COMPANION GUIDE TO ONLINE TRAINING

Use alongside the online lessons at fortunefavorsthepreprared.com/sec-06-hub/

SEC-06: APPLIED OPSEC: ANALYTICAL METHOD AND FIELD APPLICATION STUDENT COMPANION GUIDE

Your Personal OPSEC Field Reference

Exposure · Information Discipline · Threat Analysis · COMSEC · Surveillance Recognition · Public Security · Counterintelligence

OPSEC Process · Worksheets 1-A through 7-A · Operational Checklists · Incident Logs

Edition v1.0 · 2026

Semper Paratus, Semper Gumby

https://fortunefavorsthepreprared.com/

Nick Meacher

SEC-06: APPLIED OPSEC: ANALYTICAL METHOD AND FIELD APPLICATION STUDENT COMPANION GUIDE

Companion Guide to Online Training

Copyright © 2026 Nick Meacher / Fortune Favors the Prepared
All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means without the prior written permission of the publisher, except for personal use and group training directly associated with a preparedness group using this material for its intended purpose.

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

This companion guide is designed to be used alongside the SEC-06 Applied OPSEC: Analytical Method and Field Application online training series at fortunefavorstheprepared.com/sec-06-hub/. The online lessons are the instruction. This guide contains quick-reference tables, field checklists, blank worksheets, and operational logs only — it does not contain the instructional content. It cannot be used as a standalone document.

ONLINE TRAINING ACCESS

The eight online lessons are available online. Support the development and availability of these courses by subscribing to my Patreon:

patreon.com/fortunefavorstheprepared

INSTRUCTOR-LED GROUP TRAINING

Group sessions and facilitated training are available. Contact:
fortunefavorstheprepared@protonmail.com

PREREQUISITE

SEC-06 assumes SEC-02: Know What You're Showing (the entry-level OPSEC course) or equivalent familiarity with basic operational security principles. Students new to security should complete SEC-02 first.

How to Use This Companion Guide

THIS GUIDE IS A COMPANION TO THE ONLINE TRAINING
This companion guide is designed to be used alongside the SEC-06 Applied OPSEC online training series — the online lessons are the instruction. This guide contains quick-reference tables, field checklists, blank worksheets, and operational logs only. It is not a standalone document.

Support the development and availability of these courses by subscribing to my Patreon: patreon.com/fortunefavorstheprepared
Online curriculum: fortunefavorstheprepared.com/sec-06-landing/

What this guide contains

For each of the first seven online lessons: a condensed reference summary (key concepts only, not instruction), quick-lookup tables, decision checklists, blank analytical worksheets, and operational field logs. The OPSEC five-step worksheets (1-A through 7-A) build sequentially — output from each feeds directly into the next. Lesson 8, Applied Scenarios, is a practicum that draws on the tools from Lessons 1–7 and has no separate chapter or worksheet in this guide — work it directly in the online lesson. The instruction is delivered online — this guide is what you carry during active security planning and field use.

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 and worksheets here require the analytical framework the lessons deliver. The sequence below is required, not suggested.

- Step 1 — Support the development and availability of these courses by subscribing to my Patreon: patreon.com/fortunefavorstheprepared
- Step 2 — Access the online lessons at fortunefavorstheprepared.com/sec-06-hub/
- Step 3 — Complete all eight lessons including knowledge checks
- Step 4 — Use this guide during active security planning and in the field

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, the worksheets will not produce useful output — the analytical method behind each is taught in the corresponding lesson.

Guide Map — What to Reference When

When you need…	Turn to…
The OPSEC five-step process and EEFI framework	Part I, Chapter 1
SAPCE indicator characteristics and adversary types	Part I, Chapter 1
Open-source exposure categories and conversation discipline	Part I, Chapter 2
COMSEC, application evaluation, and EMCON	Part I, Chapter 3
Surveillance types, the Rule of Three, and detection indicators	Part I, Chapter 4
Site security, venue discipline, and vehicle OPSEC	Part I, Chapter 5
Decision tree: Coincidence → Attention → Confirmed Pattern	Part I, Chapter 6
Compartmentalization and probing contact recognition	Part I, Chapter 7
Your first-draft critical information baseline	Part II — Worksheet 1-A
EEFI development and the adversary test	Part II — Worksheet 2-A
Threat matrix: adversaries, tiers, disciplines	Part II — Worksheet 3-A
Indicator inventory and aggregation map	Part II — Worksheet 4-A
Digital exposure audit	Part II — Worksheet 5-A
Physical exposure audit	Part II — Worksheet 6-A
Countermeasure plan template	Part II — Worksheet 7-A
Critical information list (quick fill)	Part III — WS-01
Open-source exposure audit (quick fill)	Part III — WS-02

