GLOBAL DIGITAL FORENSICS

OT ASSESSMENT PLANNING LIBRARY

State and Local OT Research Companion

Starting sources for all 50 states and a method for local and facility requirements

Edition 2026-11-03 | November 3, 2026

> Use this companion with the sector planning packs to find the state and local rules that apply to each facility.
>
> Record each decision in the project workbook so the source, the facility facts and the sign off stay together.

Questions about this document: call (800) 868-8189 or write to info@evestigate.com.

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

Contents

1. How to use this companion
2. How to resolve a state profile
3. State and sector differences
4. Local jurisdiction work instructions
5. Information needed for local determinations
6. State starting sources
7. Local duty and contact worksheet
8. Incident notification decision worksheet
9. Sources

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

How to use this companion

This companion supports the four sector planning packs. It gives one starting source for each state with what that source covers, and a method for settling local and facility requirements.

What each profile gives you

Each state row names the agency or legislature behind the starting source, what it covers and the link. Some sources are enacted sector laws; others are agency guidance or public entity standards. A starting source covers its own topic, so confirm the rule for every sector you operate in that state.

Use with the project workbook

Filter the Applicability sheet by facility state and sector. Add a row for each distinct obligation, then link the Local duties, Evidence, Notifications and Work plan records. Keep the source note and the facility decision in separate fields.

How to resolve a state profile

The compliance owner owns the applicability decision. The project manager tracks the evidence and prevents an unresolved legal assumption from becoming a completed task.

Read the actual instrument

Start with the linked authority and obtain the current codified text, adopted rule, final order or issued directive. Verify legal status, effective date, compliance date, entity definition, system scope, exemptions and incorporated documents. Preserve the copy and retrieval date.

Prove the facility facts

Establish the legal owner and operator, public/private status, regulated service, registrations, permits, contracts and physical/control center footprint. Support population, customer count and service connections with evidence. A federal registration or grant condition can create a different boundary from a state utility franchise.

Decide and document

Use Applicable, Not applicable with reason, or Unresolved. An applicable record names the work, frequency, due date rule, evidence, recipient and authorized official. A nonapplicability record names the exclusion and the facts that satisfy it. An unresolved record names the missing instrument or fact and how it limits the assessment.

Recheck changes

Review after an ownership change, new state footprint, changed service population, material process or architecture change, new contract, amended rule or significant incident. Assign a named owner and event based or dated review. Roll an old filing date forward only after checking the governing cycle.

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

State and sector differences

Use federal scope and the state instrument together. A state can regulate an entity for a different reason than its federal sector regulator.

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/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/quality requirements and personal information duties. Use the sector instrument.
Transportation	Mode and operating authority, state DOT and local ownership, rail transit State Safety Oversight, port/airport agreements, pipeline authority, public body policies and current issued federal security instruments.

Local jurisdiction work instructions

Create a local record for each facility and significant remote site. Resolve overlapping authorities before deciding the notification and operating plan.

Identify the authorities

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

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. Confirm a local checklist's legal force from its adopting authority.

Connect physical consequences and cyber events

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

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

Confirm the route without creating an incident

Use the authority's published procedure and an authorized nonincident clarification if needed. Record the official role, verified channel, after hours route and alternate. Test the reporting route with an agreed exercise procedure. During a real incident, follow the applicable reporting duty and preserve the submission receipt.

Sources: F06, F07

Information needed for local determinations

These inputs complete a location specific local pack. The worksheets in this volume record the decision and source.

Input	Why it changes the pack
Facility and remote site addresses	Identifies city, county, tribal/other authority and emergency response district. A corporate headquarters address is insufficient.
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 outside public rulebooks.
Operating and information boundaries	Distinguishes IT/OT, process safety, quality records, SSI/CEII/CUI and cross state dependencies.
Prior reports and approvals	Establishes actual certification dates, existing regulator conditions and recurring cycles rather than estimated dates.

State starting sources

One starting source per state, with what it covers. Confirm the rule for each sector you operate in the state.

State	Starting source	What it covers
Alabama	ADEM. adem.alabama.gov	ADEM encourages periodic water and wastewater cyber assessments. Treat this page as guidance. Separately inspect applicable utility rules, permit conditions and public entity policies.
Alaska	Alaska DEC. dec.alaska.gov	DEC explains federal AWIA coverage. Confirm the actual PWSID and certification history. OT assessment frequency is set sector by sector.
Arizona	Arizona Legislature. azleg.gov	ARS 18-552 concerns investigation and notice of personal information breaches. A SCADA disruption without the statutory data trigger must be assessed under other operational, utility and contractual duties.

