Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/ot-state-local-research-companion/

OT STATE AND LOCAL RESEARCH COMPANION

The OT Research Companion, Fifty State Profiles for One Local Decision

Each state profile tells you which authority to read, what the scope question is and what the next facility decision must establish, and your facility's own facts then settle whether the plant is covered. This companion carries those fifty profiles and the local questions each one hands to your team.

State and local research scope

This companion supports the four sector planning packs. It carries a selected authority profile for each of the fifty states and a method for resolving the local and facility specific requirements, which are settled with the facility's own facts alongside the state profile. Read it as a routing document: each profile tells you which authority to read, what the scope question is and what the facility has to establish next.

What the state profiles establish

Each profile identifies the authority reviewed, the relevant scope issue and the next facility decision. Some identify an enacted sector law; others identify guidance, a public entity standard, a proposal or an open question to confirm with the agency, and the classification line says which. Other state provisions may also apply, so each profile is the first source to read and the starting point for a wider search. A state profile opens the facility determination, and the facility record completes it. Each state and sector row in the workbook starts as Unresolved and closes when a responsible person records the facility facts, the exact instrument, the evidence and the reason, and every exemption is recorded from the text that grants it.

Coverage of the Profiles

Every state has a profile with a starting source, and the instruments most likely to change an assessment plan are described in more depth. For Louisiana and Vermont, confirm any sector wide obligation directly with the state agencies. Municipal ordinances, county requirements, tribal authorities, port rules, permits, insurance terms and private agreements are researched facility by facility from a facility list, a footprint, ownership, permits and contracts, and the local jurisdiction sections below show how to do that work. The inventory covers the fifty states requested, and United States territories and the District of Columbia are researched as separate scopes when a facility sits there.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Use with the project workbook

Filter the Applicability sheet by facility state and sector. Copy a screening row for each distinct obligation and keep the source note intact beside the conclusion. Link the Local duties, Evidence, Notifications and Work plan records so the chain from authority to facility decision to evidence can be followed by any later reviewer. Keep the source note and the facility decision in separate fields.

Which of the fifty rows is yours to resolve first? Put the facility and the state in front of a senior examiner and start the record from there.

Indiana and Maryland Water Thresholds

Indiana and Maryland count their water cybersecurity duties differently, and a utility in either state should read these thresholds before it sets a calendar.

Indiana and Maryland

For Indiana, IDEM currently identifies an annual vulnerability assessment, certification by December 31 2026 and every other year thereafter, and annual reporter designation before September 1. Confirm the current IC 13-18-16.5 text, the approved tools, the actual scope and the independent incident triggers before the Indiana row is signed. For Maryland, the current Environment 9-2705 applies to community water and sewerage systems serving over 3,300 customers, with a maturity assessment by July 1 2026 and every two years. Keep the all system contact, training and reporting duties and the state office collection dates separate from the operator's own filing duties. The May 2026 MDE guidance supplies submission instructions, but its Attachment 2 counts people where the statute counts customers.

Preparation workflow

Use the Assessment prep worksheet and its CSV to prepare audits, cyber and physical assessments and penetration tests. Gather the permissions, the third party authority, the OT safety restrictions, the stop and recovery arrangements and the existing evidence before any method is agreed. Assign further state and sector research in the State research checklist, which has one row per state and sector, alongside the local, operator, permit and client facts.

Evidence and implementation

The May 2026 MDE guidance now describes secure MoveIT submission. Its Attachment 2 uses people rather than statutory customers. Record the conflict in the applicability register, confirm current account eligibility and filing instructions with the agency, and close the row with the agency's own answer.

Sources: W04 Cybersecurity for Water and Wastewater Facilities, W05 Maryland Environment 9-2705, current selected codified text, W06 MDE SB871 implementation guidance, May 2026

© 2026 Global Digital Forensics, Inc. All rights reserved.

Applying the Updated Audit Workbook

The workbook works as an execution record. Every procedure row now carries the fields an auditor will read first: the exact criterion tested, the population it was tested against, the period, the sampling rationale, the permitted method, the execution date, the actual observation, the evidence identifiers and the reviewer. A row with those fields completed is a result, a row waiting for them is a plan, and the workbook keeps the two visibly apart.

Before execution

Fill the criterion, population, period and sampling rationale before anyone touches a system, because those four fields decide whether the eventual observation means anything. Record the permitted method exactly as the activity permit states it. When the work is done, enter the execution date, what was actually observed and the evidence identifiers that support it, then hand the row to the named reviewer. Keep the source register and the operating authority record separate from the procedure rows, so each legal citation and each operating approval is read for what it is.

Open and incomplete decisions

The open count on the Start sheet includes blank decisions, invalid decision text and resolved selections awaiting a required record field. Read Fields present as the signal to start qualified review. The approval fields are signed once the responsible operating, technical and compliance people have reviewed the work, and those signatures are what mark a workbook as reviewed as well as filled.

Scope and authority

Record every proposed exclusion, its reason and the responsible reviewer in Scope decisions so deferred work stays visible to the sponsor. The State research sheet is a separately labelled routing register: its state and sector rows are a client research checklist that points to the controlling instrument, and the facility conclusion is drawn from that instrument. For New York work use the Clause matrix and questions Q01 to Q10 in the New York set. A row awaiting a current instrument or a local fact stays Unresolved, and it closes when someone retrieves the text or establishes the fact.

Source access and revision

The Sources sheet lists each source with the date it was reviewed. Request the current text of each source as you come to it, and keep the duty on the register while the text is on its way. Use the Edition record to track your own revisions and reviews, and keep the previous version when you adopt a new one.

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to resolve a state profile

The compliance owner owns the applicability decision. The project manager tracks the evidence and makes sure each legal assumption is resolved before its task is marked complete. The method below is the same for every state, and an auditor will expect to see each of its four records.

Read the actual instrument

Start with the linked authority and obtain the current codified text, the adopted rule, the final order or the issued directive from the official source. Verify legal status, effective date, compliance date, entity definition, system scope, exemptions and incorporated documents. Preserve the copy and the retrieval date in the controlled record, because the text that was read is part of the evidence for the decision.