When you need…	Turn to…
PACE plan builder	Part III — WS-03
Surveillance observation log	Part III — WS-04
Site security assessment	Part III — WS-05
SALUTE incident report	Part III — WS-06
Counterintelligence log	Part III — WS-07
Capstone: Security Baseline structure	Part III — Capstone
Doctrinal sources behind the method	Part IV — Doctrinal Sources

PART I — REFERENCE SUMMARIES

Chapter 1: The OPSEC Process and Threat Framework

Key concepts only. Full instruction in the online lessons at fortunefavorsthepreprepared.com/sec-06-hub/

The OPSEC Five-Step Process

Step	Name	What You Do
1	Identify Critical Information	List every piece of information that, if known by the wrong person, creates risk to you, your family, or your group.
2	Analyze the Threat	Identify who might want that information and why. Consider all adversary types. A threat requires both CAPABILITY and INTENT.
3	Analyze Vulnerabilities	Identify how your critical information is being revealed. What observable indicators currently exist?
4	Assess Risk	Determine which vulnerabilities matter most given your realistic threat environment. Triage by likelihood and consequence.
5	Apply OPSEC Measures	Take specific, targeted actions to reduce, eliminate, or manage each prioritized vulnerability.

SEQUENCE IS REQUIRED

Each step produces the inputs the next requires. Countermeasures applied without completing steps 1 through 4 address the wrong problem. The worksheets in Part II enforce this sequence by building on each other.

The Five Indicator Characteristics (SAPCE)

AR 530-1
Repetition is the most dangerous. Operations conducted the same way several times with little or no variation provide an adversary the information needed to determine where, when, how and with what to attack.

Characteristic	Definition and Civilian Application
Signature	The property that makes something identifiable. A lifted truck with recovery gear has a signature. A 12-month purchase history of freeze-dried food has a signature.
Association	The connections between observable elements. Your vehicle at a location + your license plate + visible gear = a linked profile.
Profile	The sum of all indicators: purchases + vehicle + social media + associations + behavior = your preparedness profile. Most people have never audited theirs.
Contrast	Change in an established pattern. Absence from your normal routine or a behavioral shift is a detection tool the adversary uses actively.
Exposure	Duration, repetition, and timing of indicator visibility. Repetition is the most dangerous. Same action, same time, same route = exploitable pattern.

EEFI and the Critical Information List

Term	Definition
EEFI	Essential Elements of Friendly Information — the questions your adversary is trying to answer about you.
Critical Information (CIL)	Your answers to your adversary's EEFI questions — the facts that enable hostile action.
The Adversary Test	"If [specific adversary] had this, what specific harm could they cause that they cannot cause now?" Items that fail this test do not belong on your CIL.
CIL Limit	Fewer than 12 items. A plan protecting everything protects nothing. Priority forces focus.
EEFI Format	State each item as an adversary question: "Does the adversary know X?" — not as a statement.

Civilian Adversary Types and Threat Tiers

Tier	Type	Motivation and Capability	Countermeasure Focus
1	Opportunistic criminals	Not sophisticated, but effective. Identify accessible targets through pattern observation: who has goods worth taking, when the home is unoccupied, whether security measures exist.	Behavioral and physical — what you display and say
2	Motivated individuals with partial knowledge	Former associates, estranged contacts, or personal adversaries. Direct questioning of others, social network exploitation, deliberate observation.	Compartmentalization, limit remaining exposure
3	Ideologically motivated actors / organized groups	May report to others, share in online communities, or take direct action. Active OSINT, coordinated collection.	Layered approach across all disciplines
4	Information harvesters / institutional actors	Collect data about preparedness communities for research, journalism, law enforcement, or political purposes. Legal process tools, technical surveillance.	Only relevant in specific circumstances

INSIDER THREAT
The most dangerous adversary type. Access to your critical information with the ability to misuse or carelessly disclose it. AR 530-1: most dangerous because of access. Addressed in Chapter 7 and Worksheet 7-A.

Chapter 2: Information Discipline

Key concepts only. Full instruction in the online lessons.

