

the FOUNDATION FOR
INFRASTRUCTURE RESILIENCE

Courseware Foundations

An Introduction

Foundation for Infrastructure Resilience

November 2026

Foundation for Infrastructure Resilience, Inc. ("FIR"™), a non-profit 501(c) (3) Delaware Corporation.

Our Vision

A secure and prosperous future where resilient and sustainable critical infrastructure empowers communities and safeguards our nation.

Our Mission

Improve the quality of life and help ensure the continuity of the United States by facilitating sustainable communities and resilient critical infrastructures, fortified against threats and meeting the needs of the 21st century.

Legal Disclaimer: The Foundation for Infrastructure Resilience makes no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the content of this document, third party content or references to services or information referenced or available through links herein, and further disclaims all warranties regarding any information contained herein, including any implied or express warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, arising out of any course of dealing or usage of trade, that the third-party service will be uninterrupted, error free or free of harmful components.

© 2026 Foundation for Infrastructure Resilience
All Rights Reserved

Contents

Introduction (if required) ..... **Error! Bookmark not defined.**
FIR Book 1: Foundations — An Introduction 1
About this book set, and who it is for 1
About this book 1
How this book is organized 2
Chapter 1 — Why this matters 3
The event this book plans for 3
The 72-hour gap 3
Why a grid-down event is different in kind 3
What this book is for 3
Chapter 2 — How a community stands up: the infrastructure dependency stack 4
A community stands up like a building 4
The stack, from the bottom up 4
Why the foundation is people, not power 4
The mutual dependency deadlock 4
The attrition spiral 5
Reading the stack 5
Sidebar: How the people restoring the grid communicate 5
Chapter 3 — Who threatens it 7
The three vectors 7
EMP and GMD, briefly 7
The four-party ecosystem 7
Pre-positioning and combined arms 7
Why an adversary would do this 8
Why some places matter more 8
Threat posture, not prediction 8
Chapter 4 — What 30 days without power actually means 9
The first hours 9
The first days 9
The first weeks 9
Why it doesn't just come back 9
Reading the timeline as a planner 9
Chapter 5 — Your own readiness 10
Can you get home 10
Personal PACE: staying in contact 10
Can your family survive 30 days 10
Water, treatment, and sanitation 11
Why this belongs in a foundations book 11
Chapter 6 — Knowing what is true 12
Two standards 12
The five source tiers 12
Four habits on every claim 12
Read the silence, and label the confidence 12
Chapter 7 — Making the case without causing paralysis 13
Why alarm backfires 13

The shape of a case that lands....13
Match the message to the room....13
The short form and the full course....13
Chapter 8 — How FIR is organized, and where you go next....13
The six lines of effort, in order....13
How readiness is measured....14
The courses and credentials....14
Where you go next....14
Appendices....15
Take the next step....15

FIR Book 1: Foundations — An Introduction

The prolonged grid-down event, the infrastructure that fails, and what a community can do.

Foundation for Infrastructure Resilience — Book 1 of the FIR introductory set. Draft of November 3, 2026.

About this book set, and who it is for

The FIR introductory set is written for people who are new to all of this. It assumes no background in emergency management, infrastructure, the military, or finance — only an interest in why a long loss of the electric grid would be so dangerous, and what can be done about it. Each term is introduced in plain words the first time it matters, and the companion *FIR Field Handbook* holds the full glossary for anything you want to look up again.

These five short books are introductions, not the full course material. Each one gives a clear overview of its part of the FIR method — enough to understand it, plan with it, and know where the detail lives — but it is not a substitute for the FIR courses, which remain the version of record for reference and instruction. A later, more detailed textbook set will carry the complete student-guide content; these introductions are the on-ramp to it. The four Foundation courses (BSE 099–102) and the free member orientation (FIR 001) cost nothing to start — browse every course and enroll at the FIR course catalog.

The set is built to be read in order:

- **Book 1, Foundations** — the problem: what a Black Sky Event is, how a community is built, who and what threatens it, and what a household can do. Everyone starts here.
- **Book 2, The Assessment Method** — how a trained assessor measures a community's readiness and turns it into a plan that can be funded.
- **Book 3, The Resilient Community** — what a community that has done the work looks like in a prolonged event: how it governs, feeds, protects, and sustains itself.
- **Book 4, The Certification Path** — how that readiness is independently verified and credentialed: the evidence standard, the Diamond Blue certification, and the people qualified to sign it.
- **Book 5, The Domains** — how each kind of infrastructure is actually hardened, sector by sector.

