FREE PREVIEW

PATROL REFERENCE PRESS

CRITICAL INFRASTRUCTURE RECOGNITION

Data Centers

for Law Enforcement & Security Professionals

VOLUME 6

OBSERVE · ASSESS · DECIDE · TEACH

This free preview contains the complete How to Use this Guide and the full first chapter, *Understanding Data Centers*, from the 65-page manual.

First Edition — 2026

patrolreferencepress.com

Free sample — not for resale

About This Free Preview

This preview gives you the complete opening of Critical Infrastructure Recognition: Data Centers (Volume 6) — the How to Use this Guide and the full first chapter, *Understanding Data Centers*. You'll see the guide's real format: the recognition-first field pages, the red-line and officer-note callouts, and the incident-management connection that carry through the full volume. If this preview helps, the full 65-page manual continues with the chapters listed on the closing page.

How to use this guide

A responder rarely gets a convenient label on an unfamiliar facility. You get a generator hum at 3 a.m. with no visible cause, a delivery truck parked at a loading dock that should be closed, a pad-mount transformer buzzing but a building dark, a fuel tank with a man on the catwalk wearing no reflective vest, a manhole cover kicked aside next to a fiber marker, or a row of cooling towers steaming on a hot, dry day. Start with the observation, not the theory. Ask: **What am I looking at? What does it do? Why is it important? What hazards and weather impacts matter? What should I observe, report, or avoid?**

Each entry is a stand-alone field page. The repeated format is deliberate: it builds recognition under stress without asking a patrol officer to become a data-center engineer, an IT architect, or a mission-critical facilities manager. Data-center design, redundancy, voltage classes, cooling architecture, fuel capacity, demarcation ownership, and security staffing vary widely by facility, landlord, operator, and jurisdiction; confirm site-specific details with the operator, the cognizant authority (the AHJ), or a qualified subject-matter expert before publication.

💡 **OFFICER NOTE**

Officer note — the first report: Give dispatch your location; what you can see, hear, or smell; whether anyone is exposed, injured, or trapped; the nature of the building or campus and what appears to be its function; visible signing, fencing, and utility markers readable from a safe position; any unusual power, cooling, fuel, vehicle, or personnel activity; weather and visibility; and the responsible-partner emergency number if posted. Do not breach a fence or perimeter, open a gate, enter a generator or confined-space area, touch any panel, transformer, tank, or cable, or walk toward a structure you cannot confirm is safe. When an immediate law-enforcement, rescue, or life-safety mission requires entry, act according to lawful authority, agency policy, training, incident command, and known hazards; do not manipulate technical equipment unless specifically trained, authorized, and required by the emergency.

Chapter 1 — Understanding Data Centers

Why recognition matters on patrol

A patrol officer is often the first trained observer at a data-center event. A power-flash near a substation, a diesel generator running at an odd hour in a residential zone, a delivery truck at a loading dock that should be closed, a person photographing a pad-mount transformer, a vapor odor downwind of a fuel area, a manhole cover moved near a fiber route, an unexplained network outage that has knocked out 911 or cellular service, or a routine beat check can place you beside the infrastructure that runs a region's digital life. Recognition changes the quality of the first five minutes: it helps you choose a safe position, protect the public, describe the problem accurately, identify the right responsible party — landlord, colocation operator, tenant, or electric/communications utility — and preserve an incident scene without creating a second emergency.

Data centers are the physical homes of the computing and networking systems that carry a community's information: emergency dispatch and records, banking and payments, medical records and hospital systems, utilities' control and billing, cellular and internet backhaul, government services, and the cloud platforms businesses and agencies depend on. When a data center fails — a power outage, a cooling loss that forces an orderly shutdown, a fiber cut, or a breach — the failure ripples beyond the building. A regional fiber cut can take 911 call-taking or a wireless carrier down; a major outage can stop commerce and government for an area. The facility itself rarely "fails" on its own from a patrol perspective; the recognition task is to see the facility as a mission-critical node and to protect it, its people, and the public while the operator, utilities, and specialists work the technical problem.

The five-minute patrol habit

1. **Observe:** Stop short. Scan for people, vehicles, fuel, power, cooling, and network infrastructure, signage, gates, perimeter conditions, and changing activity. Use binoculars rather than trespass; do not breach a fence or enter a restricted area solely to get a closer look. When an immediate law-enforcement, rescue, or life-safety mission requires entry, act according to lawful authority, agency policy, training, incident command, and known hazards.
2. **Assess:** Is there a power, cooling, fuel, or network event; a fire or smoke; an unauthorized person near a sensitive area; a suspicious vehicle at a dock, tank, or transformer; a broken fence or open gate; or an immediate life threat? Are generators running, and is diesel being delivered, off-loaded, or venting? What is the weather doing?
3. **Decide:** Use training, agency policy, and incident command. Request the data-center operator, the electric and communications utilities, and fire/HazMat early when power, fuel, cooling, network, or public exposure is possible.

