Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/gdf-audit-preparation/

AUDIT PREPARATION FOR OT AND UTILITY SPONSORS

Prepare for an OT Audit Before the First Meeting

An audit goes faster and costs less when the entity, the facilities, the records and the open questions are already written down. This walkthrough shows you how to build that starting record with GDF and what to bring to the first meeting.

What follows is planning guidance. The applicable instrument and the facts of your entity set the actual duties, so treat every prepared item as a record for the auditor to examine.

1. Define the Proposed Scope Before Anyone Gathers a Record

The project manager and the sponsor identify the legal entity, the operating owner, the actual facilities, the objective of the audit, the review period and the people who will read the report, and they write those facts on one page with the source for each. Locate the charter, license, registration and operating agreement records that establish them, because the auditor's first request is for the documents that prove the entity is what the scope says it is. A city's permits and a utility's governing orders come from the instruments themselves, so retrieve them alongside the state selection.

Record every external deadline with the source that controls it and keep internal project target dates separate, so every planning goal and every legal clock reads for what it is. Where ownership, counts or coverage are still being confirmed, choose the unresolved answer and keep the follow up action visible. An unresolved row with an owner and a next action is a controlled record that moves the file forward.

The OT builder filters sector and state research and procedures, and the New York builder filters selected detailed tracks. Ownership, service and other profile facts are declarations for review. Legal determinations rest with the people who make them, and the record shows who decided each point.

If the entity, the facilities or the review period are still being debated inside your own organization, bring that dispute to the scoping conversation; it is quickest and least costly to settle there.

2. Gather the Records That Already Exist

Open the record gathering step in the builder or the Preparation sheet in the downloaded workbook. Each action explains what to locate, why GDF needs it, who is likely to hold it and what GDF verifies once it is found. Most of these records already exist in engineering, identity and records systems; the work is finding them and writing down who holds each one.

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

Scope and criteria
Entity and facility lists, current instruments and correspondence, exclusions, prior reports and open corrective actions. Ask legal, regulatory affairs and the operating owner.

Systems and evidence
Existing inventories, architecture and data flows, access records, record populations and the review period. Ask engineering, security and the responsible data owners, and agree collection and sampling with GDF.

Operations and handoff
Operating constraints, supplier permissions, stop authority, response and recovery records and controlled evidence handling instructions. Ask operations, safety, records management and the incident lead.

Apply the five record statuses consistently

Mark a record Not reviewed until someone assesses its availability. Mark it Still needed once an owner and a next action have been identified. Mark it Located for review when a controlled record reference exists, and GDF then examines its currency, scope and sufficiency. Mark it Needs clarification when a question remains, and record the responsible person or role. Mark it Proposed not applicable with a reason, and it becomes a decision once the responsible scope review is recorded.

For example, mark the asset inventory Located for review and enter a non sensitive reference such as ENG-INV-04 while the actual network drawing stays in the controlled repository. The package flags Reference missing on a record awaiting its reference and Reason missing on a proposed exclusion awaiting its reason, because those are the two details auditors check most often in a preparation file.

---

3. Work Through the Open Questions Honestly

The Uncertainty sheet and the open questions CSV sort open items into profile facts to confirm, site records to locate, state and sector research and authority questions. Each entry says what to obtain, who may hold it and how it affects the audit plan. Record the actual decision, the responsible review and the supporting evidence in the workbook, because the recorded decision is what resolves the question, and an auditor reads the decision column before the record column.

For all state OT planning, treat the state and sector rows as a client research checklist: the source notes point to where each rule lives, and the current text for each sector and local facility completes the answer. Retrieve the current rules and orders, permits, contracts and local instructions themselves and file the copy with its retrieval date.

For water systems, obtain the actual system identifiers, the system type and the dated population, connection and customer measures, which are three distinct measures, together with any existing assessment, plan and certification records and their receipts.

For power, obtain the registration and functions, the system categorization, the applicable requirement versions and the implementation dates, and freeze them for the review period.

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

For manufacturing, obtain the actual covered process, safety, quality and executed contract criteria. Contract implementation and licensed standards are read from the current instrument with the responsible specialist.

For transportation, obtain the current operator issued directions, approved plans and mode specific permissions through authorized channels. The operator issued directions carry the current criteria, and public copies and summaries serve as background.

For New York utilities, retain questions Q01 through Q10. First year timing, apparent discrepancies in adopted text, current DPS utility instructions, entity scope, data access instruments and the operative DFS baseline are each settled with the identified evidence or written clarification.

Read the OT questions to settle before field work and the New York utility audit questions for counsel. An open question is a research task, recorded as planning work for its owner.

Where an answer is still on its way, identify the dependency and the proposed next action. GDF and the accountable owner then agree whether the affected work proceeds now, after further research or in a later phase.

Owners for open questions are the first thing we ask about on a scoping call, so bring the list as it stands.

---

4. Agree Access and Safe Work Before Anything Is Touched

Use existing approved records first. This checklist is completed from existing records, and scans, configuration changes, live failovers, switching operations and customer record collection each belong to the authorized engagement that follows. Before any activity that could affect operations, agree in writing the operating permission, the methods, the vendor restrictions, the maintenance windows, the stop authority and the recovery arrangements, with a named person and a tested phone number for the stop authority.

GDF and the evidence owners agree on the population, the sampling, the collection permissions, the time basis, the evidence references and the access limits. Preserve contrary evidence and note each record's availability. The workbook records a documented procedure and a demonstrated control in separate fields, and a proposed fix and a verified correction the same way, so each stage reads clearly later.

Keep personal information, passwords, network details and restricted transport directions in your controlled systems, and use non sensitive references in the public builder and the initial contact. Agree on the authorized recipients, the classification and an exchange method before any controlled file changes hands.

Which activities need written operating permission is a question to settle with GDF well ahead of the site visit; raise it in the scoping conversation.

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

5. Arrange the Scoping Conversation With GDF

Bring a non sensitive summary of the entity and facility scope, the audit purpose and period, the available record categories, the open questions with their owners, the proposed exclusions with their reasons, the external dates and the operating constraints. The preparation HTML, the checklist CSV and the workbook registers are the starting point for that discussion, and the initial consultation is free.

We agree scope, current criteria, research work, team responsibilities, evidence handling, safe methods, timing and deliverables before any assessment work begins. Actual technical, compliance and operating decisions are recorded by the people responsible for them.