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

State	Starting source	What it covers
Arkansas	Arkansas Division of Elementary and Secondary Education. adecm.ade.arkansas.gov	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. This law applies within its stated scope.
California	California PUC. webproda.cpuc.ca.gov	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.
Colorado	Colorado Secretary of State and PUC. sos.state.co.us	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. It governs its stated entities.
Connecticut	Connecticut DPH. portal.ct.gov	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 cyberreview instructions. Read its 2021 dates as historical milestones.
Delaware	Delaware PSC. depsc.delaware.gov	The PSC describes annual cybersecurity question and response filings for Class A utilities in DelaFile. Determine classification, filing instructions and corporate coverage. Field test mandates come from the governing instrument.
Florida	Florida Senate. flsenate.gov	Section 282.3185 governs local government cybersecurity and incident reporting. Identify the covered local government and severity/ransomware trigger before populating the clock. Apply local government obligations to local government operators.
Georgia	Georgia Technology Authority. gta.georgia.gov	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.
Hawaii	Hawaii PUC. puc.hawaii.gov	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 come from each operator's governing instrument.
Idaho	Idaho Technology Authority. Official policy text located; confirm adoption and coverage.. its.idaho.gov	Confirm operative adoption and actual agency coverage. Private facilities require separate statutory, permit and contract review.
Illinois	Illinois General Assembly. ilga.gov	HB3576 describes proposed water cybersecurity duties. Confirm enactment and the effective date from the official session law. Keep it on the watchlist and require an enacted Public Act before treating its proposed deadlines as mandatory.

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

State	Starting source	What it covers
Indiana	IDEM. in.gov	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. Read the current operative text from the official code; agency guidance explains it.
Iowa	Iowa Utilities Commission. rules.iowa.gov	The adopted Chapter 21 source addresses covered water, sanitary sewage and storm water utilities. Determine service and ownership coverage and current chapter text. This source supports facility specific audit planning.
Kansas	Kansas Legislature. kslegislature.gov	KSA 75-7244 concerns cyberincident reporting by defined public entities and government contractors. Resolve the statutory definitions and current reporting instructions. Confirm each private utility assessment requirement.
Kentucky	Kentucky PSC. psc.ky.gov	Determine PSC jurisdiction, applicable 807 KAR service rules and incident instructions. Water district commissioner training supports governance. Site orders and public entity policies remain to be checked.
Louisiana	Louisiana Legislature. legis.la.gov	Obtain current utility, water, incident reporting and public agency instruments for the named facility. Start with the Louisiana Public Service Commission for utility rules and the Louisiana Department of Health for drinking water rules. Confirm sector specific state requirements.
Maine	Maine Legislature. legislature.maine.gov	Title 35-A section 710 governs utility accident investigation and reporting. Determine whether the physical consequence meets the trigger. Review personal data breach and public agency incident duties on their own terms.
Maryland	Maryland General Assembly and MDE. mgaleg.maryland.gov	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 without replacing the statutory unit.
Massachusetts	MassDEP. mass.gov	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. Confirm current federal duties from current EPA authority.
Michigan	Michigan PSC. michigan.gov	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. Use the sector's own statute.

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

State	Starting source	What it covers
Minnesota	Minnesota Department of Health. Agency process and executive order reviewed.. health.mn.gov	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. Confirm private sector duties from statute, and take the federal population threshold from the federal text.
Mississippi	Mississippi ITS. its.ms.gov	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.
Missouri	Missouri Legislature. Codified sector clause.. revisor.mo.gov	Section 640.142 requires a cyberrisk 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. No assessment frequency or pentest requirement is supplied by this section.
Montana	Montana Department of Administration. doa.mt.gov	State guidance identifies a reporting route for large local government incidents on SummitNet. Connection and government status matter. This guidance informs the method for private industrial operators.
Nebraska	Nebraska Information Technology Commission. nitc.nebraska.gov	Determine whether NITC standards apply to the actual public entity or adopted board policy. Match each state agency standard to the public power entity's actual status. Review utility, water and public contract instruments separately.
Nevada	Nevada Legislature. leg.state.nv.us	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 run in parallel.
New Hampshire	New Hampshire Legislature. gc.nh.gov	RSA 485:3-e and 485-A:5-f establish water and wastewater cyberprogram 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.