Open-Source Exposure Categories

Category	What It Reveals / Why It Matters
Social media	Photos contain location metadata; background reveals gear, home layout, family composition. Deleted posts may be cached. Even private accounts have leakage through associations.
Vehicle markings	NRA sticker + rights decal + stick-figure family + school name = political affiliation, firearm likelihood, family composition, and school schedule. Built in a parking lot in under 30 seconds.
Purchases	Recurring large purchases of food, medical, or equipment create a profile at the retailer, through the payment method, and through delivery visibility. AR 530-1 flags purchase volume as an indicator.
Conversations	The most underrated vector. “We’re pretty well-stocked” is a sentence that changes how someone thinks about your home. Carry-over to third parties happens without the speaker knowing.
Associations	Who you’re seen with, what events you attend, what organizations you belong to, and what you’re photographed near all build your profile in ways no single element reveals alone.

Conversation Discipline Principles

Principle	Application
Answer, don’t expand	“Do you hunt?” → “Yes, do you?” — not a full account of your training schedule or supplies. Answer the question. Stop. Every additional sentence is voluntary exposure.
Redirect rather than deny	Flat denials draw attention and create social friction. “Are you a prepper?” → “I like to be ready for storms — you know how bad last winter was.” True, unremarkable, closes the thread.
Notice the probing question	A question asking for specifics — quantities, locations, timing, membership — is worth noting regardless of the questioner’s apparent intent. The question itself is data.

Principle	Application
Establish family discipline	Every member of the household must understand what not to share. State it explicitly: “We don’t discuss what we have stored, where, or how much.” Ambiguity creates gaps.

The Disclosure Decision Framework

Apply this sequence before answering any question that touches critical information:

- Who is asking, and why might they want to know?
- What do they already appear to know?
- What is the lowest-information answer that satisfies the social context?
- What are the consequences if this information spreads beyond this conversation?

Chapter 3: Communications Security

Key concepts only. Full instruction in the online lessons.

What the Adversary Learns Before They Hear a Word

AR 530-1 identifies these as OPSEC indicators from communications alone:

- Changes in message volume (increased radio, email, and telephone traffic)
- Identification of units, tasks, or locations in unsecured transmissions
- Increased communications checks between individuals
- Sudden imposition of new communications security measures
- Appearance of new radio stations or contacts in a net

KEY DISTINCTION

End-to-end encryption protects content. It does not protect metadata. A fully encrypted message still reveals that you communicated, with whom, at what time, and for how long. Pattern data is often more operationally useful to an adversary than content.

Application Evaluation Framework

Apply these questions before selecting any group communications platform:

- Is content end-to-end encrypted by default?
- Does the platform store message content, and for how long?
- What metadata does the platform collect (who communicated with whom, when, how often)?
- What legal process is required to compel the platform to produce user data?
- Does the platform have a documented history of compliance with government data requests?

Radio Discipline and EMCON

Emission Control (EMCON): the discipline of controlling your electronic emissions to prevent them from becoming indicators.

- Transmit only when necessary — unnecessary transmissions create pattern data
- Avoid identifying locations in the clear — every location reference is a fix
- Brevity reduces exposure — every second of transmission is a second of signal
- Authenticate before sharing sensitive information — verify who you are talking to
- Scheduled check-ins vs. continuous monitoring — reduces pattern predictability

Chapter 4: Recognizing Surveillance

Key concepts only. Full instruction in the online lessons.

Surveillance Type Quick Reference

Type	Definition and Indicators
Physical — Fixed	Direct observation from a stationary position. Vehicle occupied with line of sight to your property; individual in public space without apparent purpose for an extended period.
Physical — Mobile	Following on foot or vehicle. Leap-frog behavior; same vehicle through multiple turns; individual maintaining your pace without apparent destination.
Technical	Electronic collection. Communications intercept, RF detection, camera networks, device-based monitoring. Does not require physical proximity.
HUMINT-based	A human source within or adjacent to your environment reporting on your activities. Potentially the most operationally relevant for civilian preparedness communities.
Digital	Monitoring of online activity, social media, forum participation, purchasing patterns, and location data derived from devices.

The Rule of Three

Observation	Assessment	Action
Single observation	Coincidence	Note it. Maintain awareness. No behavioral change visible.
Two related observations	Attention	Begin systematic observation and written log. Do not alter behavior visibly. Notify security lead.
Three or more, or one highly anomalous observation	Pattern — requires decision	Apply decision tree (Chapter 6). Security lead activates pre-decided protocol.