4. **Teach:** Give a plain-language briefing to incoming responders. Explain what is known, what is uncertain, and what you did not touch, open, approach, or cross.

> 💡 **OFFICER NOTE**
>
> **Photography and observation doctrine:** Photography, videography, note-taking, or observation of a data-center facility may be lawful and commonplace and should not, standing alone, be treated as evidence of criminal, terrorist, or pre-operational activity. Assess the totality of observable behavior and circumstances. Greater concern may be warranted when photography or surveillance is covert or prolonged and is combined with trespass, tampering, attempts to defeat security, concealment, false statements, unusual interest in restricted access points or security systems, threats, or other articulable conduct suggesting unlawful activity. Photography or presence near the facility, standing alone, does not establish criminal intent.

> 💡 **OFFICER NOTE**
>
> **Master rules: THE OFFICER RECOGNIZES. THE OPERATOR DIAGNOSES.** Recognition is the officer's task; diagnosis of the technical condition belongs to the operator and qualified specialists. **DESCRIBE THE CONDITION BEFORE ASSIGNING THE CAUSE OR MOTIVE.** State what you observe before drawing conclusions about cause or intent.

> ⚠️ **PITFALL**
>
> **Red line:** Never treat a quiet site as a safe site. A generator can start automatically and produce deadly exhaust and moving parts with no warning; switchgear, transformers, and panels can be energized at lethal voltages even when a building appears dark; a cooling tower basin or a manhole can conceal deep water, moving machinery, or confined-space atmospheres; and a fuel tank can hold explosive vapor. Calm appearance is not a clearance test — never assume power, fuel, cooling, or mechanical systems are de-energized, isolated, empty, stopped, or safe based on appearance alone.

Federal critical-infrastructure framework

The United States currently organizes critical-infrastructure security and resilience around 16 sectors. Under National Security Memorandum 22 and related federal authorities, CISA serves as the National Coordinator for critical-infrastructure security and resilience and works with Sector Risk Management Agencies, state and local governments, law enforcement, and private owners/operators. The 16 sectors include the **Information Technology Sector**, Communications, Energy, Water and Wastewater Systems, and Emergency Services. Data centers sit at the intersection of the **Information Technology (IT)** and **Communications** sectors: the IT Sector covers computing and network infrastructure that produces, processes, and stores information, while the Communications Sector covers the networks that carry voice,

data, and 911 traffic. In practice a modern data center depends on **Energy** (grid power, generators, and fuel) and is often physically integrated with communications facilities (carrier hotels, internet exchanges, wireless backhaul). This guide treats data centers as the shared, mission-critical node that several sectors depend on. A single data center may support multiple sectors simultaneously — including Information Technology, Communications, Energy, Emergency Services, Financial Services, and Healthcare — so do not classify its role solely from its exterior; confirm actual dependencies with the operator and utility.

The sector model is a coordination framework, not a patrol classification system. Use it to identify partners and consequences. Data centers are overwhelmingly **privately owned and operated** — by enterprises for their own use, by colocation providers renting space to many tenants, by cloud/ hyperscale operators, or by communications carriers hosting exchange and backhaul equipment. There is generally no federal or state regulator that "owns" or operates a data center the way a DOT owns a road, although CISA issues voluntary guidance and the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) matter for communications facilities and public-safety spectrum considerations. Across all of it, the Information Sharing and Analysis Centers (ISACs) and CISA's public guidance provide reference points. The exact facility type, ownership, and dependencies are determination tasks for the on-scene responder, verified by the operator. The specific sector mapping and the facility's live dependencies (IT vs Communications vs Energy vs Water) vary by facility and should be operator-confirmed rather than assumed. Current federal and state guidance must be checked before publication.

Public safety, private security, and the operator: different roles, shared objective

Local law enforcement protects life, establishes lawful control of public space, manages traffic and access, protects people at data-center events, investigates crimes — including trespass, vandalism, theft, sabotage, and terrorism — and preserves evidence. Officers generally do not operate generators, switchgear, UPS systems, cooling plant, or network equipment, and do not direct how the operator restores service.

Private security controls access within the authority granted by the owner — the perimeter, gatehouse, lobby, and security operations center — observes and reports, enforces visitor and contractor procedures, protects employees and assets, and activates the facility emergency plan. Security can confirm the "who" and "where" of the facility faster than almost anyone else; they are a force multiplier, not a replacement for public safety. Security should not physically confront an unknown person near a hazardous or restricted area unless policy and immediate safety require it; preserve distance, notify the control center and public safety, and record objective observations.