Planning References and Package Contents

NIST SP 800-115 informs assessment planning, evidence and reporting, and NIST SP 800-82 Revision 3 informs OT security with its operational reliability and safety constraints. These technical guides shape the method; the legal audit requirements come from the instruments that apply to you.

For current DFS materials, start with the DFS cybersecurity resource page and reconcile the controlling text against the entity records. The New York workbook marks the points where further authority is gathered.

Each generated set includes an offline preparation walkthrough, two preparation CSVs and the project workbooks. The technical reference PDFs and the manuals remain useful alongside the preparation registers.

Open the OT planning library or the NY utility planning library for the full package contents.

Workbook field and documentation guide

Using the audit workbooks

Start with the Preparation and Uncertainty sheets. This guide describes the twenty core sheets; the current national and New York workbooks add an Assessment prep sheet, for 22 and 21 sheets respectively.

Record control

Use the Start sheet to identify the legal entity, review period, actual responsible people and approved evidence location. In the NY workbook, D22 is the single evidence location input; D38 is a linked display. The template edition is fixed. Record your project revisions separately in Edition record.

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

Amber cells accept input. Derived documentation follow up cells are protected against accidental edits, with no password set. Evidence integrity and access control come from your controlled versions, backups and repository.

Preparation and scope changes

Project or facility renaming preserves entries. Changing other scope facts with entered preparation records opens a comparison. Download current records, explicitly clear to accept the new scope, or cancel. Downloads generated before the change reflect the earlier scope, so generate fresh ones. Reset, reload and leaving the page clear in memory entries, and your records are saved when you download them, on your own machine.

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

Document examination and correction

A declared Supported, Evidence supports criterion or Verified closed result is separate from Documentation follow up. Compliance is decided by the responsible reviewer from the evidence behind both fields.

Examination records

Record the exact criterion and system boundary, population and period, sample identifiers/count and selection rationale, actual method, typed execution date, actual observations, evidence references, actual reviewer, typed review date and review disposition. Link the activity permit or explain a records only method. Where the full population is examined, document the reason and the method.

The NY Control tests register now has distinct sample rationale, observation and reviewer fields. A Supported result keeps specific follow up flags until its prerequisites are filled. Whitespace, common unresolved placeholders and invalid pasted statuses are flagged. Fields present is followed by an examination of substance and sufficiency.

Completion and closure

A Complete task needs an assigned owner, completion evidence, actual completion date and completion review. A Verified closed finding needs implementation evidence, a scoped retest result and date, and closure authority with an actual approval date. Record remaining limits and residual risk decisions. Implemented and verified closed are different states.

Enter real spreadsheet dates; the check flags a date typed as text as missing/invalid. Where work awaits permission, record the authorization status and what happens next. A proposed not applicable result is completed by a supported basis and actual review.

Sources: F03 Technical Guide to Information Security Testing and Assessment

Map requirements before concluding

Requirements is a working register that grows as your research adds the laws and standards that apply. The national state and sector rows form a client research checklist.

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

Requirement to procedure trace

Use one row per exact applicable clause or requirement part. Record instrument/version, entity/system/period, coverage evidence, effective/compliance dates and basis, required method/evidence, mapped procedures, actual conclusion and responsible review. Split grouped starter rows before a clause level conclusion. Where a requirement awaits a procedure, assign a next action and owner.

All starter requirements remain in custom exports. Work for an unselected sector or NY track is marked deferred. The 469 NY PSC/DFS clause/context rows remain, with Core and Privacy rows ready for your research. Context and definitions support the control duties they explain.

Power communications screening

P-CIP07 explicitly screens CIP-012-2 Control Center coverage and exemptions. Requirements separately identifies A.4 and R1.1-R1.5: disclosure/modification protection, communications availability, link recovery, implemented method locations and responsibilities across separate Responsible Entities. Record the actual jurisdiction, registered functions, applicable implementation plan and review period, and take each version and date from them. Use approved record review.

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, P08 CIP-012-2 communications between Control Centers

New York drinking water records

The national water workbook adds W-NY02 training, W-NY03 incident reporting and W-NY04 transition/program review. These are separate from the existing wastewater procedure. Obtain the DOH hosted Appendix 5-E and reconcile current codified text and referenced Subpart provisions.

Training and transition

Appendix 5-E.1(a) applies most duties to community water systems serving more than 3,300 people. The personnel and network monitoring provisions identified there use a combined wholesale and retail population greater than 50,000. These are population measures, distinct from customer or service connection counts.

Section 5-E.7 covers all drinking water treatment operators certified under Subpart 5-4, independent of the 5-E.2 exclusion: at least one hour of DOH approved cybersecurity training every three years. Obtain actual registration cycles and completion evidence. DOH guidance identifies the end of the first full registration cycle following the effective date. Section 5-E.1(b) makes 5-E.7 and 5-E.9 immediate upon adoption, with January 1 2027 for remaining Appendix duties.

Incident and vulnerability triggers

For a covered system, 5-E.9 requires notice as soon as possible and no later than 24 hours after determining a cybersecurity incident as defined in 5-E.3(e) has occurred which has created or may create a public health hazard. Preserve other separately applicable notices. The DOH FAQ uses detection shorthand; use the full rule trigger and resolve any operational interpretation with the responsible compliance owner or DOH.

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

Sections 5-E.1(c) and 5-E.5 require qualifying CVA vulnerability reporting within 48 hours of identification. Keep that distinct from incident reporting and the January 2027 transition. Section 5-E.5(f) requires at least annual CVA review/update and review within 30 days after major water facility infrastructure changes are operational. Obtain the referenced submission, correction and plan provisions before assigning a facility calendar.

Sources and coverage

Full official sources: https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/appendix_5e.pdf and https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-012-2.pdf . Sources W12 and P08 identify these records in the national workbook. Website summaries are supporting guidance. Site coverage, exclusion and compliance decisions are recorded by the responsible owners.

Sources: W12 NY drinking water cybersecurity Appendix 5-E, W13 NY drinking water cybersecurity FAQ and transition guidance

Use the field print view and resolve open work

Field record provides one linked procedure at a time for field use. The full register is the authoritative digital working record.