CARDINAL RULE

Never reveal that you have noticed. A surveillance team that knows you've noticed will either discontinue — losing you the intelligence value — or escalate. If you've identified surveillance, you want to observe it, not end it prematurely.

Fixed vs. Mobile Surveillance Indicators

Fixed	Mobile
Vehicle occupied for extended period with line of sight to target	Same vehicle appearing at multiple locations along your route
Same individual in public space for unusually long time without purpose	Leap-frog: vehicle passes you, stops, you pass, they pass again
New element in a previously known location (vehicle where none was before)	Same vehicle observed through multiple turns without obvious destination
	Individual on foot keeping your pace without their own apparent destination

Digital Surveillance Indicators

- Unfamiliar follows or connection requests from accounts with minimal history
- Social media accounts engaging specifically with your preparedness content and no other content
- Unusual login attempts or account access alerts
- Forum inquiries asking for more information than the context justifies
- “Research” inquiries from journalists, academics, or organizations with unclear affiliation

Chapter 5: Security in Public Environments

Key concepts only. Full instruction in the online lessons.

Site Selection Principles

Factor	Questions to Ask
Approach routes	Can you approach from multiple directions? Is any approach visible from a fixed observation point for extended time?
Observation lines	Can the site be observed from public roads, adjacent properties, or elevated positions? Is there natural screening?
Entry control	Is there a single entry point that creates a bottleneck — and therefore an observation opportunity?
Pattern visibility	Is the site close enough to public infrastructure that repeated use creates visible, recordable patterns?

Venue-Specific Discipline

Venue	Primary Risks	Key Measures
Gun range	Conversation exposure; vehicle observable; targets and drills reveal capabilities and training priorities	Apply conversation discipline; maintain vehicle discipline; nothing capability-revealing shared in the clear
Preparedness / firearms expo	Vendor forms and sign-ups create attendance records; photography common; meeting new contacts ≠ trusted contacts	Minimum-disclosure information on any form; assume you are being photographed; apply vetting criteria before sharing anything sensitive
Field training / camping event	Observable physical footprint; sound travels farther outdoors than expected; photos aggregate location, personnel, and capability data	Convoy discipline (leave separately); no group photography for public sharing; brief participants on conversation security before event

Vehicle and Parking Discipline

- Remove or cover identifying gear visible through windows before arriving at sensitive locations
- Vary arrival times when pattern-sensitivity is elevated
- Avoid the convoy effect — separate departures when group movement would create an observable pattern
- Consider whether your vehicle's make, lift, markings, and accessories already constitute a recognizable signature at recurring locations

Chapter 6: When You Think You're Being Watched

Key concepts only. Full instruction in the online lessons.

The Decision Tree

Level	Threshold	Individual Response
Level 1 — Possible	Single observation, no corroboration	Note it. Heighten awareness. Do not change behavior visibly. Notify security lead.
Level 2 — Probable	Two related observations	Begin systematic observation and written log. Heightened communications discipline. Security lead notified.
Level 3 — Confirmed	Three+ related, or one highly anomalous observation	Activate pre-decided response protocol. Operational pause until assessed.

CRITICAL DISCIPLINE
Do not skip from Level 1 to Level 3. The brain resolves ambiguity quickly and accepts confirmation before the evidence supports it. Force yourself through the decision tree deliberately. Premature certainty leads to premature, visible action.

Confirming Without Revealing

Technique	How It Works
Route variation	Add an unplanned turn or stop. A surveillance team will follow. An innocent vehicle will continue normally. This is confirmation, not evasion.
Timing variation	Change your usual departure time by 20–30 minutes. Absence of the indicator at the new time is informative data.
Deliberate observation	Position yourself naturally to observe whether the indicator reappears. Note vehicle details, partial plates, physical descriptions. Do not stare.

Escalation Mistakes to Avoid

Mistake	Why It Is Harmful
Confrontation	Reveals your awareness, creates an incident, eliminates your ability to observe the threat going forward.
Abrupt evasion	Communicates operational awareness to a professional surveillance team. They adjust; you lose observation ability and gain attention.
Broadcasting through the group	Multiple members altering behavior simultaneously creates a group-level indicator visible to the threat.
Premature certainty	Treating a Level 1 observation as confirmed and taking irreversible group-level action. The damage from a false positive can be severe.

Chapter 7: Protecting Your Intelligence Picture

Key concepts only. Full instruction in the online lessons.