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

State	Starting source	What it covers
New Jersey	New Jersey DEP and Legislature. dep.nj.gov	Use more than 500 service connections for WQAA scope (N.J.S.A. 58:31-2). The cybersecurity program must cover every industrial control system and conform to the NIST Cybersecurity Framework, the CIS Controls or ISO/IEC 27000. Join NJCCIC, report each cybersecurity incident to NJCCIC promptly after an employee becomes aware of it, and expect an NJCCIC audit within 30 days of a report (58:31-4.2). Confirm any separate BPU order. Scope the broader 2023 incident reporting law for public agencies on its own terms.
New Mexico	New Mexico DoIT. doit.nm.gov	The DoIT library identifies agency IT policy and incident standards. Obtain the current Cybersecurity Act, implementing rules and public body definitions. Apply enacted law and agency policy to the operators they name.
New York	New York DEC and DOH. dec.ny.gov	Separate DOH drinking water duties from DEC wastewater duties. Appendix 5-E covers community water systems serving more than 3,300 people: operator training and incident reports to DOH within 24 hours have applied since adoption on March 11, 2026, and the 48 hour vulnerability report, the cybersecurity program and the annual vulnerability analysis apply from January 1, 2027. DEC requires every SPDES permittee to report a cybersecurity incident within 24 hours (from March 26, 2026) with a 30 day written report; POTW controls and emergency response plans apply from March 11, 2027, with the first annual certification due March 28, 2027. PSC Part 1200 utility IT rules apply from June 1, 2026 for covered utilities.
North Carolina	North Carolina DIT. it.nc.gov	State and local government cyberincident reporting must be checked against current GS 143B-1379 and reporting instructions. A municipal operator can be covered because of government status. Private operator duties come from sector or contract triggers.
North Dakota	North Dakota Legislature. ndlegis.gov	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.
Ohio	Ohio EPA. codes.ohio.gov	OAC 3745-81-31 addresses public water reporting, including facts affecting safe operations. Determine the relevant incident trigger. Scope Ohio EPA cyber guidance and PUCO electric standards one at a time; insurance licensee rules govern insurers.
Oklahoma	Oklahoma OMES. oklahoma.gov	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.

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

State	Starting source	What it covers
Oregon	Oregon Legislature. oregonlegislature.gov	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 without becoming a rule for every operator.
Pennsylvania	Pennsylvania DEP and PUC. pa.gov	DEP provides water cybersecurity guidance. The 2025 PUC supplemental advance notice proposed changes including Chapter 104 incident reporting; track it to final adoption. Track proposed clocks until adoption. Retrieve current utility orders and any final adoption.
Rhode Island	Rhode Island Legislature. webserver.rilegislature.gov	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. The starting source covers its stated entities.
South Carolina	South Carolina DES. des.sc.gov	DES water cybersecurity materials provide practical guidance. Confirm any inspection or permit specific requirements. Water, manufacturing and transportation obligations come from sector instruments.
South Dakota	South Dakota Legislature. sdlegislature.gov	The selected law criminalizes interference with critical infrastructure. Operator specific instruments set periodic cyber assessments. Obtain PUC, environmental, public entity and contract instruments for affirmative duties.
Tennessee	Tennessee Secretary of State. Annual utility cybersecurity filing docket.. publications.tnsosfiles.com	TPUC Docket 26-00047 documents 2026 annual confidential utility cybersecurity filings, including water, wastewater and gas providers. This records current implementation; scope exceptions, the July 1 deadline and incident clocks come from the rule text. Authenticate the current codified chapter 1220-04-15 from the official code. Use the adopted rule and this utility's own filing.
Texas	Texas Legislature. Adopted electric EOP rule; confirm later amendments.. tcss.legis.texas.gov	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. Reconcile the current codified text with later amendments.
Utah	Utah DEQ. deq.utah.gov	DEQ provides a water and wastewater cyberplan route. Determine whether individual items are guidance, permit conditions or adopted requirements. Utah government IT rules govern state entities.
Vermont	Vermont Legislature. legislature.vermont.gov	OT assessment duties follow operator specific triggers. Retrieve current PUC electric and gas rules, water requirements and any public entity cyber law for the facility. Confirm enactment from the chaptered law.