Prove the facility facts

Establish the legal owner and operator, public or private status, the regulated service, registrations, permits, contracts and the physical and control center footprint. Water population, customer count and service connections need separate evidence because different states count coverage in different units. A federal registration or a grant condition can create a boundary that differs from the state utility franchise, and both are recorded.

Decide and document

Use Applicable, Not applicable with reason, or Unresolved. An applicable record names the work, the frequency, the due date rule, the evidence, the recipient and the authorized official. A nonapplicability record names the exclusion and the facts that satisfy it. An unresolved record names the instrument or fact to be obtained and states how it bears on the assessment. A Not applicable entry carries its stated reason, and that reason is what an auditor reads as the decision.

Recheck changes

Review after an ownership change, a new state footprint, a changed service population, a material process or architecture change, a new contract, an amended rule or a significant incident. Assign a named owner and an event based or dated review.

Record each decision in the project workbook from the OT assessment planning library so the source note and the facility decision travel together.

Records every state profile needs

The profiles below carry only what is specific to each state, so apply these sector records to every one of them. For water and wastewater, establish the PWSID or permit, system type, ownership, population served, customers, service connections, computerized controls and regulator, each with its own evidence, and apply the federal drinking water and wastewater duties alongside the state finding. For power and energy, establish the registered functions, system categorization, utility jurisdiction, public power or cooperative status and any pipeline or nuclear boundary, then obtain the state orders, security filings and incident instructions for each

© 2026 Global Digital Forensics, Inc. All rights reserved.

system. For manufacturing, resolve the process safety, product, environmental, public contract and incident duties; for transportation, resolve the mode, owner, public agency status, federal security instruments and local operating agreements.

Then assign an owner to retrieve the current instrument, document the site facts, identify each duty and exception and record a signed applicability decision. An item stays Unresolved while the controlling text, the enactment, a facility fact or an approval is being obtained, and the workbook records the source, the decision date and the next trigger.

State and sector differences

Use the federal scope and the state instrument together. A state can regulate an entity for a different reason than its federal sector regulator does, and the table names the additional checks that apply to each sector before a state row is closed.

Sector	Additional state and local checks
Water and wastewater	Drinking water primacy agency, wastewater permit authority, public health reporting, utility commission where applicable, public body cyber law and local emergency arrangements. Keep drinking water and wastewater populations separate.
Power and energy	State utility and pipeline jurisdiction, investor owned, municipal or cooperative status, current security and emergency orders, interconnection contracts, public entity policies and the relevant federal system boundaries.
Manufacturing	State plan occupational safety coverage, environmental and discharge permits, chemical emergency arrangements, government contracts, product and quality requirements and personal information duties.
Transportation	Mode and operating authority, state DOT and local ownership, rail transit State Safety Oversight, port and airport agreements, pipeline authority, public body policies and the current issued federal security instruments.

Local jurisdiction work instructions

Create a local record for each facility and each significant remote site. Resolve the overlapping authorities before deciding the notification and operating plan, because the local emergency manager and the permit authority will each expect to have been identified in advance.

Identify the authorities

Confirm the street address, municipality, county, state, tribal jurisdiction if relevant, owner, operator, permit identifiers and emergency response district for each site. Include the local emergency manager, the fire or HazMat authority, the water or sewer authority, the port or airport authority and the relevant transportation or

© 2026 Global Digital Forensics, Inc. All rights reserved.

utility board as each applies. Answer each of these from the site's own address; the corporate headquarters address belongs to a different record.

Identify the controlling record

Review permit conditions, local ordinances, franchise or concession agreements, board policies, leases, procurement requirements, mutual aid agreements, emergency plans and insurer terms. Record whether each is law, permit, adopted policy, contract or voluntary guidance, because the five carry different weight when a finding is challenged.

Connect physical consequences and cyber events

An OT event can require separate cyber, public health, environmental, safety, customer and contractual notices, each on its own clock. Where EPCRA or CERCLA applies, EHS determines the chemical thresholds and the appropriate state, tribal and local emergency recipients. Treat the release decision independently of whether personal data was taken.

Confirm the reporting route in advance

Use the authority's published procedure and, where needed, an authorized clarification clearly framed as a routing inquiry. Record the official role, the verified channel, the after hours route and the alternate. During a real incident follow the applicable reporting duty and preserve the submission receipt.

Sources: F06 State Plans, F07 Emergency Release Notifications under EPCRA

Information needed for local determinations

A location specific local pack is completed from the following inputs. The worksheets in this volume record the decision and its source, and each input below changes the pack in the way the table describes.

Input	Why it changes the pack
Facility and remote site addresses	Identifies the city, county, tribal or other authority and the emergency response district. Each site is placed by its own address, separate from the corporate headquarters.
Owner operator and public body status	Determines public agency cyber duties, utility jurisdiction, board policies and responsibility for filings.
Permits licenses registrations and awards	Identifies required plans, operating conditions, audit or reporting duties and the actual filing official.
Contracts leases and insurance terms	Identifies supplier, landlord, customer, grant, franchise and insurance requirements that sit in private documents outside the public rulebooks.
Operating and information boundaries	Distinguishes IT and OT, process safety, quality records, SSI, CEII and CUI, and cross state dependencies.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Input	Why it changes the pack
Prior reports and approvals	Establishes actual certification dates, existing regulator conditions and recurring cycles rather than estimated dates.

Alabama applicability profile

ADEM encourages periodic water and wastewater cyber assessments. Treat this page as guidance. Separately inspect applicable utility rules, permit conditions and public entity policies.

Authority: ADEM. **Type:** Agency guidance.

Sources: S01 Alabama selected authority

Alaska applicability profile

DEC explains federal AWIA coverage. Confirm the actual PWSID and certification history.

Authority: Alaska DEC. **Type:** Agency guidance.

Sources: S02 Alaska selected authority

Arizona applicability profile

ARS 18-552 concerns investigation and notice of personal information breaches. A SCADA disruption that falls outside the statutory data trigger is assessed under the operational, utility and contractual duties that apply.