How an Outsider Builds a Picture

Collection Method	What They Learn
Open source	Social media, forum posts, public event attendance, vehicle markings, purchase patterns. Adversaries can satisfy up to 80% of their information needs through open source alone (AR 530-1).
Human collection	Direct conversation, relationships developed over time, information from mutual acquaintances, or placement of a source adjacent to your environment.
Pattern collection	Routine observation of behavior over time. Vehicle movements, recurring locations, timing patterns, and associations build an operational picture even when no single observation is informative.

Compartmentalization Principles

- Not every member needs to know the location of every supply cache
- Not every member needs to know every other member's home address
- Not every member needs to know the full membership list
- Leadership security decisions are shared with those who need them, not broadcast to the group
- When a member leaves, their access to group information is reviewed and closed immediately

Recognizing a Probing Contact

A probing contact is one that:

- Seeks specific information beyond what casual conversation would naturally reach
- Asks about quantities, locations, timing, membership, or capabilities
- Establishes a relationship quickly and moves to sensitive topics faster than genuine relationships develop
- Presents as similarly prepared or ideologically aligned to lower your guard
- Has details in their stated background that are inconsistent or do not hold up under casual examination

RESPONSE PROTOCOL

Note it. Log it. Do not answer specifically. Redirect. Report to security lead if you believe it is part of a pattern. Do not share your concern with the general group until the security lead has assessed.

Insider Concern Indicators

- Asking questions beyond their operational need to know
- Unusual interest in leadership decisions or security arrangements
- Sudden change in financial circumstances or legal situation
- New external relationships they are not forthcoming about
- Behavior that does not fit the pattern of who you understood them to be

PROCESS NOTE

An insider concern assessment is not a decision for one person. Security lead and group leadership assess together. SEC-01 MAG Vetting provides the pre-admission framework; this module addresses post-admission monitoring. The two are complementary, not redundant.

PART II — ANALYTICAL WORKSHEETS (1-A THROUGH 7-A)

The seven analytical worksheets implement the OPSEC five-step process sequentially. Complete each worksheet during or immediately after the corresponding online lesson. Worksheets 1-A through 6-A feed directly into Worksheet 7-A. All fields must have an entry — write “N/A” rather than leaving any line blank.

ORDER MATTERS
Worksheets 1-A through 6-A build your Countermeasure Plan in 7-A. Your plan is only as good as the analysis documented in the preceding worksheets. Complete them in sequence and do not skip the adversary test or aggregation steps.

WORKSHEET 1-A

OPSEC Baseline

Lesson 1: The OPSEC Process. First-pass inventory of critical information, known threats, and potential vulnerabilities. Sets the foundation all subsequent worksheets refine.

WHY THIS WORKSHEET EXISTS

Before you can protect anything, you must name it. Your answers here are deliberately unpolished — you will refine them in Worksheets 2-A through 6-A and convert them to action in 7-A.

SECTION 1 — HOUSEHOLD / GROUP PROFILE

How do you describe your household or group? (size, location type, dependency on outside systems)

What is your primary preparedness concern or planning scenario?

SECTION 2 — FIRST-DRAFT CRITICAL INFORMATION LIST

List information that could allow an adversary to exploit, target, coerce, or compromise you. Do not filter — get it on paper.

#	Critical Information Item	Why It Matters If Exposed

SECTION 3 — KNOWN THREATS (FIRST PASS)

Adversary Type	Likely Intent	Capability You Are Aware Of

SECTION 4 — KNOWN VULNERABILITIES (FIRST PASS)

Vulnerability / Exposure Point	What It Reveals	Current Control?

WORKSHEET 2-A

EEFI Development Worksheet

Lesson 2: Critical Information. Apply the adversary test to each first-draft item. Classify by category. Produce your finalized CIL.

THE ADVERSARY TEST

For each item from Worksheet 1-A: “If [specific adversary] had this, what specific harm could they cause that they cannot cause now?” Items that do not produce a concrete, specific answer do not belong on your CIL.

SECTION 1 — ADVERSARY TEST

Information Item (from WS 1-A)	Adversary Action If Known	Passes EEFI Test? (Y/N)	Notes

SECTION 2 — CATEGORY CLASSIFICATION

EEFI Item	Category	Primary Exposure Channel
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	
	[ ] Capabilities [ ] Activities [ ] Limitations [ ] Intentions	

SECTION 3 — FINALIZED CRITICAL INFORMATION LIST (CIL)

Keep to fewer than 12 items. State each as an adversary question: "Does the adversary know X?"