This is Book 1. It is the one book everyone should read, whatever their role. Later books build on it; where they move quickly, the idea underneath was explained here.

About this book

This is Book 1 of the FIR introductory set. It is the shared picture every later part of the FIR method rests on: what a prolonged grid-down event is, how a community is actually built, who and what threatens it, and what a reader can do about it.

It is written as a standalone professional book that also serves enrolled students. The level is a professional handbook, about grades 10 to 12, and it is written for every level of government — from a township or parish to a state — as well as for the emergency manager, the utility manager, and the community member. It assumes no prior FIR course.

The book is a narrative. The companion reference — the glossary of record, the Foundation and course field cards, and the sources — lives in the *FIR Field Handbook*. Where a definition is in question, the Handbook carries it. Where instruction is in question, the online courses are the version of record.

How this book is organized

The eight chapters move from why a prolonged grid-down event matters, through how a community works and what threatens it, to what a reader can do and how to make the case to others.

Chapter 1 — Why this matters: the grid-down event this book plans for, and FIR's 30-day horizon. Chapter 2 — How a community stands up: the infrastructure dependency stack. Chapter 3 — Who threatens it: the three vectors and the four-party ecosystem. Chapter 4 — What 30 days without power actually means: the cascade on a clock. Chapter 5 — Your own readiness: getting home, then holding thirty days. Chapter 6 — Knowing what is true: source discipline. Chapter 7 — Making the case without causing paralysis. Chapter 8 — How FIR is organized, and where you go next.

Chapter 1 — Why this matters

Most emergencies end. A storm passes. Crews drive in from the next state. The lights come back in hours or days, because somewhere nearby the grid is still up and help is still coming. A Black Sky Event is the emergency that does not work that way.

The event this book plans for

A Black Sky Event is a grid-down event lasting weeks or longer: a wide-area failure of the electric grid and the infrastructure that depends on it, with no unaffected region able to send help. The cause can be a cyber attack, a physical attack, a severe solar storm, or an electromagnetic pulse. The cause matters less than the length. For planning, FIR treats a Black Sky Event as lasting at least 30 days.

That one feature — no unaffected neighbor — changes everything. Ordinary disaster planning assumes mutual aid: the outside world is intact and sends people, fuel, water, and money. Strip that assumption away and the plans built on it stop working.

The 72-hour gap

Households and communities are usually told to prepare for 72 hours. That number assumes help arrives on the third day. In a Black Sky Event, no help arrives on the third day. The shortfall begins on Day 4, and it widens from there.

FIR plans for at least 30 days. The point is not that the event ends at 30 days — it may not. The point is that a household and a community able to hold 30 days have crossed the gap where most people fail, and have bought the time that recovery needs.

Why a grid-down event is different in kind

A Black Sky Event is not a bigger storm. It is a different kind of problem. Modern life runs on electricity, and almost everything else runs on electricity too: water pressure, fuel pumps, payment systems, refrigeration for food and medicine, the networks people use to coordinate. Take the grid down for long enough and each of these fails in turn, and then they begin to pull on one another. The next chapter shows how.

The danger lives in the duration. A short outage is an inconvenience. A long one, with no outside help, is a threat to the life of a community.

What this book is for

Book 1 gives the shared picture. It is meant to be read once for understanding and kept as a reference. A reader in government will use it to grasp the scale of the exposure and the order in which things fail. A community member will use it to see why household readiness is not a private hobby but a piece of the whole. Everything FIR does — the assessment, the scoring, the roadmap, the training — is built on the foundation this book lays down.

Chapter 2 — How a community stands up: the infrastructure dependency stack

A modern community looks like many separate services — the power company, the water utility, the hospital, the grocery chain, the phone network — each with its own staff, budget, and building. It does not fail like many separate services. It fails like one structure, in a fixed order, because the services rest on one another. The infrastructure dependency stack is FIR's model of that structure: it places the sixteen critical infrastructure sectors in tiers and shows which sectors depend on which, and in what order they fail.