Print and field handoff

Choose a listed procedure ID in B5 and recalculate. The view links to the procedure, boundary/criterion, expected and actual records, evidence references and review/permission reference. Enter evidence and observations in the owning control register. Review the linked Activity permits record for targets, approved methods/window, baseline, stop conditions, recovery and operating/technical approvals before activity.

Print areas and repeated labels are configured. Full registers print at readable scale across several pages. The field view may span several pages and long narratives need a controlled continuation. Check print preview on the actual Letter/A4 device.

Unresolved items stay on the plan

Assign an accountable owner and next evidence for every unresolved authority, missing record and proposed exclusion. Agree engagement criteria, competence, independence, access, safe methods and deliverables with GDF. Use the current restricted transportation instruments, contract instructions and licensed standards where applicable. The qualified team applies the professional standards that fit the engagement, with the template as its starting record.

Every manual on this site is free to read. Downloads start directly, and introducing yourself to GDF first is optional.

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.

Extend controlled working registers

Use the local workbook extension tool on the GDF audit preparation page. It accepts a saved OT or NY workbook, including a previously customized or extended copy. Files remain in browser memory. This operation adds rows; the assessment itself happens in the engagement.

Before extending

Save the current controlled workbook and record its edition. Select the owning register: Requirements, Control checks or Control tests, Work plan, or Findings. Choose 10, 25 or 50 additional rows. The tool checks the workbook structure and accepts supported OT and NY workbook files.

What changes

New unique ADD identifiers are assigned. New records start blank or unresolved, with the applicable listed pending status. Existing records are preserved. New criteria and input fields are editable; derived follow up formulas remain protected. Table/filter ranges, validation ranges, print areas and control ID selectors/field record lookup bounds are extended.

After download

Use the downloaded copy as the next controlled version. Check the displayed register counts and new IDs. Fill in actual scope, criteria, procedures and required evidence before execution. Select a new control ID in Field record to read or print it. Repeat the extension operation if needed within its stated size limits. Retain the prior version and have the actual reviewer check the new records.

Capacity

The tool adds working capacity to supported macro free workbooks, up to 50 rows per operation within a 10,000 row register, and GDF handles the legal research, applicability and evidence review with you.

Dates, unfinished entries and attribution

Documentation follow up is a bounded record check, and compliance and evidence quality are decided by the reviewer. Record planned dates separately from actual events.

Actual chronology

Actual execution, review, completion, retest, closure and decision dates must be valid dates on or before the current day. Review follows execution, and closure follows the required retest. Blank dates, future actual dates and reversed chronology generate follow up warnings. Correct errors or record a justified limitation with the actual reviewer.

Unfinished entries

TBD, TBC, pending, pending client records, unknown, not provided, not established, unresolved, n/a and to be determined are treated as missing when they stand alone. Case, ordinary surrounding whitespace and nonbreaking spaces are normalized. The list catches the common placeholders, and the actual reviewer reads each entry for the rest. Use a real evidence ID or secure reference; record pending requests in next action fields.

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

People who did the work

NY Control tests now asks for the actual examiner, carried into Field record and the documentation check. NY Evidence separately asks for the actual collector or an identified collection record reference. Accountable owner, custodian, examiner, collector and actual reviewer have different meanings.

Human review

Once documentation is recorded, the actual reviewer evaluates sufficiency, sample rationale, contradictory evidence, permissions, source currency and the stated conclusion.

Dedicated New Jersey Planning Set

For a New Jersey engagement, use the dedicated state set to assign evidence requests, resolve authority questions and build the facility specific duty calendar.

Open the New Jersey water, wastewater, electric and gas utility set, or customize a New Jersey utility set (evestigate.com/tools/nj-ot-audit-builder/).

Prepare for the Assessment Being Proposed

Plan the engagement, organize the supporting records and identify the permissions before the work begins. A completed checklist prepares the assessment, the compliance decision and the authority to test.

The five preparation tracks apply across utilities, manufacturing and transportation. They organize records and planning questions; the actual criteria, scope, methods and testing permissions are agreed with the qualified assessment team.

Common preparation

AP01 Define the preparation brief

Gather: Requested service and decision; facilities/entities; intended users; proposed period; known exclusions; deliverables and assessment limitations.

Responsible role: Sponsor and GDF engagement lead

Purpose and boundary: An audit, control review and penetration test answer different questions; preparation identifies the requested work.

AP02 Identify owners and authority

Gather: Legal asset/site owners; operating authority; landlord/shared site rights; third party/cloud/vendor approval requirements; actual approvers.

Responsible role: Organization legal and operating owners

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

Purpose and boundary: Ownership, access and testing authority can belong to different parties.

AP03 Organize one facility and system inventory

Gather: Entity/site IDs; organization functions; municipalities/counties; critical processes; asset and zone/conduit diagrams; dependencies and remote locations.

Responsible role: Organization PM and engineering

Purpose and boundary: Reuse the same inventory for state, local, privacy, environmental and gas applicability work.

AP04 Gather governing instruments

Gather: Current rules/orders/permits/contracts; coverage facts; versions and effective periods; unresolved interpretation; independent review needs.

Responsible role: Compliance owner and qualified advisers

AP05 Prepare safe evidence access

Gather: Evidence request index; record periods; custodians; redaction; approved secure transfer or supervised review; classification; retention/legal holds.

Responsible role: Evidence custodian and privacy/security lead

Purpose and boundary: Keep secrets, customer data, SSI and sensitive facility details in approved repositories; use references in the guide.

AP06 Identify operations and safety constraints

Gather: Service continuity limits; fragile/legacy systems; vendor restrictions; safety systems; change freezes; outage windows; emergency and stop contacts.

Responsible role: Operations, engineering and safety owners

Purpose and boundary: Preparation establishes boundaries, and test safety is confirmed by the qualified team during method approval.

AP07 Arrange participants and escalation

Gather: Sponsor; PM; operations/safety; IT/OT; physical security; legal; vendor contacts; deputies; available interview windows and escalation channels.

Responsible role: Organization PM

Purpose and boundary: Name actual people and their availability.

AP08 Prepare an exceptions and open questions register

Gather: Missing records; inaccessible sources; proposed exclusions with reasons; affected work; responsible owner; next action and planning target.

Responsible role: Organization PM and GDF lead

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

Purpose and boundary: A record still being located is a collection task, and substantive assessment decides whether any finding follows.