CIL #	Critical Information Item	Category	Protection Priority (H/M/L)

WORKSHEET 3-A

Threat Matrix

Lesson 3: Threat Identification. Map EEFI items to adversaries, assign tiers, and identify collection disciplines.

CAPABILITY + INTENT = THREAT

Both elements must be present. Capability without intent is not an operational threat. Intent without capability is not a practical threat.

SECTION 1 — ADVERSARY IDENTIFICATION

Adversary Tier & Type	Capability Assessment	Intent Assessment	Threat Level (H/M/L)	Notes

SECTION 2 — COLLECTION DISCIPLINE MAPPING

Adversary	HUMINT	OSINT	SIGINT	IMINT / GEOINT	Notes

SECTION 3 — EEFI-TO-THREAT MATRIX

EEFI / CIL Item	Adversary(ies) Targeting It	Primary Collection Discipline	Risk Priority

SECTION 4 — THREAT SUMMARY

Which adversary poses the highest overall threat to your critical information? Why?

Which collection discipline represents your greatest current exposure?

WORKSHEET 4-A

Indicator Inventory and Aggregation Map

Lesson 4: Vulnerabilities and Indicators. Catalog every observable signature. Map how indicators combine into patterns.

THE AGGREGATION PROBLEM

No single indicator may be critical. But indicators combine. Catalog them exhaustively, then run the aggregation test: if an adversary collected your three most observable indicators, what could they now infer?

SECTION 1 — INDICATOR INVENTORY

EEFI / CIL Item	Indicator (what is observable)	Type (Sig / Pat)	Channel	Current Control

SECTION 2 — AGGREGATION MAP

Indicator Set (list 2+ indicators)	Combined Picture Revealed	Aggregation Risk (H/M/L)

SECTION 3 — RISK ASSESSMENT (PRELIMINARY)

Rate Threat, Vulnerability, and Impact on a 1–5 scale. Score above 30 = immediate countermeasure required.

Indicator / Combination	Threat (1-5)	Vuln (1-5)	Impact (1-5)	Risk Score (T×V×I)	Priority

WORKSHEET 5-A

Digital Exposure Audit

Lesson 5: Your Digital Signature. Inventory platforms, accounts, username linkages, metadata, and device emissions.

OSINT IS YOUR ADVERSARY'S FIRST STOP

Open source collection costs an adversary nothing and can be conducted without your knowledge. Every platform you use, every username that links accounts, and every public record is a collection opportunity.

SECTION 1 — PLATFORM INVENTORY

Platform / App	Username / Handle	Real Name Attached?	Account Status	EEFI Visible? (list items)

SECTION 2 — USERNAME LINKAGE MAP

Username / Handle	Platforms Where Used	Information Visible Across Linked Accounts	Linkage Risk (H/M/L)

SECTION 3 — METADATA AND DEVICE EMISSIONS

Source	Emission Type	What It Reveals	Current Mitigation
Smartphone (location services)			
Photos uploaded online (EXIF data)			
Wi-Fi / Bluetooth broadcasting			
Fitness tracker / GPS device			
Vehicle GPS / infotainment system			
Smart home devices			

SECTION 4 — DIGITAL EXPOSURE SUMMARY

Which EEFI items are currently most exposed in the digital domain?

What is the highest-priority digital mitigation action you can take within 30 days?

WORKSHEET 6-A

Physical Exposure Audit

Lesson 6: Physical Signature. Inventory property, vehicles, routines, materials, and disposal practices.

PHYSICAL SIGNATURES ARE PERMANENT BROADCASTS

A visible antenna, identifying stickers, or a predictable daily routine cannot be unseen. Physical indicators are observable by HUMINT and IMINT without any digital collection.

SECTION 1 — PROPERTY SIGNATURES

Observable Feature	What It Signals	Visible To	Current Control	Risk (H/M/L)
Antennas / masts visible from street or air				
Generator or fuel storage				
Unusual deliveries / supply shipments				
Security measures (cameras, gates, lighting)				
Garden / livestock				
Solar panels / off-grid equipment				
Signage or visible markings				

SECTION 2 — VEHICLE SIGNATURES

Vehicle	Stickers / Markings	Equipment Visible	Routine Pattern	Risk (H/M/L)

SECTION 3 — ROUTINE AND BEHAVIORAL SIGNATURES

Routine / Behavior	What It Reveals	How Observable	Current Variation Practice	Risk (H/M/L)

SECTION 4 — TRASH AND DISPOSAL ANALYSIS

Discarded Material Type	What It Reveals	Current Disposal Practice	Improvement Needed?