Authority: Arizona Legislature. **Type:** Selected enacted law.

Sources: S03 Arizona selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Arkansas applicability profile

An official Act 260 implementation memo identifies public entity and contractor security incident reporting to the Legislative Auditor. Verify the current statute and covered entity definition before using its five business day reference. Private industry OT assessment duties sit outside this memo and are researched under other instruments.

Authority: Arkansas Division of Elementary and Secondary Education. **Type:** Official implementation memo.

Sources: S04 Arkansas selected authority

California applicability profile

Use the CPUC emergency reporting route for covered utilities. Identify applicable general orders and utility specific decisions separately. Municipal utilities, investor owned utilities, ports and state agencies can have different authorities.

Authority: California PUC. **Type:** Regulator reporting page.

Sources: S05 California selected authority

Colorado applicability profile

Selected 4 CCR 723-3 Rule 3539 requires a distribution grid cybersecurity and physical security narrative in the relevant planning context. Verify current rule version, filing scope and utility status. Manufacturing sites are researched under other instruments, because this rule speaks to utility planning.

Authority: Colorado Secretary of State and PUC. **Type:** Selected rule text.

Sources: S06 Colorado selected authority

Connecticut applicability profile

The DPH circular is an older implementation record. Use it to identify water planning and self assessment expectations, then obtain current DPH requests and PURA cyber review instructions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authority: Connecticut DPH. **Type:** Historical agency circular.

Sources: S07 Connecticut selected authority

Delaware applicability profile

The PSC describes annual cybersecurity question and response filings for Class A utilities in DelaFile. Determine classification, filing instructions and corporate coverage.

Authority: Delaware PSC. **Type:** Regulator program.

Sources: S08 Delaware selected authority

Florida applicability profile

Section 282.3185 governs local government cybersecurity and incident reporting. Identify the covered local government and severity/ransomware trigger before populating the clock.

Authority: Florida Senate. **Type:** Selected enacted law.

Sources: S09 Florida selected authority

Georgia applicability profile

The GTA reporting page identifies public agency and utility reporting routes and references HB156. Obtain current statutory text and determine whether a federal report or public entity status triggers the particular state duty.

Authority: Georgia Technology Authority. **Type:** Agency reporting source.

Sources: S10 Georgia selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Hawaii applicability profile

Use the PUC statute and order library to identify the regulated electric or gas entity. County water systems and transportation operators require their own agency and board policy review. Assessment intervals are confirmed entity by entity from the applicable order or policy.

Authority: Hawaii PUC. **Type:** Regulator directory.

Sources: S11 Hawaii selected authority

Idaho applicability profile

ITS Information Security Policy Manual version 4.0 was current when reviewed on October 17, 2026. It sets policy for the state agencies it covers, so confirm operative adoption and actual agency coverage. Private facilities require separate statutory, permit and contract review.

Authority: Idaho Technology Authority. Official policy text; confirm adoption and coverage for the facility.

Sources: S12 Idaho ITS Information Security Policy Manual, version 4.0

Illinois applicability profile

HB3576 describes proposed water cybersecurity duties. Confirm enactment and the effective date with the legislature before applying it. Keep it on the watchlist and treat its proposed deadlines as mandatory once an enacted Public Act is confirmed.

Authority: Illinois General Assembly. **Type:** Bill status unresolved.

Sources: S13 Illinois selected authority

Indiana applicability profile

IDEM currently identifies annual vulnerability assessment, certification by December 31 2026 and every other year, and annual reporter designation before September 1. Confirm current IC 13-18-16.5, approved tools, actual scope and independent incident triggers.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authority: IDEM. **Type:** Agency implementation guidance.

Sources: S14 Indiana selected authority

Iowa applicability profile

The adopted Chapter 21 source addresses covered water, sanitary sewage and storm water utilities. Determine service and ownership coverage and current chapter text. OT cyber audit duties for the utility are researched in its own orders and permits beyond this source.

Authority: Iowa Utilities Commission. **Type:** Selected utility rule.

Sources: S15 Iowa selected authority

Kansas applicability profile

KSA 75-7244 concerns cyber incident reporting by defined public entities and government contractors. Resolve the statutory definitions and current reporting instructions.

Authority: Kansas Legislature. **Type:** Selected enacted law.

Sources: S16 Kansas selected authority

Kentucky applicability profile

Determine PSC jurisdiction, applicable 807 KAR service rules and incident instructions. Site orders and public entity policies are the next records to check.

Authority: Kentucky PSC. **Type:** Regulator reporting page.

Sources: S17 Kentucky selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Louisiana applicability profile

Obtain current utility, water, incident reporting and public agency instruments for the named facility. Search results centered on insurance licensee cybersecurity law, which was set aside as a basis for industrial obligations. Sector specific state requirements are confirmed directly with the state agency.

Authority: Louisiana Legislature. **Type:** Confirm with the state agency.

Sources: S18 Louisiana selected authority

Maine applicability profile

Title 35-A section 710 governs utility accident investigation and reporting. Determine whether the physical consequence meets the trigger. Personal data breach and public agency incident duties require separate review.

Authority: Maine Legislature. **Type:** Selected enacted law.

Sources: S19 Maine selected authority

Maryland applicability profile

Current Environment 9-2705 applies to community water/sewerage systems serving over 3,300 customers; maturity assessment by July 1 2026 and every two years. Separate all system contact/training/reporting duties and state office collection dates. May 2026 MDE guidance supplies submission instructions but its Attachment 2 uses people instead of statutory customers; obtain clarification and keep the statutory unit of customers.

Authority: Maryland General Assembly and MDE. **Type:** Enacted sector law.

Sources: S20 Maryland Environment 9-2705, current selected codified text, W06 MDE SB871 implementation guidance, May 2026

© 2026 Global Digital Forensics, Inc. All rights reserved.

Massachusetts applicability profile

MassDEP publishes cybersecurity assessment resources and sanitary survey inspection notices. Obtain the current facility specific request and controlling state authority before deciding mandatory scope or frequency. A current federal duty is confirmed from current instruments, with older EPA survey policies read as background.