A community stands up like a building

The model looks like a building because it behaves like one. A building stands on its foundation; load runs downward; and if the foundation gives way, everything above comes down, however sound the upper floors are. The dependency stack follows the same logic, with one difference that makes a prolonged outage so dangerous: the lower floors do not merely rest on the foundation — several of them hold one another up. Pull one out and the others cannot stand alone.

The stack, from the bottom up

Dependency flows upward; failure is read from the bottom. When a lower tier fails, every tier above it fails in sequence — which is why the order of the tiers, not the prominence of any one sector, is what matters.

Why the foundation is people, not power

It is tempting to put energy at the very bottom and stop there. FIR places two human tiers beneath it on purpose. Every sector, the power grid included, runs on people — operators, dispatchers, repair crews, nurses, drivers — and those people have households that come first in a crisis. That is Tier 0H, the Human Foundation, and it is the deepest dependency in the stack: no sector recovers faster than its workforce is willing and able to stay at its post. Beneath governance in the same sense sits Tier 0S — security, governance, and the rule of law. Without legitimate authority and basic order, infrastructure is not an asset to be restored; it becomes something to be fought over. Energy is the single point of failure, but people and lawful order decide whether energy can be brought back at all.

The mutual dependency deadlock

Energy and the three lifeline sectors — water and wastewater, communications, and transportation — do not fail and recover independently. Each needs the others to return. The power plant needs water to cool it and fuel delivered by road; the water utility needs electricity to pump and communications to coordinate; the fuel trucks and repair crews need open roads and working phone and radio networks to find the fault and reach it. This is the mutual dependency deadlock: none of the four can be restarted by itself, so recovery is not a matter of

hours or days but of bringing the whole set back together. It is the central reason a true grid-down event is measured in months rather than days.

The attrition spiral

The deepest tier is also the quickest to turn an outage into a catastrophe. When the taps stop and the shelves empty, the operators who keep every sector running face the same shortages as everyone else — and they leave their posts to protect their families. Fewer operators slow restoration; slower restoration deepens the shortage; the deeper shortage sends more operators home. This is the Tier 0H attrition spiral, and it sets the ceiling on every recovery effort. It is the mechanism that converts a grid outage into a civilization-level event, and it is why household readiness — the subject of later chapters — is not a personal indulgence but a piece of infrastructure in its own right.

Reading the stack

The stack is a diagnostic tool, not a diagram to admire. Read from the bottom, it tells a planner where to look first and what a loss truly costs. A threat to a single operations-tier plant is serious; a threat to energy or to a lifeline is structural, because of everything that stands on it; a gap in the workforce or in lawful order is deeper still. Every later part of the FIR method — the assessment, the scoring, the roadmap — inherits this order: it reads a community from the foundation up, hardens the tiers that carry the most weight first, and never treats a top-floor fix as a substitute for a sound foundation.

Sidebar: How the people restoring the grid communicate

When the public cell network goes down, the crews restoring power are usually not silent. Electric utilities run their own two-way radio systems — land mobile radio, in digital standards such as P25 and DMR — to carry voice between field crews and dispatch, with one-button push-to-talk talkgroups, and increasingly a private data layer on licensed spectrum. Against the cyber and physical vectors, and against ordinary storms, this is a genuine strength: in one hurricane a utility's trunked radio kept working for the days its cell service was down. Owned radio is independent of the public network, and transmission sites often sit beyond cell coverage anyway.

The EMP/GMD vector is different because radio is easy to over-claim here. A high-altitude electromagnetic pulse damages unprotected electronics, and radio infrastructure is exposed in exactly the places that give it its reach: repeaters, base stations, and the trunking controller are fixed electronics tied to tower-top antennas and to power and feed lines, which act as the paths the pulse travels in. Plan on the wide-area repeater and trunked layer being degraded or down — and the grid power it runs on with it. What tends to survive is the smallest, simplest equipment: handheld radios with short antennas, especially spares stored powered-off in shielded (Faraday) containers, used simplex — radio to radio — within line of sight, at a fraction of the normal range. A high-altitude burst also disturbs the ionosphere, so long-range HF can be

blacked out for a few hours before it recovers, while groundwave and line-of-sight are not affected.