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

State	Starting source	What it covers
Virginia	Virginia Legislature. law.lis.virginia.gov	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.
Washington	Washington Legislature. apps.leg.wa.gov	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.
West Virginia	West Virginia Legislature. code.wvlegislature.gov	The codified cybersecurity program section addresses agency risk assessments. The separate cyber incident reporting chapter 15-5C and current definitions must also be checked. Private operator coverage turns on the statutory definition.
Wisconsin	Wisconsin DNR. dnr.wisconsin.gov	DNR provides water cybersecurity resources. Use the actual PWS and utility authority to determine obligations.
Wyoming	Wyoming ETS and PSC. ets.wyo.gov	ETS security and risk assessment standards require an agency scope decision. PSC jurisdiction and current water or electric orders must be reviewed separately. Apply an agency standard to the entities it names.

Local duty and contact worksheet

Complete for a named facility. Record local requirement reviews with sources and reviewers.

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

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

Compliance decision unresolved facts approval date and next review

Incident notification decision worksheet

Record concurrent duties separately. Use the applicable definition and clock, and escalate a possible reporting duty ahead of complete attribution.

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

Each source is linked to the issuing authority or publisher. The date shows when the entry was last checked.

W04 Cybersecurity for Water and Wastewater Facilities. Indiana IDEM. Agency implementation guidance. IC 13-18-16.5; covered facility types; 2026 assessments and incident reporting. https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/ (checked October 15, 2026)

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

W05 Maryland Environment 9-2705, current selected codified text. Maryland General Assembly. Selected current codified statute. 9-2705(a), (b). Over 3,300 customers for this section. Other Subtitle 27 duties have different scope. Confirm current implementation and reconcile the attachment discrepancy. https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2705&enactments=false (checked October 17, 2026)

W06 MDE SB871 implementation guidance, May 2026. Maryland MDE. Agency guidance. Sections 3-9; Attachments 1-2. Statute and regulation govern; guidance explains. Attachment 2 people threshold differs from statute customers; confirm current instructions and provider deadlines. https://mde.maryland.gov/programs/water/water_supply/Documents/SB871.pdf (checked October 17, 2026)

F01 Guide to Operational Technology Security Revision 3. NIST. Final guidance. September 2023 final publication; chapters 4 through 6 and OT control tailoring. https://csrc.nist.gov/pubs/sp/800/82/r3/final (checked October 15, 2026)

F03 Technical Guide to Information Security Testing and Assessment. NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints; the operating owner authorizes production testing. https://csrc.nist.gov/pubs/sp/800/115/final (checked October 15, 2026)

F06 State Plans. OSHA. Jurisdiction directory. State and federal occupational safety jurisdiction. Check public employee coverage and industry exceptions for the actual workplace. https://www.osha.gov/stateplans/ (checked October 15, 2026)

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. https://www.epa.gov/epcra/epcra-emergency-release-notifications (checked October 15, 2026)

S01 Alabama starting source. ADEM. Agency guidance. State authority and applicability sources current to October 15, 2026. https://adem.alabama.gov/water/drinking-water-branch/information-public-water-systems/cybersecurity-resources-public-water-systems (checked October 15, 2026)

S02 Alaska starting source. Alaska DEC. Agency guidance. State authority and applicability sources current to October 15, 2026. https://dec.alaska.gov/eh/dw/security/regulations/awia-regulations (checked October 15, 2026)

S03 Arizona starting source. Arizona Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://azleg.gov/ars/18/00552.htm (checked October 15, 2026)

S04 Arkansas starting source. Arkansas Division of Elementary and Secondary Education. Official implementation memo. State authority and applicability sources current to October 15, 2026. https://adecm.ade.arkansas.gov/ViewApprovedMemo.aspx?Id=4848 (checked October 15, 2026)

S05 California starting source. California PUC. Regulator routing source. State authority and applicability sources current to October 15, 2026. https://webproda.cpuc.ca.gov/regulatory-services/safety/emergency-reporting (checked October 15, 2026)

S06 Colorado starting source. Colorado Secretary of State and PUC. Selected rule text. State authority and applicability sources current to October 15, 2026. https://www.sos.state.co.us/CCR/GenerateRulePdf.do?fileName=4+CCR+723-3&ruleVersionId=10399 (checked October 15, 2026)