Authority: MassDEP. **Type:** Agency program with scope review.

Sources: S21 Massachusetts selected authority

Michigan applicability profile

MPSC incident instructions and electric technical standards provide distinct utility reporting and security review paths. Confirm utility classification, the current R 460.3205 text and event thresholds.

Authority: Michigan PSC. **Type:** Regulator implementation source.

Sources: S22 Michigan selected authority

Minnesota applicability profile

MDH requests annual assessment and completion certification for public water systems using OT. Its form says before July 1; its page says by July 1. Obtain current instructions and receipts; retain assessment findings securely. EO 22-20 paragraph 3(d) directs agencies to require or encourage annual certification within existing authority. EO 24-07 amends the agency definition.

Authority: Minnesota Department of Health. Agency process and executive order; confirm coverage for the facility.

Sources: S23 Minnesota selected authority, S23E Minnesota Executive Order 22-20, S23A Minnesota Executive Order 24-07, S23C Minnesota annual cyber assessment certification form

© 2026 Global Digital Forensics, Inc. All rights reserved.

Mississippi applicability profile

ITS identifies state agency incident reporting requirements under the enterprise security program and state law. Determine whether a public operator is within that scope. Private sector utility and plant duties require separate instruments.

Authority: Mississippi ITS. **Type:** Agency reporting source.

Sources: S24 Mississippi selected authority

Missouri applicability profile

Section 640.142 requires a cyber risk plan including assessments and controls. Exemptions include systems without internet connected controls; state parks; cities above 30,000 inhabitants; specified charter county population bands; and PSC regulated utilities above 30,000 customers. Document every exclusion and actual entity facts.

Authority: Missouri Legislature. Codified sector clause; confirm the exclusions for the facility.

Sources: S25 Missouri selected authority

Montana applicability profile

State guidance identifies a reporting route for large local government incidents on SummitNet. Connection and government status matter.

Authority: Montana Department of Administration. **Type:** Agency guidance.

Sources: S26 Montana selected authority

Nebraska applicability profile

Determine whether NITC standards apply to the actual public entity or adopted board policy. Review utility, water and public contract instruments separately.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authority: Nebraska Information Technology Commission. **Type:** Standards directory.

Sources: S27 Nebraska selected authority

Nevada applicability profile

NRS 480 addresses political subdivision cybersecurity incident response planning. The selected NAC 480 implementation material also identifies incident reporting. Obtain current codified sections and scope before fixing a clock. Utility safety and personal data duties remain separate.

Authority: Nevada Legislature. **Type:** Selected enacted law.

Sources: S28 Nevada selected authority

New Hampshire applicability profile

RSA 485:3-e and 485-A:5-f establish water and wastewater cyber program duties with Internet connected control exemptions. Read each enacted section separately and obtain implementing rules. Electric utility cyber plans require a separate current rule check.

Authority: New Hampshire Legislature. **Type:** Enacted sector law.

Sources: S29 New Hampshire selected authority, NH-WW Wastewater cybersecurity protection program

New Jersey applicability profile

For WQAA scope, use more than 500 service connections, the WQAA measure, in place of AWIA population. Annual controls assessment and certification, program maintenance and incident duties must be mapped to WQAA and any BPU order. The broader 2023 incident reporting law needs its own scope review.

Authority: New Jersey DEP and Legislature. **Type:** Enacted sector framework.

Sources: S30 New Jersey selected authority, W08 Water cybersecurity amendments

© 2026 Global Digital Forensics, Inc. All rights reserved.

New Mexico applicability profile

The DoIT library identifies agency IT policy and incident standards. Obtain the current Cybersecurity Act, implementing rules and public body definitions.

Authority: New Mexico DoIT. **Type:** Policy directory and scope review.

Sources: S31 New Mexico selected authority

New York applicability profile

Separate DOH drinking water requirements, DEC SPDES incident duties and POTW controls, and PSC utility IT rules. DEC identifies a 24 hour initial and 30 day second incident report for SPDES permittees. POTW controls and initial certification have distinct March 2027 dates.

Authority: New York DEC and DOH. **Type:** Adopted sector rules.

Sources: S32 New York selected authority, W09 New York drinking water cybersecurity applicability

North Carolina applicability profile

State and local government cyber incident reporting must be checked against current GS 143B-1379 and reporting instructions. A municipal operator can be covered because of government status. Private operators are assessed through sector or contract triggers.

Authority: North Carolina DIT. **Type:** Agency implementation guidance.

Sources: S33 North Carolina selected authority

North Dakota applicability profile

Chapter 54-59.1 addresses cyber incident reporting and coordinated response. Resolve covered public entities and current instructions. Electric reliability planning and private entity duties require separate utility instruments.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authority: North Dakota Legislature. **Type:** Selected enacted law.

Sources: S34 North Dakota selected authority

Ohio applicability profile

OAC 3745-81-31 addresses public water reporting, including facts affecting safe operations. Determine the relevant incident trigger. Ohio EPA cyber guidance and PUCO electric standards must be scoped separately; insurance licensee rules apply to insurance licensees and are set aside for this industrial analysis.

Authority: Ohio EPA. **Type:** Selected operational reporting rule.

Sources: S35 Ohio selected authority

Oklahoma applicability profile

OMES identifies statutory and regulatory IT reporting for state agencies. Resolve government status and the applicable standard. OCC utility rules, water permits and private entity contractual duties remain facility specific.

Authority: Oklahoma OMES. **Type:** Agency reporting directory.

Sources: S36 Oklahoma selected authority

Oregon applicability profile

ORS 276A and state cyber security services define government IT responsibilities. Identify the covered body and contract. ODOT technical requirements can bind a specific transportation procurement, and they reach the operators party to that procurement.

Authority: Oregon Legislature. **Type:** Selected enacted law.

Sources: S37 Oregon selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Pennsylvania applicability profile

DEP provides water cybersecurity guidance. The 2025 PUC supplemental advance notice proposed changes including Chapter 104 incident reporting; confirm whether a final rule has been adopted before applying it. Retrieve current utility orders and any final adoption.