AP33 Review the preparation handoff

Gather: Missing information; owner/action list; agreed proposed scope and exclusions; approval documents still needed; secure evidence index and responsible reviewer.

Responsible role: Organization sponsor, PM and GDF engagement lead

Purpose and boundary: Use a documented handoff in place of a readiness score. The appropriate qualified team decides what work proceeds and on what terms.

Audit preparation

AP09 Confirm the audit basis

Gather: Audit purpose; criteria; period; populations; intended reliance; competence/independence; any actual regulator direction or appointment.

Responsible role: Sponsor, compliance and GDF audit lead

Purpose and boundary: The sponsor appoints the auditor, and the auditor forms the assurance opinion.

AP10 Assemble the audit evidence request

Gather: Policies; control ownership; relevant logs/tickets; prior findings; remediation evidence; sample populations and known missing periods.

Responsible role: Control owners and evidence custodians

Purpose and boundary: The auditor selects and evaluates evidence, and the control result comes from that evaluation.

AP11 Identify specialist interfaces

Gather: Privacy, pipeline safety, electrical/process safety, environmental and other specialist criteria; actual boundaries and referrals.

Responsible role: Compliance and specialist leads

AP12 Plan the audit handoff

Gather: Indexed records; open matters; interview schedule; agreed reporting recipients; factual review process; secure workpaper handling.

Responsible role: Organization PM and GDF audit lead

Purpose and boundary: The handoff supports the independent assessment and carries open questions forward.

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

Cybersecurity assessment preparation

AP13 Prepare the cyber architecture review

Gather: Current IT/OT diagrams; data flows; zones/conduits; remote/vendor access; cloud/shared service interfaces; legacy and unsupported assets.

Responsible role: IT/OT and engineering owners

Purpose and boundary: Identify proposed review boundaries and interfaces that need specialist attention.

AP14 Gather control and resilience records

Gather: Configuration exports through approved methods; access reviews; monitoring coverage; backups/restoration records; incident exercises and change history.

Responsible role: IT/OT control owners

Purpose and boundary: The assessor will determine evidence sufficiency and whether demonstrations are appropriate.

AP15 Agree assessment methods

Gather: Proposed record review/interviews; passive observation access; tooling/connection restrictions; lab versus production; approval and safety contacts.

Responsible role: GDF technical lead and operations

Active scans or demonstrations proceed under their own method specific approval.

AP16 Define intended assessment outputs

Gather: Expected architecture/control observations; risk context; coverage limits; remediation planning and retest arrangements.

Responsible role: Sponsor and assessment lead

Purpose and boundary: The assessment report reflects the actual work, and the security conclusions come from that report.

Physical security assessment preparation

AP17 Prepare an escorted site review plan

Gather: Facility boundaries; lawful access and escorts; visitor/contractor rules; photography restrictions; restricted, hazardous and shared areas.

Responsible role: Facility security, operations and safety

Purpose and boundary: An escorted walkthrough differs from an attempted physical intrusion.

AP18 Gather protective system records

Gather: Approved site plans; access/visitor records; key/badge management; alarm/CCTV coverage and retention; lighting, barriers, cabinets and guard arrangements.

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

Responsible role: Physical security and facilities owners

Purpose and boundary: Provide sensitive plans through an approved secure channel.

AP19 Map physical and cyber dependencies

Gather: Access control/CCTV networks; power and communications dependencies; control rooms and remote cabinets; incident escalation and outage effects.

Responsible role: Physical security and OT engineering

Purpose and boundary: Electronic protective systems can have OT and service continuity consequences.

AP20 Arrange observation and specialist referrals

Gather: Approved walkthrough times; escorts; safety induction; restricted observations; fire/life safety or engineering specialist referrals.

Responsible role: Facilities, safety and assessment lead

Purpose and boundary: Alarm activation, lock bypass, electrical work and safety system tests are each authorized separately, in the engagement itself.

Cyber penetration test preparation

AP21 Define the proposed cyber test objective

Gather: Business question; proposed target IDs and ownership; internal/external boundaries; exclusions; test environment; permitted proof limits.

Responsible role: Sponsor and GDF test lead

AP22 Gather written cyber testing authority

Gather: Signed engagement and asset specific authorization; third party/provider permissions; scope approvers; activity windows and revocation/stop authority.

Responsible role: Legal, system owners and test lead

AP23 Prepare rules of engagement

Gather: Approved and prohibited activities; target boundaries; source identifiers; credentials handling; rate/impact limits; contacts; incident versus test distinction; stop/recovery criteria.

Responsible role: GDF test lead, operations, security and legal

Purpose and boundary: Keep an approved, versioned ROE separate from unsigned preparation notes. Exploitation procedures belong to the signed ROE and the authorized test team.

AP24 Separate IT testing from production OT

Gather: Proposed lab/replica options; segmentation boundaries; fragile assets; vendor safety review; maintenance/outage plan and validated restoration arrangements where relevant.

Responsible role: OT operations, safety, vendor and test lead

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

Any live OT scanning, exploitation, denial of service test or control change is planned with the plant under its own written authorization and a qualified safety review.

AP25 Plan test communications and evidence

Gather: Monitoring/detection objectives; informed versus limited knowledge participants as expressly agreed; on call contacts; secure proof collection; data minimization and urgent escalation.

Responsible role: Security operations, privacy and test lead

Purpose and boundary: Record what is intentionally undisclosed and to whom; retain an authorized emergency controller able to stop the work.

AP26 Prepare cleanup and follow up requirements

Gather: Agreed removal/revocation inventory; restoration ownership; proof handling; report recipients; validation and retest scope; acceptance records.

Responsible role: System owners and test lead

Purpose and boundary: Preparation defines required follow up; actual cleanup and findings are documented by the authorized test team.

Physical penetration test preparation

AP27 Define the proposed physical exercise

Gather: Named sites/owners; specific objectives; proposed areas/times; exclusions; participants; permitted proof and stop authority.

Responsible role: Sponsor, facility owner and GDF test lead

Purpose and boundary: A physical penetration test is a separately authorized exercise with its own objectives and controls.

AP28 Gather physical test authorization

Gather: Written property/operating owner authority; shared site/landlord permissions; approved activities; emergency verification contacts and carry documentation.