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

S07 Connecticut starting source. Connecticut DPH. Historical agency circular. State authority and applicability sources current to October 15, 2026. 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 (checked October 15, 2026)

S08 Delaware starting source. Delaware PSC. Regulator program. State authority and applicability sources current to October 15, 2026. https://depsc.delaware.gov/cybersecurity/ (checked October 15, 2026)

S09 Florida starting source. Florida Senate. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://www.flsenate.gov/Laws/Statutes/2026/282.3185 (checked October 15, 2026)

S10 Georgia starting source. Georgia Technology Authority. Agency reporting source. State authority and applicability sources current to October 15, 2026. https://gta.georgia.gov/contact-us/cybersecurity-incidents (checked October 15, 2026)

S11 Hawaii starting source. Hawaii PUC. Regulator directory. State authority and applicability sources current to October 15, 2026. https://puc.hawaii.gov/about/statutes-rules-orders/ (checked October 15, 2026)

S12 Idaho ITS Information Security Policy Manual, version 4.0. Idaho Technology Authority. Official policy text located; confirm adoption and coverage. Confirm operative adoption and actual agency coverage. Private facilities require separate statutory, permit and contract review. Verify current operative adoption and entity scope. Binds the facilities within its stated scope. https://its.idaho.gov/wp-content/uploads/2025/10/2025-ITS-Information-Security-Policy-Manual-4.0.FINAL_.pdf (checked October 17, 2026)

S13 Illinois starting source. Illinois General Assembly. Pending bill. State authority and applicability sources current to October 15, 2026. https://www.ilga.gov/Legislation/BillStatus?DocNum=3576&DocTypeID=HB&GAID=18&LegId=0&Print=1&SessionID=114 (checked October 15, 2026)

S14 Indiana starting source. IDEM. Agency implementation guidance. State authority and applicability sources current to October 15, 2026. IDEM guidance separates the annual assessment from the every other year certification. Confirm the current statute and the entity facts. https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/ (checked October 17, 2026)

S15 Iowa starting source. Iowa Utilities Commission. Selected utility rule. State authority and applicability sources current to October 15, 2026. https://rules.iowa.gov/Notice/Details/8846C (checked October 15, 2026)

S16 Kansas starting source. Kansas Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://kslegislature.gov/b2023_24/laws/075_000_0000_chapter/075_072_0000_article/075_072_0044_section/075_072_0044_k/ (checked October 15, 2026)

S17 Kentucky starting source. Kentucky PSC. Regulator routing source. State authority and applicability sources current to October 15, 2026. https://psc.ky.gov/Home/UtilForms (checked October 15, 2026)

S18 Louisiana starting source. Louisiana Legislature. State legislature. State authority and applicability sources current to October 15, 2026. https://legis.la.gov/ (checked October 15, 2026)

S19 Maine starting source. Maine Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://www.legislature.maine.gov/legis/statutes/35-A/title35-Asec710.html (checked October 15, 2026)

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

S20 Maryland Environment 9-2705, current selected codified text. Maryland General Assembly and MDE. Selected current codified statute. 9-2705(a), (b). Over 3,300 customers for this section. Other Subtitle 27 duties have different scope. Confirm current implementation and reconcile the attachment discrepancy. https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2705&enactments=false (checked October 17, 2026)

S21 Massachusetts starting source. MassDEP. Agency program with scope review. State authority and applicability sources current to October 15, 2026. https://www.mass.gov/info-details/public-drinking-water-system-operations (checked October 15, 2026)

S22 Michigan starting source. Michigan PSC. Regulator implementation source. State authority and applicability sources current to October 15, 2026. https://www.michigan.gov/mpsc/regulatory/emergency-management/utility-incident-notification-procedures (checked October 15, 2026)

S23 Minnesota starting source. Minnesota Department of Health. Agency process and executive order reviewed. 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. Confirm private sector duties from statute, and take the federal population threshold from the federal text. https://www.health.mn.gov/communities/environment/emergency/water/securityassess.html (checked October 17, 2026)

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, and confirm operator specific authority and current agency implementation. https://mn.gov/governor/assets/EO%2022-20_tcm1055-539386.pdf (checked October 17, 2026)