Authority: Pennsylvania DEP and PUC. **Type:** Guidance and rulemaking watchlist.

Sources: S38 Pennsylvania selected authority

Rhode Island applicability profile

Section 39-2-26 addresses investor owned electric and gas emergency response planning. Determine whether cyber loss scenarios need integration into that plan and inspect current PUC standards. Its reach is investor owned electric and gas utilities, so a manufacturing site looks to other instruments for cyber audit duties.

Authority: Rhode Island Legislature. **Type:** Selected utility law.

Sources: S39 Rhode Island selected authority

South Carolina applicability profile

DES water cybersecurity materials provide practical guidance. Confirm any inspection or permit specific requirements. Insurance licensee cybersecurity duties were excluded as a basis for water, manufacturing or transportation obligations.

Authority: South Carolina DES. **Type:** Agency guidance.

Sources: S40 South Carolina selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

South Dakota applicability profile

The selected law criminalizes interference with critical infrastructure. Obtain the PUC, environmental, public entity and contract instruments, which are where the research looks for periodic operator assessment and other affirmative duties.

Authority: South Dakota Legislature. **Type:** Criminal statute only.

Sources: S41 South Dakota selected authority

Tennessee applicability profile

TPUC Docket 26-00047 documents 2026 annual confidential utility cybersecurity filings, including water, wastewater and gas providers. This corroborates current implementation, and the scope exceptions, July 1 deadline and incident clocks are read from the current codified chapter 1220-04-15, obtained from the Tennessee Secretary of State.

Authority: Tennessee Secretary of State. Current 2026 filing practice; obtain the rule text.

Sources: S42 Tennessee selected authority, TN-DOCKET Annual utility cybersecurity plan reports, S42D 2026 annual utility cybersecurity filing docket 26-00047

Texas applicability profile

The December 26, 2025 Texas Register adopts amended 16 TAC 25.53 effective January 1, 2026. Prepare applicable cyber and physical security annexes, annual March 15 updates with full refiling at least every three calendar years, secure unredacted delivery, affidavit/training records and annual drill evidence including the activation exception. Apply the specific electric entity and facility scope; the rule addresses emergency operations planning, and penetration testing is scoped under other instruments where they apply. Reconcile the current codified text and any later amendments.

Authority: Texas Legislature. Adopted electric EOP rule; check for later amendments.

Sources: S43 Texas selected authority, S43E Adopted electric emergency operations plan rule

© 2026 Global Digital Forensics, Inc. All rights reserved.

Utah applicability profile

DEQ provides a water and wastewater cyber plan route. Determine whether individual items are guidance, permit conditions or adopted requirements. Utah government IT rules apply within their own scope, so a privately operated plant is checked against that scope before they are applied.

Authority: Utah DEQ. **Type:** Agency guidance.

Sources: S44 Utah selected authority

Vermont applicability profile

Sector wide OT assessment duties are the open research question here, so retrieve current PUC electric and gas rules, water requirements and any public entity cyber law for the facility. Treat a bill as enacted once it has passed both chambers and become law.

Authority: Vermont Legislature. **Type:** Confirm with the state agency.

Sources: S45 Vermont selected authority

Virginia applicability profile

Section 32.1-174.5 and 12 VAC 5-590-570 identify water contaminant release and equipment malfunction reporting. Determine physical and public health consequences independently of personal data breach analysis. State agency IT policies require a separate scope decision.

Authority: Virginia Legislature. **Type:** Selected enacted operational law.

Sources: S46 Virginia selected authority

Washington applicability profile

RCW 43.105.470 addresses major state agency cyber incidents under agency policy. Resolve entity coverage. DOH water guidance, utility tariffs and local public utility policies can create other assessment or reporting expectations.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authority: Washington Legislature. **Type:** Selected enacted agency law.

Sources: S47 Washington selected authority

West Virginia applicability profile

The codified cybersecurity program section addresses agency risk assessments. The separate cyber incident reporting chapter 15-5C and current definitions must also be checked. A private operator's coverage turns on those definitions and its own status, and operating critical infrastructure is one fact among them.

Authority: West Virginia Legislature. **Type:** Selected enacted agency law.

Sources: S48 West Virginia selected authority

Wisconsin applicability profile

DNR provides water cybersecurity resources. Use the actual PWS and utility authority to determine obligations.

Authority: Wisconsin DNR. **Type:** Agency guidance.

Sources: S49 Wisconsin selected authority

Wyoming applicability profile

ETS security and risk assessment standards require an agency scope decision. PSC jurisdiction and current water or electric orders must be reviewed separately.

Authority: Wyoming ETS and PSC. **Type:** Standards directory.

Sources: S50 Wyoming selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Local duty and contact worksheet

Complete this worksheet for a named facility. A completed form is the evidence that local requirements were reviewed, and the auditor will ask for the verified contact behind every row.

Working record fields

Facility address owner operator municipality county and other jurisdiction

Authority regulator emergency role and official source

Law permit policy contract version section and evidence ID

Duty applicability trigger deadline rule and exceptions

Verified recipient channel after hours route and authorized reporter

Compliance decision unresolved facts approval date and next review

Incident notification decision worksheet

Record concurrent duties separately, each with its own definition and clock. The clock starts at awareness.

Working record fields

Event facts process consequence awareness time and timezone

Applicable instrument and exact triggering definition

Clock start deadline calculation calendar or business days and source

Recipient approved channel responsible official and alternate

Initial facts submission time receipt and required follow up

Open questions decision owner and escalation record

Sources F01 to S01, federal guidance and state authorities

F01 Guide to Operational Technology Security Revision 3

NIST. Final guidance. September 2023 final publication; chapters 4 through 6 and OT control tailoring.

© 2026 Global Digital Forensics, Inc. All rights reserved.

F03 Technical Guide to Information Security Testing and Assessment

NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints.

F06 State Plans

OSHA. Jurisdiction directory. State and federal occupational safety jurisdiction. Check public employee coverage and industry exceptions for the actual workplace.