Responsible role: Legal, facilities and exercise controller

Purpose and boundary: The authorization letter works within the law and the rights of third parties, and legal review settles the actual authority and its boundaries.

AP29 Agree physical safety and exclusions

Gather: No go hazardous/energized/confined/process areas; life safety and emergency egress; public interaction limits; restricted items; environmental/service consequences.

Responsible role: Safety, operations, physical security and test lead

Purpose and boundary: The signed rules of engagement set the permitted activities and address damage, forced entry, alarm disablement and contact with weapons, safety systems or live processes in writing.

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

AP30 Plan emergency deconfliction

Gather: Exercise controller; verified stop phrase/process; site/guard/police/emergency coordination where approved; unexpected real incident response and medical arrangements.

Responsible role: Exercise controller, legal and physical security

Purpose and boundary: Keep emergency roles clear, with notification and disclosure decisions agreed in writing.

AP31 Document permitted human interactions

Gather: Whether any social engineering interaction is proposed; specific consent/approvals, personnel protections, privacy/labor considerations, exclusions and escalation.

Responsible role: Legal, HR/privacy, sponsor and test lead

Purpose and boundary: Human interaction enters the exercise when it is expressly scoped and approved.

AP32 Prepare accountability and closeout

Gather: Participant/site access accountability; approved evidence limits; badge/key/item return; any equipment restoration; reporting, welfare and factual review arrangements.

Responsible role: Exercise controller and facility owner

Purpose and boundary: The authorized team records actual activities, recovery and findings after execution, and test results come from that record.

Methodology: NIST SP 800-115 and NIST SP 800-82 Rev. 3. The preparation tasks are GDF planning aids built on those methods.

State Coverage and the Research Each State Needs

The national set gives each state a starting source profile and a client research checklist. New Jersey has its own dedicated planning set; every other state starts from the profile below. The review register splits water and wastewater, electric, gas, manufacturing and transportation into separate state and sector records, so each one can be researched and decided on its own.

Comparable depth requires authenticated current instruments, entity and ownership thresholds and exclusions, reporting clocks and recipients, recurring duties, practical collection records, assessment boundaries, local and operator interfaces and documented qualified review. A state with guidance or a voluntary program is described in its own terms, distinct from a state with a statute.

Indiana and Maryland Water Updates

Indiana: Current IDEM guidance separates an annual assessment from certification every other year. Confirm the current statute text before you set a legal deadline. Read IDEM guidance.

Maryland: Current Environment §9-2705 reviewed October 17, 2026 applies to community water/sewerage systems serving over 3,300 customers. Other Subtitle 27 duties are reviewed separately. Read §9-2705.

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

The current national workbook, water manual and state companion reflect these points.

Maryland implementation update

MDE May 2026 guidance supplies secure submission instructions. Its Attachment 2 uses people rather than the customers threshold in §9-2705. Keep the statutory unit and record a clarification task for account eligibility, scope and filing timing. Guidance and current adopted criteria are kept distinct.

Additional State Source Notes

Idaho

What the source says: 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 are reviewed under their own statutes, permits and contracts.

Gather: Gather the actual agency or organizational relationship, dated adoption instrument, applicable policy version and exceptions. A statewide agency policy sets duties for the agencies it covers, and a private utility or manufacturer takes its duties from its own instruments.

- S12 Idaho ITS Information Security Policy Manual, version 4.0

Minnesota

What the source says: 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.

Gather: Gather PWS ID, actual OT use inventory, assessment date and scope, certifying person, annual certification and receipt. Request the current due date instruction and authority for the actual operator. Keep detailed assessment findings in the controlled repository. For other sectors, obtain the regulator's actual implementation instrument and coverage basis.

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

Missouri

What the source says: 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.

Gather: Gather legal entity, community water classification, internet connected control inventory, city population, charter county classification/population and PSC customer count with dates and sources. Review each section 640.142 exclusion separately before treating the plan duty as applicable. Gather the cyber risk plan, assessments and control decisions if applicable.

- S25 Missouri selected authority

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

Tennessee

What the source says: 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 clock are confirmed from the codified chapter. Obtain the current codified chapter 1220-04-15 from the Tennessee Secretary of State.

Gather: Gather TPUC jurisdiction/classification, actual filing direction, current chapter and amendments, annual filing and receipt, incident trigger criteria and approved confidential delivery method. Your deadlines and coverage come from the codified rule and your own filing direction, with docket titles and other utilities' submissions as context.

- S42 Tennessee selected authority
- S42D 2026 annual utility cybersecurity filing docket 26-00047

Texas

What the source says: 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 rule's specific electric entity and facility scope, which centers on emergency operations plans and their annexes. Reconcile the current codified text and later amendments.

Gather: Gather electric registration/entity type, facility functions and ERCOT footprint, current EOP and cyber/physical annexes, prior filing dates, material change assessment, current executive summary template, affidavit, training/distribution records and authorized delivery instructions. Gather drill or qualifying activation evidence, advance notifications and post drill revisions. Confirm later amendments before adopting the calendar.

- S43 Texas selected authority
- S43E Adopted electric emergency operations plan rule

What the selected source means for preparation

Sources reviewed October 17, 2026.

Maryland

Priority: First: correct a supported scope error and verify implementation

Coverage scope: Water/wastewater for these provisions; electric, gas, manufacturing and transportation are researched under their own instruments

What the source supports: Environment 9-2704 addresses cybersecurity contacts and annual training for all community water/sewerage providers. Section 9-2705 has a separate over-3,300 customer scope and an OT/IT maturity assessment by July 1, 2026, then every two years. The reviewed current 9-2705 text differs from the earlier version, which carried an additional vulnerability determination qualifier. That section places the assessment duty on the provider and leaves the choice of assessor open.

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

Gather: Record the legal provider, system definitions and actual customer count with date and basis. Gather contact appointment, training attendance, adopted standards and version, maturity assessment scope/results, improvement actions and zero trust implementation planning. Identify physical access and building/fire control systems where the statutory OT definition includes them.

Calendar boundary: 9-2706 assigns an October 1, 2026 and biennial collection/reporting duty to the state office. Section 9-2707 delegates incident circumstances, manner and time period to an established process.

Next step: Authenticate definitions incorporated from 9-401/9-501, amendment history, actual promulgated minimum standards, approved training and the May 2026 MDE secure submission instructions and current DoIT standards. Confirm the customers/people discrepancy and provider filing timing. Preserve the July 2026 historical assessment date; obtain actual completion evidence measured against that date.