S23A Minnesota Executive Order 24-07. Minnesota Legislative Reference Library. Amending executive order. Paragraphs 4 and 8. Amends the agency definition; EO 22-20 continues with its existing scope. https://www.lrl.mn.gov/archive/execorders/24-07.pdf (checked October 17, 2026)

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. Submit findings on the regulator's request. https://www.health.mn.gov/communities/environment/water/docs/cyberform.pdf (checked October 17, 2026)

S24 Mississippi starting source. Mississippi ITS. Agency reporting source. State authority and applicability sources current to October 15, 2026. https://www.its.ms.gov/services/security/Enterprise-Cybersecurity-Incident-Reporting (checked October 15, 2026)

S25 Missouri starting source. Missouri Legislature. Codified sector clause. Section 640.142 requires a cyberrisk 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. No assessment frequency or pentest requirement is supplied by this section. https://revisor.mo.gov/main/OneSection.aspx?section=640.142 (checked October 17, 2026)

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

S26 Montana starting source. Montana Department of Administration. Agency guidance. State authority and applicability sources current to October 15, 2026. https://doa.mt.gov/SITSD/cybersecurity (checked October 15, 2026)

S27 Nebraska starting source. Nebraska Information Technology Commission. Standards directory. State authority and applicability sources current to October 15, 2026. https://nitc.nebraska.gov/standards-and-guidelines/ (checked October 15, 2026)

S28 Nevada starting source. Nevada Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://www.leg.state.nv.us/nrs/nrs-480.html (checked October 15, 2026)

S29 New Hampshire starting source. New Hampshire Legislature. Enacted sector law. State authority and applicability sources current to October 15, 2026. https://gc.nh.gov/rsa/html/L/485/485-3-e.htm (checked October 15, 2026)

NH-WW Wastewater cybersecurity protection program. New Hampshire Legislature. Enacted sector law. RSA 485-A:5-f; current codified text. https://www.gc.nh.gov/rsa/html/L/485-A/485-A-5-f.htm (checked October 15, 2026)

S30 New Jersey starting source. New Jersey DEP and Legislature. Enacted sector framework. State authority and applicability sources current to October 15, 2026. https://dep.nj.gov/watersupply/drinking-water-systems/water-quality-accountability-act/ (checked October 15, 2026)

W08 Water Quality Accountability Act amendments, P.L.2021, c.262. New Jersey Legislature. Enacted law. N.J.S.A. 58:31-2 (more than 500 service connections), 58:31-4.1 (program covering all industrial control systems), 58:31-4.2 (prompt NJCCIC reporting; NJCCIC audit within 30 days). https://pub.njleg.gov/bills/2020/PL21/262_.HTM (checked November 3, 2026)

S31 New Mexico starting source. New Mexico DoIT. Policy directory and scope review. State authority and applicability sources current to October 15, 2026. https://www.doit.nm.gov/about/doit-act-policies-and-rules (checked October 15, 2026)

S32 New York starting source. New York DEC and DOH. Adopted sector rules. State authority and applicability sources current to October 15, 2026. https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources (checked October 15, 2026)

W09 New York drinking water cybersecurity applicability. New York DOH. Current rule page. 10 NYCRR Appendix 5-E: community water systems serving more than 3,300 people. https://regs.health.ny.gov/content/section-5-e1-applicability (checked October 15, 2026)

S33 North Carolina starting source. North Carolina DIT. Agency implementation guidance. State authority and applicability sources current to October 15, 2026. https://it.nc.gov/programs/cybersecurity-risk-management/cyber-incident-reporting (checked October 15, 2026)

S34 North Dakota starting source. North Dakota Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://ndlegis.gov/cencode/t54c59-1.pdf (checked October 15, 2026)

S35 Ohio starting source. Ohio EPA. Selected operational reporting rule. State authority and applicability sources current to October 15, 2026. https://codes.ohio.gov/ohio-administrative-code/rule-3745-81-31 (checked October 15, 2026)

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

S36 Oklahoma starting source. Oklahoma OMES. Agency reporting directory. State authority and applicability sources current to October 15, 2026. https://www.oklahoma.gov/omes/divisions/information-services/about-information-services/it-statutory-and-regulatory-reporting.html (checked October 15, 2026)

S37 Oregon starting source. Oregon Legislature. Selected enacted law. State authority and applicability sources current to October 15, 2026. https://www.oregonlegislature.gov/bills_laws/ors/ors276a.html (checked October 15, 2026)