F07 Emergency Release Notifications under EPCRA

EPA. Agency guidance. EPCRA 304 and CERCLA release notification. Chemical thresholds, release facts and recipients require a separate EHS determination.

S01 Alabama selected authority

ADEM. Agency guidance.

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, F06 State Plans, F07 Emergency Release Notifications under EPCRA, S01 Alabama selected authority

---

Sources S02 to S06, state authorities

S02 Alaska selected authority

Alaska DEC. Agency guidance.

S03 Arizona selected authority

Arizona Legislature. Selected enacted law.

S04 Arkansas selected authority

Arkansas Division of Elementary and Secondary Education. Official implementation memo.

S05 California selected authority

California PUC. Regulator reporting page.

S06 Colorado selected authority

Colorado Secretary of State and PUC. Selected rule text.

Sources: S02 Alaska selected authority, S03 Arizona selected authority, S04 Arkansas selected authority, S05 California selected authority, S06 Colorado selected authority

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources S07 to S11, state authorities

S07 Connecticut selected authority

Connecticut DPH. Historical agency circular.

S08 Delaware selected authority

Delaware PSC. Regulator program.

S09 Florida selected authority

Florida Senate. Selected enacted law.

S10 Georgia selected authority

Georgia Technology Authority. Agency reporting source.

S11 Hawaii selected authority

Hawaii PUC. Regulator directory.

Sources: S07 Connecticut selected authority, S08 Delaware selected authority, S09 Florida selected authority, S10 Georgia selected authority, S11 Hawaii selected authority

Sources S12 to S16, state authorities

S12 Idaho ITS Information Security Policy Manual, version 4.0

Idaho Technology Authority. Official agency policy manual. Incident Response IR-06; establish actual agency and system scope. Replaces the S6010 link as the selected research route. Verify current operative adoption and entity scope. Binds by agency and system scope; private facilities are checked separately.

S13 Illinois selected authority

Illinois General Assembly. Bill status unresolved.

S14 Indiana selected authority

IDEM. Agency implementation guidance.

S15 Iowa selected authority

Iowa Utilities Commission. Selected utility rule.

© 2026 Global Digital Forensics, Inc. All rights reserved.

S16 Kansas selected authority

Kansas Legislature. Selected enacted law.

Sources: S12 Idaho ITS Information Security Policy Manual, version 4.0, S13 Illinois selected authority, S14 Indiana selected authority, S15 Iowa selected authority, S16 Kansas selected authority

---

Sources S17 to W06, water and wastewater instruments and state authorities

S17 Kentucky selected authority

Kentucky PSC. Regulator reporting page.

S18 Louisiana selected authority

Louisiana Legislature. Confirm with the state agency.

S19 Maine selected authority

Maine Legislature. Selected enacted law.

S20 Maryland selected authority

Maryland General Assembly and MDE. Enacted sector law.

W06 Guidance on Senate Bill 871

Maryland MDE. May 2026 SB871 implementation guidance, sections 3-9 and Attachments 1-2. Secure submission instructions now exist. Attachment 2 uses people instead of statutory customers; current provider timing and scope require clarification.

Sources: S17 Kentucky selected authority, S18 Louisiana selected authority, S19 Maine selected authority, S20 Maryland Environment 9-2705, current selected codified text, W06 MDE SB871 implementation guidance, May 2026

Sources S21 to S25, state authorities

S21 Massachusetts selected authority

MassDEP. Agency program with scope review.

© 2026 Global Digital Forensics, Inc. All rights reserved.

S22 Michigan selected authority

Michigan PSC. Regulator implementation source.

S23 Minnesota selected authority

Minnesota Department of Health. Agency expectation needing confirmation.

S24 Mississippi selected authority

Mississippi ITS. Agency reporting source.

S25 Missouri selected authority

Missouri Legislature. Selected enacted sector law.

Sources: S21 Massachusetts selected authority, S22 Michigan selected authority, S23 Minnesota selected authority, S24 Mississippi selected authority, S25 Missouri selected authority

---

Sources S26 to S29, state authorities

S26 Montana selected authority

Montana Department of Administration. Agency guidance.

S27 Nebraska selected authority

Nebraska Information Technology Commission. Standards directory.

S28 Nevada selected authority

Nevada Legislature. Selected enacted law.

S29 New Hampshire selected authority

New Hampshire Legislature. Enacted sector law.

NH-WW Wastewater cybersecurity protection program

New Hampshire Legislature. Enacted sector law. RSA 485-A:5-f; current codified text.

Sources: S26 Montana selected authority, S27 Nebraska selected authority, S28 Nevada selected authority, S29 New Hampshire selected authority, NH-WW Wastewater cybersecurity protection program

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources S30 to W09, water and wastewater instruments and state authorities

S30 New Jersey selected authority

New Jersey DEP and Legislature. Enacted sector framework.

W08 Water cybersecurity amendments

New Jersey Legislature. Enacted chapter law. P.L. 2021, c. 262 and N.J.S.A. 58:31-4.1.

S31 New Mexico selected authority

New Mexico DoIT. Policy directory and scope review.

S32 New York selected authority

New York DEC and DOH. Adopted sector rules.

W09 New York drinking water cybersecurity applicability

New York DOH. Current rule page. 10 NYCRR Appendix 5-E.1; Subpart 5-1.33. The January 1 2027 transition and immediate training/reporting exceptions appear in the Department of Health rule summary; obtain the full rule text before facility signoff.

Sources: S30 New Jersey selected authority, W08 Water cybersecurity amendments, S31 New Mexico selected authority, S32 New York selected authority, W09 New York drinking water cybersecurity applicability

Sources S33 to S37, state authorities

S33 North Carolina selected authority

North Carolina DIT. Agency implementation guidance.

S34 North Dakota selected authority

North Dakota Legislature. Selected enacted law.

S35 Ohio selected authority

Ohio EPA. Selected operational reporting rule.

S36 Oklahoma selected authority

Oklahoma OMES. Agency reporting directory.

© 2026 Global Digital Forensics, Inc. All rights reserved.

S37 Oregon selected authority

Oregon Legislature. Selected enacted law.