The data-center operator, landlord, or colocation provider owns the building and its critical systems and knows its redundancy, fuel capacity, hazards, and emergency procedures. **The electric utility** owns the grid feed and everything beyond the utility point of demarcation (the meter or the utility-owned

transformer); **the communications carriers** own the fiber and circuits up to the demarcation and inside the building provide the actual network services. **Fire/HazMat** may lead or support fire suppression, hazardous-materials response, technical rescue, monitoring, and decontamination according to local authority and the established incident organization. **Emergency management** may coordinate or support resource management, public information, evacuation, continuity, and recovery functions depending on jurisdiction and incident scale. No officer should promise the public that a facility or network is safe, secure, or restored without qualified confirmation.

> 💡 **OFFICER NOTE**
>
> "Who owns this" is not a single answer. It is an **on-scene determination**: a landlord may own the shell and power, a colocation operator may run the data-hall and security, a tenant may own its racks and network gear, and utility ownership is defined by the service point, tariff, and interconnection arrangement — not assumed from the meter. Ask who is the responsible party for the specific thing that is wrong — power, fuel, cooling, network, or physical access — rather than assuming one owner for the whole building. Facility ownership, op-model (single-tenant vs colocation vs carrier hotel), and the utility points of demarcation vary by site.

> ⚠️ **PITFALL**
>
> **RED LINE — TECHNICAL INFRASTRUCTURE IS NOT A PATROL CONTROL:** Electrical and communications ownership, maintenance responsibility, and points of demarcation vary by utility/carrier agreement and facility design. Do not infer ownership from a meter, transformer, fence line, cable-entry point, cabinet, or equipment appearance; identify the responsible party through the operator and utility/carrier rather than assuming it from equipment. Treat electrical infrastructure as hazardous and technically controlled until the data-center operator and electric utility identify the responsible party and confirm system status. Do not open panels, reset breakers, restore power, or touch any energized or possibly-energized component. The person who "flips a breaker" at a data center can take down cooling or servers for an entire campus — and can be hurt or killed doing it.

Incident management connection

Use NIMS/ICS principles even on a small call: establish command, name an incident location in terms both you and the operator can use (building, campus, dock, generator yard, utility vault, tank), identify hazards, set an objective, assign perimeter and traffic functions, and communicate a common operating picture. **Unified command** may be appropriate when multiple jurisdictions, agencies, or organizations have primary authority or functional responsibility for the incident. A private owner/operator may participate when it is a responsible party with an appropriate command role. Organizations providing technical

expertise or resources without command authority may instead coordinate through Liaison or another appropriate ICS function. Document times, weather, power and network status, observations, notifications, and instructions received; these records support later safety reviews and criminal investigations.

> 💡 **OFFICER NOTE**
>
> **Officer note — emergency services dependency:** Data centers carry a surprising share of emergency services traffic — 911 call routing, records, CAD backup, and cellular backhaul can all depend on a single building or a single fiber route. A "routine" network outage call, a downed fiber, or a suspicious cut can be an emergency-services event. Ask dispatch and the operator whether 911, cellular, or other public-safety services are affected and flag it in your report.

Get the Full 65-Page Manual

Chapter 1 framed how to see a data center. The full volume walks the site asset by asset.

- **Chapter 2: Site Anatomy** — the perimeter, gate, loading dock, fuel & generator yard, cooling plant, substation, and signage — each entry on a stand-alone field page.
- **Chapter 3: Power & Cooling Systems** — the power path and the cooling path, UPS & battery, generators, high-voltage red lines, and the thermal event.
- **Chapter 4: Communications & Network Layer** — fiber, ducts & manholes, demarcation, RF backhaul, and the 911 knock-on effect.
- **Chapter 5: Physical Security & Access** — access control, the SOC & cameras, tenant/staff/visitor determination, trespass & insider-threat indicators.
- **Chapter 6: Data-Center Incidents** — power loss, cooling loss, network outage, breach, fire/smoke, flood, and suspicious activity — plus **6 Field Recognition Drills**.
- **Closing Field Card & Comms** — the Observe. Assess. Decide. Teach. card, the dispatch-update template, and the handoff.

$19.99

Instant digital download — carry it on your phone, tablet, or print for your duty bag

GET THE FULL MANUAL

buy.stripe.com — Data Centers (Vol. 6)

Patrol Reference Press — First Edition, 2026

This guide is a recognition and response reference for public safety, security, and emergency-response professionals. It is not an operations manual. Consult your agency's policies and the owning operator/utility for jurisdiction-specific guidance.