The take away is: a community or utility that can keep talking through a cyber attack or a storm has earned that against those vectors; keeping a radio layer alive through an EMP is a separate, harder problem that takes deliberate hardening — shielded sites, surge protection on antenna and power leads, protected backup power — and a simplex, line-of-sight fallback plan. Communications is a lifeline that stands on Energy and on survivable electronics: plan it one vector at a time.

Chapter 3 — Who threatens it

A community can fail from a solar storm that targets no one. It can also fail because someone chose it. Both belong in a plan, and they are planned for in the same way: by the kind of damage they do, not by the name on the threat.

The three vectors

FIR measures readiness against three threats, and scores each on its own. They are never blended into a single number, because a community strong against one can be wide open to another.

Cyber is remote reach and patience — the patient intruder. An attacker can be inside a network for a long time before acting, and the first sign of trouble is often the attack itself. Physical is locality and access — the arriving attacker. It takes presence: someone at the substation, the pump station, the fiber run. EMP/GMD is simultaneity and reach — the single event that touches everything at once, with no unaffected neighbor to help. A plan that counts on outside aid has no answer to it.

EMP and GMD, briefly

An electromagnetic pulse has three parts, and they do different damage. E1 arrives in nanoseconds and damages electronics directly. E3 builds over seconds to minutes and drives the kind of current that damages large transformers. E2 behaves like lightning, so most systems are already protected against it. A geomagnetic disturbance — severe solar activity — does E3-type damage to long transmission lines and the transformers tied to them.

The reason EMP and GMD sit in their own vector is the combination of reach, simultaneity, and slow repair. The components most at risk — large power transformers — are long-lead items: many months to replace one, and longer when many fail at once.

The four-party ecosystem

When the threat is deliberate, FIR plans against a documented set of adversaries: China, Russia, Iran, and North Korea, together with their proxies, treated as mutually reinforcing threats to U.S. infrastructure. FIR calls this the four-party ecosystem.

It is a planning basis, not a prophecy. FIR centers on it because it is concrete, documented, and public — one threat posture broad enough to plan against, not the only one. A community's full picture still has to include its own local hazards.

Pre-positioning and combined arms

Two patterns matter most to a planner. Pre-positioning is quiet, persistent access established inside infrastructure networks without acting — access held for a day the adversary chooses. Public advisories from U.S. agencies have described exactly this inside communications, energy,

water, and transportation networks. The lesson is that the absence of an incident is not the absence of a threat.

Combined arms is the coordinated use of more than one vector in sequence — for example, a cyber attack first, while systems are still powered and operators can be blinded, followed by physical damage that is harder to undo. The practical point is simple: an adversary-caused outage does not behave like a storm. It can hit many sectors at once, strike the systems a community would use to respond, and time a second blow against the recovery.

Why an adversary would do this

A fair question is why a hostile state would attack another country's water plants and substations instead of its army. The answer is that the infrastructure is the way to the army — and to the economy. A modern military cannot deploy, and a modern economy cannot run, without the same civilian power, water, fuel, transportation, and communications everyone else uses. An adversary who cannot match the United States force-on-force can still blunt it: disable the infrastructure a base depends on, and the force on that base is held in place without a shot fired. Do it widely enough, and troops stay home managing a domestic crisis instead of deploying abroad. The same blow strikes the economy, because the economy runs on the same grid.

That is what makes civilian infrastructure the target. It is interconnected, so damage spreads; much of it is lightly defended, because it was built for reliability and low cost rather than for attack; and a great deal of how it works is public. The honest summary is that the exposure is large and, in many places, under-defended. That is not a reason for fear — it is the reason these books exist, and the exposure is the one thing a community can actually change.

Why some places matter more

This is why FIR does not treat every asset as equal. Some are strategic nodes — a military installation, a major port, a refinery, a financial or data hub — whose loss would matter well beyond the local area. A strategic node depends on keystone infrastructure: the specific power feed, water source, fuel line, or communications path it cannot operate without. And that keystone usually concentrates at an anchor site — a particular substation, pump station, or terminal. An adversary studying a strategic node looks for its anchor sites, because taking one can neutralize the node without ever touching the node itself. A defender who maps the same chain — node, to keystone, to anchor site — gets there first and hardens the handful of places that carry the most weight. Finding and prioritizing these chains is exactly what FIR's assessment and tools are built to do.