S38 Pennsylvania starting source. Pennsylvania DEP and PUC. Guidance and rulemaking watchlist. State authority and applicability sources current to October 15, 2026. https://www.pa.gov/agencies/dep/programs-and-services/water/bureau-of-safe-drinking-water/cybersecurity (checked October 15, 2026)

S39 Rhode Island starting source. Rhode Island Legislature. Selected utility law. State authority and applicability sources current to October 15, 2026. https://webserver.rilegislature.gov/statutes/title39/39-2/39-2-26.htm (checked October 15, 2026)

S40 South Carolina starting source. South Carolina DES. Agency guidance. State authority and applicability sources current to October 15, 2026. https://www.des.sc.gov/programs/bureau-water/water-utilities-cybersecurity (checked October 15, 2026)

S41 South Dakota starting source. South Dakota Legislature. Criminal statute only. State authority and applicability sources current to October 15, 2026. https://sdlegislature.gov/Statutes/22-34-28 (checked October 15, 2026)

S42 Tennessee starting source. Tennessee Secretary of State. Annual utility cybersecurity filing docket. TPUC Docket 26-00047 documents 2026 annual confidential utility cybersecurity filings, including water, wastewater and gas providers. This records current implementation; scope exceptions, the July 1 deadline and incident clocks come from the rule text. Authenticate the current codified chapter 1220-04-15 from the official code. Use the adopted rule and this utility's own filing. https://publications.tnsosfiles.com/rules_filings/06-31-23.pdf (checked October 17, 2026)

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. https://tpucdockets.tn.gov/dockets/2500042.htm (checked October 15, 2026)

S42D 2026 annual utility cybersecurity filing docket 26-00047. Tennessee Public Utility Commission. Current filing implementation record. 2026 annual confidential reports. The docket records implementation; rule text and entity facts set deadlines and coverage. https://tpucdockets.tn.gov/dockets/2600047.htm (checked October 17, 2026)

S43 Texas starting source. Texas Legislature. Adopted electric EOP rule; confirm later amendments. 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. Reconcile the current codified text with later amendments. https://tcss.legis.texas.gov/resources/UT/htm/UT.39.htm (checked October 17, 2026)

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

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 with the current codification. Apply electric entity, facility and activation exceptions. Not a penetration test duty. https://www.sos.state.tx.us/texreg/archive/December262025/Adopted%20Rules/16.ECONOMIC%20REGULATION.html (checked October 17, 2026)

S44 Utah starting source. Utah DEQ. Agency guidance. State authority and applicability sources current to October 15, 2026. https://deq.utah.gov/general/cybersecurity (checked October 15, 2026)

S45 Vermont starting source. Vermont Legislature. State legislature. State authority and applicability sources current to October 15, 2026. https://legislature.vermont.gov/ (checked October 15, 2026)

S46 Virginia starting source. Virginia Legislature. Selected enacted operational law. State authority and applicability sources current to October 15, 2026. https://law.lis.virginia.gov/vacode/title32.1/chapter6/section32.1-174.5/ (checked October 15, 2026)

S47 Washington starting source. Washington Legislature. Selected enacted agency law. State authority and applicability sources current to October 15, 2026. https://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.470 (checked October 15, 2026)

S48 West Virginia starting source. West Virginia Legislature. Selected enacted agency law. State authority and applicability sources current to October 15, 2026. https://code.wvlegislature.gov/5a-6B-4/ (checked October 15, 2026)

S49 Wisconsin starting source. Wisconsin DNR. Agency guidance. State authority and applicability sources current to October 15, 2026. https://dnr.wisconsin.gov/topic/DrinkingWater/cybersecurity.html (checked October 15, 2026)

S50 Wyoming starting source. Wyoming ETS and PSC. Standards directory. State authority and applicability sources current to October 15, 2026. https://ets.wyo.gov/resources/policies-standards/security-privacy (checked October 15, 2026)

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

Plan the assessment with a senior examiner

A senior GDF examiner can map your facilities to the state and local rules that apply and recommend the assessment scope on the first call.

Get a free consultation. The initial consultation is free, and requests are handled in confidence.

Call (800) 868-8189 at any hour, or write to info@evestigate.com.

Request a consultation online at evestigate.com/contact.

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