WORKSHEET 7-A

Countermeasure Plan Template

Lesson 7: Applying Countermeasures. Consolidate risk findings from Worksheets 1-A through 6-A into a prioritized, written plan.

THREE TYPES OF COUNTERMEASURES

ACTION — change what you do (alter routine, modify behavior, stop an activity) CONTROL — limit access or exposure (restrict who can observe, hear, or access) DECEPTION — provide a false or misleading signal (use with care; only where legally and ethically appropriate)

SECTION 1 — MASTER COUNTERMEASURE PLAN

Vulnerability / Indicator	Source WS	CM Type (A/C/D)	Specific Action	Assigned To	Deadline	Residual Risk

SECTION 2 — PRIORITY MATRIX

	Low Effort	Medium Effort	High Effort
High Risk			
Medium Risk			
Low Risk			

SECTION 3 — DIGITAL COUNTERMEASURE ACTIONS (from WS 5-A)

Digital Exposure	Action	Platform / Tool	Complete By	Done

SECTION 4 — PHYSICAL COUNTERMEASURE ACTIONS (from WS 6-A)

Physical Signature	Action (Conceal / Vary / Remove)	Responsible	Complete By	Done

SECTION 5 — REVIEW SCHEDULE

Review Type	Trigger or Frequency	Next Scheduled Date	Responsible
Full OPSEC review (all worksheets)	Annually or after major life change		
Digital audit refresh (WS 5-A)	Every 6 months or after new platform use		
Physical audit refresh (WS 6-A)	Every 6 months or after change in property/vehicle		
CIL review (WS 2-A)	After any change in capabilities, activities, or situation		
Threat assessment update (WS 3-A)	After significant regional or situational change		

SECTION 6 — OPERATIONAL NOTES

What is the most important OPSEC change you will make in the next 30 days?

What is the hardest indicator to control in your current situation, and why?

What would change in your OPSEC posture if your situation escalated significantly?

PART III — OPERATIONAL WORKSHEETS AND LOGS

The operational worksheets are quick-fill field tools that do not require the full analytical sequence. Use them on demand during active security planning and field operations.

Each entry in the observation and CI logs documents one observation. Store logs securely — not in an unsecured phone note, not in the group chat, not in cloud storage accessible to others.

WS-01: Personal / Family Critical Information List

Complete after finishing Lesson 2. Review and update every 90 days.

Critical Information Category	Specific Items to Protect
Supply storage (location, contents, quantity)	
Defensive measures and their locations	
Group membership and meeting locations/times	
Medical capabilities and providers	
Communications methods and frequencies	
Financial reserves and procurement patterns	
Training schedule and locations	
Relationships with other prepared individuals/groups	
Other:	
Other:	

Date completed: _____ **Next review date:** _____

WS-02: Open-Source Exposure Audit

Audit your own open-source footprint. What does an outside observer see?

Exposure Area	What You Found / Action Required
Social media accounts (list each)	
Profile photos and background content	
Location data in posts or photo metadata	
Vehicle markings and decals	
Recurring purchase patterns / delivery visibility	
Event registration or vendor form history	
Forum or online community participation	
Public records (address, property, voter registration)	
Photos taken at training events or expos	
Associations / individuals you are publicly linked to	

Highest-priority exposures to address first:

WS-03: PACE Plan Builder

Complete after finishing Lesson 3 (COMSEC). Every tier must be tested before it is needed.

Tier	Method / Platform	Status / Last Tested
P — Primary		
A — Alternate		
C — Contingency		
E — Emergency		

Meeting trigger conditions (when do we move down the PACE tiers?):

Meeting Site Security Checklist

Five-minute exercise before any group meeting at a recurring location.

- Can the location be observed from public roads or adjacent properties?
- Is entry to the site visible from public access?
- Can conversation be heard from outside the meeting space at normal speaking volume?
- Are active Wi-Fi, smart speakers, or smartphones present? (Disconnect or remove before sensitive discussion)
- Does the meeting time and location vary, or does it create a predictable, observable pattern?

WS-04: Surveillance Observation Log

Each entry documents one observation. Store this log securely.