Responsible role: Water compliance lead and CISO; counsel reviews scope and current implementation

Done when: Current operative instruments and implementation records authenticated; each duty mapped to its own scope/clock; utility facts documented; collection request reviewed.

- Definitions, 9-2701
- Department duties, 9-2702
- Contact/training, 9-2704
- Maturity assessment, 9-2705
- State collection duty, 9-2706
- Incident process, 9-2707

Indiana

Priority: First: authenticate the operative cadence before legal calendar approval

Coverage scope: Selected water/wastewater guidance.

What the source supports: IDEM currently describes annual vulnerability assessment beginning December 31, 2026 and certification every other year beginning that date. Authenticate the full current code next, and read the earlier digest as history, with any conflict confirmed from the current operative authorities.

Gather: Gather actual system type, population basis, computerized control use, assessment report and scope, remediation or mitigation planning, emergency plan, prior certifications and designated incident reporter records. Guidance identifies CWS serving 500 or more, POTWs and Class III/IV semipublic facilities with computerized monitoring/control. Confirm those facts against the operative statute before accepting scope.

Calendar boundary: Guidance separates operation impact incidents (24 hours after discovery) from those without operational impact (two business days), annual reporter contact and the assessment/certification cadences. These serve as guidance based planning leads, confirmed once current code and instructions are authenticated.

Next step: Obtain authenticated current IC 13-18-16.5 and amendments; reconcile the enacted text, current code, agency instructions and certification form version. Draft a focused written clarification where authenticated texts conflict.

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

Responsible role: Jurisdiction research lead and water compliance counsel; operator supplies actual records

Done when: Controlling cadence and scope supported by current operative text and implementation instructions, or a documented open interpretation with the affected decision held for clarification.

- IDEM implementation guidance
- IDEM assessment tools/timeline
- Official 2025 bill history/digest, read as history beside the current code

Delaware

Priority: Next: acquire underlying direction and current annual questionnaire

Coverage scope: PSC Class A utility reporting context; coverage of private manufacturers and transport operators is confirmed from their own instruments

What the source supports: The PSC program page describes annual DelaFile reports for Class A utilities containing staff questions and responses. It asks about IT/OT distinctions, audits, risk, recovery, training, remote access and privacy. Each question asks about a practice, and any specific penetration test or assessment frequency comes from an underlying binding instrument.

Gather: Gather actual utility classification, docket/order, current questionnaire, prior report and receipt, scope of corporate responses, IT/OT policies, risk register, training, third party access, recovery exercises and supporting evidence references. Keep security plans in the approved repository.

Calendar boundary: Annual reporting is described on the agency page. Specific due date, operative order, exemptions, confidential filing procedure and current question version are authenticated next.

Next step: Retrieve Docket 16-0659 operative direction and current filing instructions; separate each report question from an independently binding underlying duty.

Responsible role: Regulatory affairs lead with CISO and evidence custodians

Done when: Class A status, current operative reporting direction, date/version and secure filing procedure documented; each proposed response linked to operator evidence for later assessment.

- PSC cybersecurity program and questionnaire

Connecticut

Priority: Next: distinguish voluntary program from current utility specific directions

Coverage scope: 2016 utility collaboration plan; water DPH and other sector/operator requirements are researched separately

What the source supports: The reviewed 2016 PURA plan describes voluntary collaboration and annual review meetings. It describes Connecticut's program in its own voluntary terms, distinct from the mandate New Jersey imposes. Later orders, agreements and actual regulated entity coverage are reviewed separately.

Gather: Gather actual PURA/DPH entity status, participation agreements, meeting requests, prior review materials, risk/control evidence, improvement plans and current regulator correspondence. Record confidentiality restrictions and access conditions for the actual records.

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

Calendar boundary: Annual meetings in the historical plan are scheduled collaboration, recorded apart from any statutory assessment or penetration test deadline.

Next step: Inspect later PURA orders, recent program reports and actual utility specific directions; identify any independently applicable adopted rules. Resolve water, municipal, manufacturing and transportation interfaces separately.

Responsible role: Utility regulatory affairs lead and CISO; counsel confirms authority classification

Done when: Current obligations distinguished from voluntary participation and historical practice, with operator specific scope, records and review limits documented.

- PURA utility cybersecurity program
- 2016 collaboration plan

Florida

Priority: Next: identify county/municipal ownership and independent sector duties

Coverage scope: 2026 section 282.3185 local government scope; private operators are researched under their own instruments

What the source supports: The reviewed statute differentiates qualifying local government cyber incidents and ransomware notice. Its 48 hour and 12 hour discovery based windows address distinct triggers for the local governments it covers, and each Florida utility, manufacturer or transportation business takes its incident deadlines from its own governing instruments.

Gather: Gather legal ownership/governing entity, affected systems, event severity rationale, actual discovery times with zone, ransomware facts, incident escalation contacts, reporting records, training and the adopted program. Confirm current reporting instructions and concurrent operational/public health/federal duties.

Calendar boundary: Use the actual statutory coverage and trigger before assigning a window. Internal planning targets are separate from legal deadlines; simultaneous duties need independent decision records.

Next step: Map the current statute clause by clause, confirm the local government definition and incident categories, then retrieve utility, environmental, port/airport/transit, pipeline and contract specific instruments for the actual facility.

Responsible role: Local government legal/risk lead, CISO and sector operations representative

Done when: Covered entity and each reporting trigger supported by law and actual facts; current destinations, records and concurrent duties reviewed.

- 2026 Florida statute 282.3185

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

Starting Sources for Every State

Each state below lists the source to read first, as reviewed on October 17, 2026. Each starting source is read in its current version from the publisher listed. Treat that source as a starting point: water, wastewater, electric, gas, manufacturing and transportation each need their own applicability review, so retrieve the current clauses and any local or operator instruments for the actual facility, then record exclusions, amendment dates, reporting triggers and evidence requests in the five sector records. A water rule or a public agency policy sets duties for the organizations it names, and each other organization looks to its own instruments. The state and local research companion carries the full profile for each state.

Alabama

Starting source: ADEM agency guidance.

Alaska

Starting source: Alaska DEC agency guidance.