Threat posture, not prediction

FIR does not forecast dates, and it does not attribute attacks beyond what public sources already say. It reads documented classes and patterns, states exposure honestly, and hardens to break the attack chain earlier. This keeps the work usable and keeps it honest — a briefing built on posture survives scrutiny in a way that a prediction never does.

Chapter 4 — What 30 days without power actually means

The dependency stack says what fails and in what order. This chapter puts that order on a clock. The times below are a planning picture, not a prophecy; the value is in seeing where the hard edges fall.

The first hours

At first, little looks wrong. Backup generators and batteries carry hospitals, emergency operations, and some communications. Traffic signals go dark. Cell towers run on battery, then begin to drop as that battery runs down. Water still flows for a while on stored pressure and gravity. This is the window in which everything still seems recoverable.

The first days

Then the dependencies start to bite. Once pumps lose power, water pressure falls and then fails. Fuel cannot be pumped from station tanks without electricity, so vehicles and generators cannot refill. Stores sell out quickly, and payment systems go down — first cards, then the registers themselves, leaving cash, and then nothing. Refrigerated food and medicine spoil. The households that prepared for 72 hours reach the end of their supplies, and Day 4 is where the unprepared hit the wall.

The first weeks

Sanitation is the quiet crisis. Sewage moves on powered pumps; when they stop, waste backs up, and disease risk climbs in exactly the conditions — no clean water, no refrigeration — that spread it. Generators fall silent as their fuel runs out. And the grid cannot simply be switched back on, because of the mutual dependency deadlock: power needs water and fuel and roads and communications, each of which needs power. Through all of it, the attrition spiral runs in the background — operators leaving their posts to protect their own families, which slows every repair.

Why it doesn't just come back

The single hardest fact of a Black Sky Event is that its end is not scheduled. The components most likely to be destroyed — large power transformers above all — are long-lead items: 18 to 24 months to replace each, and multi-year when many fail at once. A community should plan for an outage measured at minimum in weeks and stressed toward months and beyond, with no certain restoration date to count down to.

Reading the timeline as a planner

The timeline is a tool, not a forecast. Read it to find where an intervention changes the outcome, and to see what a given loss truly costs once the tiers above it are counted. Every day a community crosses depends on the foundation beneath it — people willing to stay, lawful order intact, energy and the lifelines brought back together. Harden those, and the clock runs slower.

Chapter 5 — Your own readiness

The deepest tier in the stack is people, and people go home to households. A ready household keeps its member at their post, which is what lets every tier above it recover. That is why household readiness is treated here as infrastructure, not as a private hobby. Two questions organize it: can you get home, and can your household hold thirty days.

Can you get home

The get-home bag is built for moving through suburban and urban terrain after infrastructure has failed — not a wilderness kit. Target about 25 pounds, and make every item justify its weight in one sentence. Eight categories cover it: water, carried plus a way to filter more; food that is high-calorie, no-cook, and shelf-stable, judged by calories per ounce; shelter such as a bivvy or space blanket, a poncho, and cordage; medical, starting with blister care and personal prescriptions; communications, including a hand-crank AM/FM/NOAA radio, a whistle, and written contacts and rally points; navigation by paper map and compass with a primary and an alternate route; safety items such as a headlamp, a multi-tool, small bills, ID copies, and lawful personal protection; and clothing — broken-in shoes, layers, rain gear, and spare socks.

Plan the route without GPS. Mark a paper map from work to home with a primary and an alternate route, the hazards to avoid (flood zones, industrial sites, high-crime areas, water you cannot cross), and the resource points along the way. Plan for 3 to 10 miles a day on foot. Two truths govern the walk: water is the clock, and feet stop more people than anything else. Match the load to the distance in three nested tiers — 24 hours on your body and in the vehicle, 48 to 72 hours in the get-home bag, and five or more days in a larger expedition bag.

Personal PACE: staying in contact

PACE stands for Primary, Alternate, Contingency, and Emergency — a ranked plan so that losing one way to communicate is not losing all of them. A workable household plan: Primary, the cell phone, text first; Alternate, a landline; Contingency, an FRS or GMRS handheld radio on a channel the family agreed on in advance; Emergency, a physical rally point at a set time; and a Minimum of a hand-crank NOAA radio and a written plan that names the rally point.