Sources: S33 North Carolina selected authority, S34 North Dakota selected authority, S35 Ohio selected authority, S36 Oklahoma selected authority, S37 Oregon selected authority

---

Sources S38 to S42, state authorities

S38 Pennsylvania selected authority

Pennsylvania DEP and PUC. Guidance and rulemaking watchlist.

S39 Rhode Island selected authority

Rhode Island Legislature. Selected utility law.

S40 South Carolina selected authority

South Carolina DES. Agency guidance.

S41 South Dakota selected authority

South Dakota Legislature. Criminal statute only.

S42 Tennessee selected authority

Tennessee Secretary of State. Filed utility rule.

Sources: S38 Pennsylvania selected authority, S39 Rhode Island selected authority, S40 South Carolina selected authority, S41 South Dakota selected authority, S42 Tennessee selected authority

---

Sources S43 to S46, state authorities

TN-DOCKET Annual utility cybersecurity plan reports

Tennessee PUC. Implementation docket. 2025 annual utility filing docket under TCA 65-4-127. Individual reports are confidential.

S43 Texas selected authority

Texas Legislature. Selected enacted utility law.

© 2026 Global Digital Forensics, Inc. All rights reserved.

S44 Utah selected authority

Utah DEQ. Agency guidance.

S45 Vermont selected authority

Vermont Legislature. Confirm with the state agency.

S46 Virginia selected authority

Virginia Legislature. Selected enacted operational law.

Sources: TN-DOCKET Annual utility cybersecurity plan reports, S43 Texas selected authority, S44 Utah selected authority, S45 Vermont selected authority, S46 Virginia selected authority

---

Sources S47 to S50, state authorities

S47 Washington selected authority

Washington Legislature. Selected enacted agency law.

S48 West Virginia selected authority

West Virginia Legislature. Selected enacted agency law.

S49 Wisconsin selected authority

Wisconsin DNR. Agency guidance.

S50 Wyoming selected authority

Wyoming ETS and PSC. Standards directory.

Sources: S47 Washington selected authority, S48 West Virginia selected authority, S49 Wisconsin selected authority, S50 Wyoming selected authority

---

October 17 follow up sources

S23E Minnesota Executive Order 22-20

Minnesota Governor. Executive order. Paragraphs 1 and 3; agency action within existing authority. Read together with EO 24-07; confirm operator specific authority and current agency implementation.

© 2026 Global Digital Forensics, Inc. All rights reserved.

S23A Minnesota Executive Order 24-07

Minnesota Legislative Reference Library. Amending executive order. Paragraphs 4 and 8. Amends agency definition.

S23C Minnesota annual cyber assessment certification form

Minnesota Department of Health. Agency implementation form. September 2024 form; annual certification before July 1. Page uses by July 1 while form says before July 1; current instructions and actual authority/applicability require review.

S42D 2026 annual utility cybersecurity filing docket 26-00047

Tennessee Public Utility Commission. Current filing implementation record. 2026 annual confidential reports. The docket shows how the rule is being implemented; read it with the codified rule for deadlines and coverage.

S43E Adopted electric emergency operations plan rule

Texas Secretary of State. Adopted rule text. 16 TAC 25.53; TRD-202504607; effective January 1, 2026. Reconcile later amendments and current codification. Apply electric entity, facility and activation exceptions. Emergency operations planning rule; penetration testing is scoped separately.

Sources: S23E Minnesota Executive Order 22-20, S23A Minnesota Executive Order 24-07, S23C Minnesota annual cyber assessment certification form, S42D 2026 annual utility cybersecurity filing docket 26-00047, S43E Adopted electric emergency operations plan rule

---

When a Profile Says Unresolved, Call an Examiner to Close It

Most facilities will start with several rows marked Unresolved, and each one closes with facts: the legal owner and operator, the permits, the service population, the control center footprint and the controlling instrument in its current form. Those facts live with your facility, and the determination belongs to your compliance owner and counsel.

Global Digital Forensics has served counsel and businesses since 1992. Our court tested and certified examiners help an operator assemble those facts, trace the IT and OT dependencies a determination turns on, and prepare the notification and evidence records a local authority or regulator will ask for after an event. Discuss a state or facility determination or call (800) 868-8189. The first consultation is free. The sector manuals and the workbook are in the OT assessment planning library, and the questions to settle before field work are in OT questions to settle first.

Web Addresses for the Sources Cited

1. W04 Cybersecurity for Water and Wastewater Facilities: https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/

© 2026 Global Digital Forensics, Inc. All rights reserved.