Date / Time	Location	Description of Observation

Entry #	Assessment (Coincidence / Attention / Confirmed) + Action Taken
1	
2	
3	
4	
5	
6	
7	
8	

WS-05: Site Security Assessment

Location assessed: _____ **Date:** _____

Step	What to Assess	Findings
1	Walk the approach from the main road. What is visible to a public observer?	
2	Walk the perimeter. Where are the observation lines?	
3	Identify new elements since last use (vehicles, cameras, changed vegetation).	
4	Identify entry/exit points and their visibility from public access.	
5	Assess audio exposure: what conversations are audible from where?	

Security concerns identified / measures recommended:

WS-06: SALUTE Incident Report

Complete immediately after any Level 2 or Level 3 observation. Transmit to security lead via your pre-agreed channel only — not the general group chat.

Element	Your Report
S — Size (how many vehicles or individuals)	
A — Activity (what were they doing)	
L — Location (where you observed it)	
U — Unit/Uniform (vehicle description, individual appearance)	
T — Time (when)	
E — Equipment (visible gear, cameras, equipment)	

Recommended group action based on current level:

WS-07: Counterintelligence Log

A CI log externalizes memory and enables pattern recognition. Store securely.

Date / Time	Location	Description of Event, Contact, or Observation

Entry #	Names / Descriptions + Assessment + Action Taken
1	
2	
3	
4	
5	
6	
7	
8	

CAPSTONE — YOUR SECURITY BASELINE

The capstone deliverable is a completed Security Baseline document covering all seven module areas. Standard: a working document that a different group member could pick up and use. All seven worksheets in this guide feed directly into your Security Baseline.

Capstone Section	Source in This Guide
1. Critical Information List	WS-01 / Worksheet 2-A (CIL)
2. Open-Source Exposure Audit	WS-02 / Worksheet 5-A
3. Communications Assessment (PACE Plan)	WS-03
4. Surveillance Awareness Plan	WS-04 observation log + Chapter 6 decision tree
5. Public Environment Assessment	WS-05 / Worksheet 6-A
6. Pre-Decided Response Protocol	Chapter 6 three-level reference — build your group's version
7. Countermeasure Plan	Worksheet 7-A
8. CI Log	WS-07

COMPLETION STANDARD

A sample completed baseline for a fictional three-person preparedness household is available in the online course after capstone submission. Complete your own baseline before reviewing the sample. The purpose of the sample is verification, not substitution.

PART IV — DOCTRINAL SOURCES

Doctrinal Sources

Source	Publisher	Relevance
AR 530-1: Operations Security	Department of the Army	Primary doctrinal source for the OPSEC five-step process, SAPCE indicator characteristics, and open-source exposure doctrine throughout this course.
DoDD 5205.02E	Department of Defense	Policy authority for OPSEC program requirements, countermeasure mandates, and the role of threat analysis.
DoDM 5205.02-M	Department of Defense	Operational manual for the OPSEC process; CIL development, risk assessment, and vulnerability analysis procedures.
JP 3-13.3: Operations Security	Joint Chiefs of Staff	Joint doctrine for OPSEC planning; source for countermeasure types (action, control, deception) and threat analysis methodology.
FM 2-22.3: HUMINT Collection Operations	Department of the Army, 2006	Human intelligence collection doctrine, surveillance recognition frameworks, and counterintelligence fundamentals.
FM 34-2-1: Reconnaissance and Surveillance	Department of the Army	Surveillance detection and reconnaissance doctrine; systematic observation and indicator analysis methodology.
MCRP 2-10A.1: Signals Intelligence	US Marine Corps	Radio discipline, EMCON principles, and communications security doctrine adapted for civilian group use.
MCRP 3-11.3: Scouting and Patrolling	US Marine Corps	Tactical site assessment and route selection principles underpinning Chapter 5 public environment content.
Camp X SOE Training Manual (STS 103)	Special Operations Executive	Tradecraft source for cover and conversation discipline, anti-surveillance protocols, and information security under operational conditions.

Source	Publisher	Relevance
Counterintelligence for National Security	CIA / Defense Intelligence School	CI fundamentals, insider threat doctrine, and source recognition principles underlying Chapter 7.
DoDI 3115.12: Open Source Intelligence (OSINT)	Department of Defense	Defines OSINT as an intelligence discipline; foundational to digital exposure and open-source collection methodology.

OPSEC is not about paranoia. It is about knowing what you are showing and making deliberate decisions about it.

A prepared person who understands their own exposure is not more fearful — they are more effective. That is the purpose of this course.

SEC-06 Student Companion Guide · fortunefavorstheprepared.com