Match the layers to the threat. In a storm or a cyber outage, two-way radio outlasts the cell network. Under EMP, expect the repeaters down — fall back to simplex, line-of-sight handhelds and spares stored powered-off in a shielded, Faraday container.

Can your family survive 30 days

Size everything to your actual household, and build the plan around its most vulnerable member. The planning figures are steady: water about 1.5 gallons per person per day, with a minimum of 1 gallon for drinking and hygiene — roughly 180 gallons for a family of four over 30 days — and calories about 2,000 per person per day. Children, nursing mothers, the sick, anyone working hard, and hot weather all raise the need; heat alone can double the water. Store toward the full 30 days, and size a way to produce or treat water to the daily need rather

than trusting storage alone. There are free reserves already in the house: the water heater, the toilet tanks (not the bowls), and the pipes, if you can shut and drain the main safely.

Water, treatment, and sanitation

Match the treatment to what is in the water. Boiling and bleach kill living things only. Filters add capacity — gravity and pump units make many gallons a day, and carbon cuts some chemicals — but only reverse osmosis or distillation reliably removes chemicals and heavy metals. To boil, hold a rolling boil for 1 minute, or 3 minutes above 6,500 feet. To treat with plain, unscented household bleach, read the label for its strength and add 8 drops of 6% or 6 drops of 8.25% per gallon (2 drops per quart), doubled if the water is cloudy or very cold; stir, wait 30 minutes, and a faint chlorine smell should remain. Never use scented, color-safe, or cleaner-added bleach, and remember that neither boiling nor bleach does anything for chemicals — when that is the risk and you cannot distill, find another source.

Sanitation is the step most plans skip, and it is disease prevention. Set up a lined bucket or bowl with a seat and cover material; seal solids and store them away from living and water areas; put a hand-wash station with soap at every toilet point; and decide in advance how the drinking, gray, and black water streams stay separate.

Why this belongs in a foundations book

A household that can hold 30 days keeps its member able to stay at their post, which is the thing the whole recovery depends on. The fuller treatment — the bag in detail, the route, the thirty-day household — is in the Field Handbook's Foundation field cards and in the free courses BSE 101 and BSE 102.

Chapter 6 — Knowing what is true

A planner acts on claims: about the threat, about a community's own systems, about what will work. Source discipline is how you separate what you actually know from what you have merely heard. It is taught before the facts because the facts change, and because a claim that cannot be sourced has no place in a plan or a briefing.

Two standards

Two sentences carry the whole chapter. You have not verified a claim until you can cite its primary source. You have not achieved a capability until you have demonstrated it. The first keeps a briefing honest; the second keeps a readiness score honest.

The five source tiers

Rank every source, treating the rank as a floor rather than a final verdict. Tier 1 is primary — original documents, filings, raw data, sworn testimony — and it is what settles a technical claim. Tier 2 is qualified secondary: experts who cite their own primaries, reliable when the analysis shows its work. Tier 3 is curated aggregation: journalists who cite their sources, best used to find the primary. Tier 4 is general media — what the public is told, never a technical fact. Tier 5 is a government press release — a policy posture, never a technical fact. Motivation, recency, and corroboration then adjust the tier up or down.

Four habits on every claim

Apply four habits to every claim that matters. Cite it, with document, publisher, date, and locator. Read the original, not the summary of the summary. Evaluate the motivation behind the source. And cross-reference for independence — three echoes of one source are still one source.

Read the silence, and label the confidence

Go to the primary feeds directly and read them against a baseline of what should be there; a gap between the two is itself a finding. Then label the confidence of every conclusion plainly: confirmed, when Tier 1 or 2 evidence corroborates; assessed, when the reasoning is sound but the evidence is partial; possible, when it is a hypothesis held open. Labeling confidence is not hedging — it is telling the reader exactly how far the evidence reaches, which is what lets them act on it.

Chapter 7 — Making the case without causing paralysis

The picture in this book alarms people, and alarm cuts both ways. It can move someone to act, or it can freeze them. The difference is almost never the facts. It is how the case is made.

Why alarm backfires

Fear with no next step does not produce action; it produces denial, fatalism, or a quick dismissal — "doomsday talk." Overstated certainty does its own damage: it invites the audience to find the single weak claim and reject the whole case with it. A briefing that frightens and then offers nothing to do has failed, however accurate it was.