Arizona

Starting source: Arizona Legislature enacted law.

Arkansas

Starting source: Arkansas Division of Elementary and Secondary Education official implementation memo.

California

Starting source: California PUC regulator reporting page.

Colorado

Starting source: Colorado Secretary of State and PUC rule text.

Connecticut

Starting source: Connecticut DPH historical agency circular.

Delaware

Starting source: Delaware PSC regulator program.

Florida

Starting source: Florida Senate enacted law.

Georgia

Starting source: Georgia Technology Authority agency reporting source.

Hawaii

Starting source: Hawaii PUC regulator directory.

Idaho

Starting source: Idaho ITS Information Security Policy Manual, version 4.0.

Illinois

Starting source: Illinois General Assembly bill status, to be confirmed.

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

Indiana

Starting source: IDEM agency implementation guidance.

Iowa

Starting source: Iowa Utilities Commission utility rule.

Kansas

Starting source: Kansas Legislature enacted law.

Kentucky

Starting source: Kentucky PSC regulator reporting page.

Louisiana

Starting source: Louisiana Legislature.

Maine

Starting source: Maine Legislature enacted law.

Maryland

Starting source: Maryland General Assembly and MDE enacted sector law.

Massachusetts

Starting source: MassDEP agency program with scope review.

Michigan

Starting source: Michigan PSC regulator implementation source.

Minnesota

Starting source: Minnesota Department of Health agency expectation needing confirmation.

Mississippi

Starting source: Mississippi ITS agency reporting source.

Missouri

Starting source: Missouri Legislature enacted sector law.

Montana

Starting source: Montana Department of Administration agency guidance.

Nebraska

Starting source: Nebraska Information Technology Commission standards directory.

Nevada

Starting source: Nevada Legislature enacted law.

New Hampshire

Starting source: New Hampshire Legislature enacted sector law.

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

New Jersey

Starting source: New Jersey DEP and Legislature enacted sector framework.

New Mexico

Starting source: New Mexico DoIT policy directory and scope review.

New York

Starting source: New York DEC and DOH adopted sector rules.

North Carolina

Starting source: North Carolina DIT agency implementation guidance.

North Dakota

Starting source: North Dakota Legislature enacted law.

Ohio

Starting source: Ohio EPA operational reporting rule.

Oklahoma

Starting source: Oklahoma OMES agency reporting directory.

Oregon

Starting source: Oregon Legislature enacted law.

Pennsylvania

Starting source: Pennsylvania DEP and PUC guidance and rulemaking watchlist.

Rhode Island

Starting source: Rhode Island Legislature utility law.

South Carolina

Starting source: South Carolina DES agency guidance.

South Dakota

Starting source: South Dakota Legislature criminal statute only.

Tennessee

Starting source: Tennessee Secretary of State filed utility rule.

Texas

Starting source: Texas Legislature enacted utility law.

Utah

Starting source: Utah DEQ agency guidance.

Vermont

Starting source: Vermont Legislature.

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

Virginia

Starting source: Virginia Legislature enacted operational law.

Washington

Starting source: Washington Legislature enacted agency law.

West Virginia

Starting source: West Virginia Legislature enacted agency law.

Wisconsin

Starting source: Wisconsin DNR agency guidance.

Wyoming

Starting source: Wyoming ETS and PSC standards directory.

Workbook format and field preparation

The workbooks use consistent cell styles, fitted headers and Excel table definitions, and the master, selected and extended files open normally in Excel.

Use amber cells for intended entries. National and NY key instructions and formulas remain protected; row resizing is allowed. NJ uses unprotected tables, so save controlled versions. After choosing a Field record procedure in B5, recalculate and use Home > Format > AutoFit Row Height for rows 6 to 24. Adjust merged warning cells manually or attach a controlled continuation. Preview every printed page after adding longer notes.

The underlying Normal style can use a different fallback font for unformatted new cells; copy existing table formatting or apply Arial 11 with Wrap Text. Some retained reference PDFs use standard viewer fonts. The archive includes a workbook guide.

These materials prepare the record for an audit, a security assessment or a cyber or physical penetration test. The engagement itself, with its signed authorization, comes next.

Information Gathering Packages

Prepare the records and questions your specialist will ask for.

The packages cover DFS, New York privacy, CMMC and NIST, and EAR and ITAR.

Legal gathering guides address departed employees, contract disputes and medical matters.

