision to tolerate it | Low-priority items; a recorded decision, not complacency |

## Chapter 7: Countermeasures and the Continuous Cycle

Countermeasures are the final step — selected after analysis, matched to the specific collection method the adversary uses, and scaled to the priority of the vulnerability they address. The OPSEC cycle does not end at implementation. It restarts.

### Three Categories of Countermeasures

| CATEGORY | HOW IT WORKS | OPERATIONAL COST |
|---|---|---|
| Action Control | Change or stop the activity generating the indicator. Attacks the vulnerability at its source. | Highest — requires changing how you operate |
| Physical and Technical Measures | Reduce adversary collection capability without changing the underlying activity. Encryption, concealment, access controls. | Medium — does not change behavior, only blocks collection |
| Counter-Analysis | Operate on the adversary's analysis. Deception, cover stories, false indicators. | Requires planning and maintenance to remain credible |

### The Matching Principle

Every countermeasure must match the collection method it is designed to defeat. Encrypting communications addresses signals collection — it does nothing against physical observation. Applying a countermeasure to the wrong vector wastes resources and leaves the actual vulnerability open.

> **SELECTION QUESTION**
> What is the lowest-cost countermeasure that reduces this vulnerability to an acceptable risk level? Reserve high-cost solutions for vulnerabilities where lower-cost behavioral changes are insufficient.

### Cycle Restart Triggers

| TRIGGER | WHY IT MATTERS |
|---|---|
| Significant change in operations or plans | New activities produce new indicators; existing CIL may not cover the changed situation |
| Change in membership or personnel | New HUMINT exposure; departing members carry existing knowledge of CIL items |
| New threat identified or adversary gains capability | Changes the vulnerability analysis for existing indicators |
| Set review schedule (minimum quarterly) | Degradation is often invisible until it produces a problem; catches slow drift |

# PART II — WORKSHEETS

## Critical Information List Worksheet

| **Prepared by:** | **Date:** |
|---|---|
| _____ | _____ |

Instructions: Each entry must be a specific fact, not a category. Use the adversary-first method from Chapter 3. Aim for 8–12 entries maximum. Review and update quarterly.

| # | CIL ENTRY (specific fact) | ADVERSARY WHO NEEDS IT | PRIORITY (H/M/L) |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |

## Threat Assessment Worksheet

| **Prepared by:** | **Date:** |
|---|---|
| _____ | _____ |

Instructions: For each adversary, apply the three-part test from Chapter 4. Name the adversary specifically — not a category. List the CIL items they are interested in and the collection methods available to them.

### Adversary 1

| ELEMENT | YOUR ASSESSMENT |
|---|---|
| Name or description | |
| Capability (collection methods available) | |
| Intent (why they want your CIL items) | |
| CIL items they are targeting | |
| PASSES THREE-PART TEST? (Yes / No) | |

### Adversary 2

| ELEMENT | YOUR ASSESSMENT |
|---|---|
| Name or description | |
| Capability (collection methods available) | |
| Intent (why they want your CIL items) | |
| CIL items they are targeting | |
| PASSES THREE-PART TEST? (Yes / No) | |

### Adversary 3

| ELEMENT | YOUR ASSESSMENT |
|---|---|
| Name or description | |
| Capability (collection methods available) | |
| Intent (why they want your CIL items) | |
| CIL items they are targeting | |
| PASSES THREE-PART TEST? (Yes / No) | |

## Vulnerability and Risk Scoring Worksheet

| **Prepared by:** | **Date:** |
|---|---|
| _____ | _____ |

Instructions: For each indicator, apply the intersection test from Chapter 5. Only indicators that pass the intersection test for a named adversary are vulnerabilities. Score each vulnerability using the formula from Chapter 6: Risk = Probability × Impact × Timeliness (1–3 scale each).

| INDICATOR | CIL ITEM REVEALED | ADVERSARY | PROB | IMPACT | TIME | SCORE | RESPONSE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**SCORING REMINDER**

Probability x Impact x Timeliness = Risk Score. Use 1=Low, 2=Medium, 3=High for each. Response options: Mitigate / Eliminate / Accept. Scores of 18 or above = high priority. Scores of 6 or below may be acceptable risks.

## Countermeasure Plan Worksheet

| **Prepared by:** | **Date / Review Due:** |
|---|---|
| | |

Instructions: For each high-priority vulnerability from the risk worksheet, select the lowest-cost countermeasure that reduces risk to an acceptable level. Verify that the countermeasure category matches the adversary's collection method.

| VULNERABILITY | RISK SCORE | COUNTERMEASURE | CATEGORY | MATCHES COLLECTION METHOD? |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

### Review Schedule

| **Next scheduled review date:** | **Trigger condition (if earlier):** |
|---|---|
| | |

**CYCLE REMINDER**

The OPSEC process is continuous. This completed worksheet set is the input for your next cycle and for SEC-06 Applied OPSEC. File it, set your review date, and return to Chapter 1 when conditions change.