The shape of a case that lands

A case that moves people has a predictable shape. Lead with what is at stake in the audience's own terms. State the threat as documented posture, not prophecy. Show enough of the dependency picture that the scale lands. Then, immediately, give a concrete and affordable first step — because the moment of alarm is also the moment the mind looks for an exit, and the first step should be an exit toward action rather than away from the problem. Keep the certainty honest throughout, using the confirmed-assessed-possible labels from the last chapter. Pair every hard fact with something the audience can do, and end on agency rather than doom.

Match the message to the room

A mayor, a utility manager, and a family facing the same event do not share the same stakes or the same first step. The threat posture stays the same; the opening and the ask change to fit the room. What never changes is the honesty: never manufacture certainty to win a decision, because the credibility spent to win it is the credibility needed to keep it.

The short form and the full course

This chapter is the short form. FIR's free companion course, FIR 002 (Making the Case), teaches the method in depth — how to communicate an alarming picture so that people act rather than freeze.

Chapter 8 — How FIR is organized, and where you go next

FIR is organized so that the picture in this book becomes work at every level of government and community. Two things orient a new reader: how the Foundation is organized, and how a reader goes further.

The six lines of effort, in order

FIR works six lines of effort, in a deliberate order. Education and Training comes first, because nothing moves without a shared picture. National Recognition and Organizing builds the demand and the coalition for action. Defense — Force Protection and Mission Assurance —

addresses the military's dependence on the same civilian infrastructure. State Planning and Readiness puts planning at the level where nationwide work actually coordinates. Critical Infrastructure Sectors engages the owners and operators who must harden what they run. Resilient Communities comes last. They can be built independently to merge into a broader regional or national framework, but are built best when coordinated from the blocks the higher levels help prioritize. Also, a local community can act without waiting for or requiring higher coordination. For this reason, much of FIR's training and tooling supports local action.

A resilient community, in FIR's sense, is one that can hold its stack for its own residents and for the neighbors it has agreed in writing to help before the event. It is a network, not a fortress.

How readiness is measured

The method rests on four ideas. Readiness is scored against three vectors — cyber, physical, and EMP/GMD — each on its own, never blended. Each vector earns one of four levels: Bronze, Silver, Gold, or Diamond, with Diamond-N stating the days of supply set by the binding constraint once a vector is hardened. Diamond Blue is the apex, reached only when all three vectors in a declared scope stand at Diamond and the community can demonstrate the ability to operate as a functioning limited society after a Black Sky Event. The work proceeds in seven steps: inventory, target architecture, gap assessment, roadmap and budget, the affordability decision, roadmap refinement, and exercise validation. The Field Handbook carries the full definitions of record.

The courses and credentials

Learning follows the same order. The free Foundation is four short courses — BSE 099, then 101, then 102, then 100 — about 24 hours in all, and it is bundled free with every municipal assessment. Four credentials build from there: CRL, the leadership credential; then CRC, CIRP, and CBRA, the assessor and practitioner ladder that ends at the Diamond Blue assessment. Exam preparation lives inside the courses; this book set is the reference that sits beside them.

Where you go next

If you are a resident, start with your own household — Chapter 5 — and the free member orientation, FIR 001. If you work in government or run infrastructure, your path runs through the dependency stack in Chapter 2 and into the assessment method, which the next books in this set cover: how to assess a community, how to score it, and how to build the roadmap that moves it up the levels.

Everything that follows in the FIR method reads a community from the foundation up. This book is that foundation.

Appendices

The reference material for this book — the glossary of record, the Foundation and course field cards, and the sources — is gathered in the companion *FIR Field Handbook* rather than repeated here, so that one document stays the single source of record. Where this book and the Handbook ever differ on a definition, the Handbook governs; where either differs from the online courses on instruction, the course governs, and the difference should be reported for correction.

Take the next step

This book is a free introduction. To learn the method in full — and to earn FIR's credentials — take the courses, which are the version of record for instruction. From the Foundation, the paid tracks build through the Common Core and the governance and domain courses to the CRL, CRC, CIRP, and CBRA credentials. Whatever your path, the four Foundation courses (BSE 099, 101, 102, and 100) and the free member orientation (FIR 001) are the place to start, and they cost nothing. Browse every course and enroll at the FIR course catalog, and learn more about FIR at fir.foundation.