- Information gathering packages

Web Addresses for the Sources Cited

1. NIST SP 800-115: https://csrc.nist.gov/pubs/sp/800/115/final

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

2. NIST SP 800-82 Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final
3. DFS cybersecurity resource page: https://www.dfs.ny.gov/cybersecurity
4. P08 CIP-012-2 communications between Control Centers: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-012-2.pdf
5. W12 NY drinking water cybersecurity Appendix 5-E: https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/appendix_5e.pdf
6. W13 NY drinking water cybersecurity FAQ and transition guidance: https://healthweb-back.health.ny.gov/environmental/emergency/water/drinking/cybersecurity/cybersecurity_faq.htm
7. Read IDEM guidance: https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/
8. Read §9-2705: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2705&enactments=false
9. MDE May 2026 guidance: https://mde.maryland.gov/programs/water/water_supply/Documents/SB871.pdf
10. 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
11. S23 Minnesota selected authority: https://www.health.mn.gov/communities/environment/emergency/water/securityassess.html
12. S23E Minnesota Executive Order 22-20: https://mn.gov/governor/assets/EO%2022-20_tcm1055-539386.pdf
13. S23A Minnesota Executive Order 24-07: https://www.lrl.mn.gov/archive/execorders/24-07.pdf
14. S23C Minnesota annual cyber assessment certification form: https://www.health.mn.gov/communities/environment/water/docs/cyberform.pdf
15. S25 Missouri selected authority: https://revisor.mo.gov/main/OneSection.aspx?section=640.142
16. S42 Tennessee selected authority: https://publications.tnsosfiles.com/rules_filings/06-31-23.pdf
17. S42D 2026 annual utility cybersecurity filing docket 26-00047: https://tpucdockets.tn.gov/dockets/2600047.htm
18. S43 Texas selected authority: https://tcss.legis.texas.gov/resources/UT/htm/UT.39.htm
19. S43E Adopted electric emergency operations plan rule: https://www.sos.state.tx.us/texreg/archive/December262025/Adopted%20Rules/16.ECONOMIC%20REGULATION.html
20. Definitions, 9-2701: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2701&enactments=false
21. Department duties, 9-2702: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2702&enactments=false
22. Contact/training, 9-2704: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2704&enactments=false
23. State collection duty, 9-2706: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2706&enactments=false
24. Incident process, 9-2707: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2707&enactments=false
25. IDEM assessment tools/timeline: https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/cybersecurity-risk-assessment-tools/
26. Official 2025 bill history/digest, read as history beside the current code: https://iga.in.gov/legislative/2025/bills/senate/459/details
27. PSC cybersecurity program and questionnaire: https://depsc.delaware.gov/cybersecurity/
28. PURA utility cybersecurity program: https://portal.ct.gov/pura/electric/cybersecurity-and-connecticut-public-utility-companies
29. 2016 collaboration plan: https://portal.ct.gov/-/media/PURA/ForAgencyLandingPage/cyber_report_April_6_2016.pdf
30. 2026 Florida statute 282.3185: https://www.flsenate.gov/Laws/Statutes/2026/282.3185
31. ADEM agency guidance: https://adem.alabama.gov/water/drinking-water-branch/information-public-water-systems/cybersecurity-resources-public-water-systems
32. Alaska DEC agency guidance: https://dec.alaska.gov/eh/dw/security/regulations/awia-regulations
33. Arizona Legislature enacted law: https://azleg.gov/ars/18/00552.htm
34. Arkansas Division of Elementary and Secondary Education official implementation memo: https://adecm.ade.arkansas.gov/ViewApprovedMemo.aspx?Id=4848
35. California PUC regulator reporting page: https://webproda.cpuc.ca.gov/regulatory-services/safety/emergency-reporting
36. Colorado Secretary of State and PUC rule text: https://www.sos.state.co.us/CCR/GenerateRulePdf.do?fileName=4+CCR+723-3&ruleVersionId=10399

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

37. Connecticut DPH historical agency circular: 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
38. Georgia Technology Authority agency reporting source: https://gta.georgia.gov/contact-us/cybersecurity-incidents
39. Hawaii PUC regulator directory: https://puc.hawaii.gov/about/statutes-rules-orders/
40. Illinois General Assembly bill status, to be confirmed: https://www.ilga.gov/Legislation/BillStatus?DocNum=3576&DocTypeID=HB&GAID=18&LegId=0&Print=1&SessionID=114
41. Iowa Utilities Commission utility rule: https://rules.iowa.gov/Notice/Details/8846C
42. Kansas Legislature enacted law: https://kslegislature.gov/b2023_24/laws/075_000_0000_chapter/075_072_0000_article/075_072_0044_section/075_072_0044_k/
43. Kentucky PSC regulator reporting page: https://psc.ky.gov/Home/UtilForms
44. Louisiana Legislature: https://legis.la.gov/
45. Maine Legislature enacted law: https://www.legislature.maine.gov/legis/statutes/35-A/title35-Asec710.html
46. Maryland General Assembly and MDE enacted sector law: https://mgaleg.maryland.gov/2025RS/chapters_noln/Ch_495_sb0871T.pdf
47. MassDEP agency program with scope review: https://www.mass.gov/info-details/public-drinking-water-system-operations
48. Michigan PSC regulator implementation source: https://www.michigan.gov/mpsc/regulatory/emergency-management/utility-incident-notification-procedures
49. Mississippi ITS agency reporting source: https://www.its.ms.gov/services/security/Enterprise-Cybersecurity-Incident-Reporting
50. Missouri Legislature enacted sector law: https://revisor.mo.gov/main/OneSection.aspx?bid=48367&section=640.142
51. Montana Department of Administration agency guidance: https://doa.mt.gov/SITSD/cybersecurity
52. Nebraska Information Technology Commission standards directory: https://nitc.nebraska.gov/standards-and-guidelines/
53. Nevada Legislature enacted law: https://www.leg.state.nv.us/nrs/nrs-480.html
54. New Hampshire Legislature enacted sector law: https://gc.nh.gov/rsa/html/L/485/485-3-e.htm
55. New Jersey DEP and Legislature enacted sector framework: https://dep.nj.gov/watersupply/drinking-water-systems/water-quality-accountability-act/
56. New Mexico DoIT policy directory and scope review: https://www.doit.nm.gov/about/doit-act-policies-and-rules
57. New York DEC and DOH adopted sector rules: https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources
58. North Carolina DIT agency implementation guidance: https://it.nc.gov/programs/cybersecurity-risk-management/cyber-incident-reporting
59. North Dakota Legislature enacted law: https://ndlegis.gov/cencode/t54c59-1.pdf
60. Ohio EPA operational reporting rule: https://codes.ohio.gov/ohio-administrative-code/rule-3745-81-31
61. Oklahoma OMES agency reporting directory: https://www.oklahoma.gov/omes/divisions/information-services/about-information-services/it-statutory-and-regulatory-reporting.html
62. Oregon Legislature enacted law: https://www.oregonlegislature.gov/bills_laws/ors/ors276a.html
63. Pennsylvania DEP and PUC guidance and rulemaking watchlist: https://www.pa.gov/agencies/dep/programs-and-services/water/bureau-of-safe-drinking-water/cybersecurity
64. Rhode Island Legislature utility law: https://webserver.rilegislature.gov/statutes/title39/39-2/39-2-26.htm
65. South Carolina DES agency guidance: https://www.des.sc.gov/programs/bureau-water/water-utilities-cybersecurity
66. South Dakota Legislature criminal statute only: https://sdlegislature.gov/Statutes/22-34-28
67. Utah DEQ agency guidance: https://deq.utah.gov/general/cybersecurity
68. Vermont Legislature: https://legislature.vermont.gov/
69. Virginia Legislature enacted operational law: https://law.lis.virginia.gov/vacode/title32.1/chapter6/section32.1-174.5/
70. Washington Legislature enacted agency law: https://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.470
71. West Virginia Legislature enacted agency law: https://code.wvlegislature.gov/5a-6B-4/
72. Wisconsin DNR agency guidance: https://dnr.wisconsin.gov/topic/DrinkingWater/cybersecurity.html
73. Wyoming ETS and PSC standards directory: https://ets.wyo.gov/resources/policies-standards/security-privacy

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

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.