2. W05 Maryland Environment 9-2705, current selected codified text: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2705&enactments=false
3. W06 MDE SB871 implementation guidance, May 2026: https://mde.maryland.gov/programs/water/water_supply/Documents/SB871.pdf
4. F01 Guide to Operational Technology Security Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final
5. F03 Technical Guide to Information Security Testing and Assessment: https://csrc.nist.gov/pubs/sp/800/115/final
6. F06 State Plans: https://www.osha.gov/stateplans/
7. F07 Emergency Release Notifications under EPCRA: https://www.epa.gov/epcra/epcra-emergency-release-notifications
8. S01 Alabama selected authority: https://adem.alabama.gov/water/drinking-water-branch/information-public-water-systems/cybersecurity-resources-public-water-systems
9. S02 Alaska selected authority: https://dec.alaska.gov/eh/dw/security/regulations/awia-regulations
10. S03 Arizona selected authority: https://azleg.gov/ars/18/00552.htm
11. S04 Arkansas selected authority: https://adecm.ade.arkansas.gov/ViewApprovedMemo.aspx?Id=4848
12. S05 California selected authority: https://webproda.cpuc.ca.gov/regulatory-services/safety/emergency-reporting
13. S06 Colorado selected authority: https://www.sos.state.co.us/CCR/GenerateRulePdf.do?fileName=4+CCR+723-3&ruleVersionId=10399
14. S07 Connecticut selected authority: https://portal.ct.gov/dph/-/media/departments-and-agencies/dph/dph/drinking_water/pdf/circular_letter-2021-89_erp_and_cybersecurity_self_assessment_12012021.pdf
15. S08 Delaware selected authority: https://depsc.delaware.gov/cybersecurity/
16. S09 Florida selected authority: https://www.flsenate.gov/Laws/Statutes/2026/282.3185
17. S10 Georgia selected authority: https://gta.georgia.gov/contact-us/cybersecurity-incidents
18. S11 Hawaii selected authority: https://puc.hawaii.gov/about/statutes-rules-orders/
19. S12 Idaho ITS Information Security Policy Manual, version 4.0: https://its.idaho.gov/wp-content/uploads/2025/10/2025-ITS-Information-Security-Policy-Manual-4.0.FINAL_.pdf
20. S13 Illinois selected authority: https://www.ilga.gov/Legislation/BillStatus?DocNum=3576&DocTypeID=HB&GAID=18&LegId=0&Print=1&SessionID=114
21. S15 Iowa selected authority: https://rules.iowa.gov/Notice/Details/8846C
22. S16 Kansas selected authority: https://kslegislature.gov/b2023_24/laws/075_000_0000_chapter/075_072_0000_article/075_072_0044_section/075_072_0044_k/
23. S17 Kentucky selected authority: https://psc.ky.gov/Home/UtilForms
24. S18 Louisiana selected authority: https://legis.la.gov/
25. S19 Maine selected authority: https://www.legislature.maine.gov/legis/statutes/35-A/title35-Asec710.html
26. S21 Massachusetts selected authority: https://www.mass.gov/info-details/public-drinking-water-system-operations
27. S22 Michigan selected authority: https://www.michigan.gov/mpsc/regulatory/emergency-management/utility-incident-notification-procedures
28. S23 Minnesota selected authority: https://www.health.mn.gov/communities/environment/emergency/water/securityassess.html
29. S23E Minnesota Executive Order 22-20: https://mn.gov/governor/assets/EO%2022-20_tcm1055-539386.pdf
30. S23A Minnesota Executive Order 24-07: https://www.lrl.mn.gov/archive/execorders/24-07.pdf
31. S23C Minnesota annual cyber assessment certification form: https://www.health.mn.gov/communities/environment/water/docs/cyberform.pdf
32. S24 Mississippi selected authority: https://www.its.ms.gov/services/security/Enterprise-Cybersecurity-Incident-Reporting
33. S25 Missouri selected authority: https://revisor.mo.gov/main/OneSection.aspx?section=640.142
34. S26 Montana selected authority: https://doa.mt.gov/SITSD/cybersecurity
35. S27 Nebraska selected authority: https://nitc.nebraska.gov/standards-and-guidelines/
36. S28 Nevada selected authority: https://www.leg.state.nv.us/nrs/nrs-480.html
37. S29 New Hampshire selected authority: https://gc.nh.gov/rsa/html/L/485/485-3-e.htm
38. NH-WW Wastewater cybersecurity protection program: https://www.gc.nh.gov/rsa/html/L/485-A/485-A-5-f.htm

© 2026 Global Digital Forensics, Inc. All rights reserved.

39. S30 New Jersey selected authority: https://dep.nj.gov/watersupply/drinking-water-systems/water-quality-accountability-act/
40. W08 Water cybersecurity amendments: https://www.nj.gov/dep/watersupply/pdf/water-cybersecurity.pdf
41. S31 New Mexico selected authority: https://www.doit.nm.gov/about/doit-act-policies-and-rules
42. S32 New York selected authority: https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources
43. W09 New York drinking water cybersecurity applicability: https://regs.health.ny.gov/content/section-5-e1-applicability
44. S33 North Carolina selected authority: https://it.nc.gov/programs/cybersecurity-risk-management/cyber-incident-reporting
45. S34 North Dakota selected authority: https://ndlegis.gov/cencode/t54c59-1.pdf
46. S35 Ohio selected authority: https://codes.ohio.gov/ohio-administrative-code/rule-3745-81-31
47. S36 Oklahoma selected authority: https://www.oklahoma.gov/omes/divisions/information-services/about-information-services/it-statutory-and-regulatory-reporting.html
48. S37 Oregon selected authority: https://www.oregonlegislature.gov/bills_laws/ors/ors276a.html
49. S38 Pennsylvania selected authority: https://www.pa.gov/agencies/dep/programs-and-services/water/bureau-of-safe-drinking-water/cybersecurity
50. S39 Rhode Island selected authority: https://webserver.rilegislature.gov/statutes/title39/39-2/39-2-26.htm
51. S40 South Carolina selected authority: https://www.des.sc.gov/programs/bureau-water/water-utilities-cybersecurity
52. S41 South Dakota selected authority: https://sdlegislature.gov/Statutes/22-34-28
53. S42 Tennessee selected authority: https://publications.tnsosfiles.com/rules_filings/06-31-23.pdf
54. TN-DOCKET Annual utility cybersecurity plan reports: https://tpucdockets.tn.gov/dockets/2500042.htm
55. S42D 2026 annual utility cybersecurity filing docket 26-00047: https://tpucdockets.tn.gov/dockets/2600047.htm
56. S43 Texas selected authority: https://tcss.legis.texas.gov/resources/UT/htm/UT.39.htm
57. S43E Adopted electric emergency operations plan rule: https://www.sos.state.tx.us/texreg/archive/December262025/Adopted%20Rules/16.ECONOMIC%20REGULATION.html
58. S44 Utah selected authority: https://deq.utah.gov/general/cybersecurity
59. S45 Vermont selected authority: https://legislature.vermont.gov/
60. S46 Virginia selected authority: https://law.lis.virginia.gov/vacode/title32.1/chapter6/section32.1-174.5/
61. S47 Washington selected authority: https://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.470
62. S48 West Virginia selected authority: https://code.wvlegislature.gov/5a-6B-4/
63. S49 Wisconsin selected authority: https://dnr.wisconsin.gov/topic/DrinkingWater/cybersecurity.html
64. S50 Wyoming selected authority: https://ets.wyo.gov/resources/policies-standards/security-privacy

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.