GLOBAL DIGITAL FORENSICS

New Jersey Utility OT Audit Preparation Manual

Water and wastewater, electric and gas utilities

Edition 2026-11-03 | November 3, 2026

> Prepare the entity scope, records, permissions and open questions an operational technology audit or assessment needs, with the New Jersey and federal duties that set each reporting clock.
>
> Use with the NJ Utility Audit Preparation workbook and the CSV work records in this set.

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

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

Contents

1. How to use this set
2. Preparation tracks for the proposed engagement
3. The New Jersey decisions that need particular care
4. Project walkthrough and gates
5. Information gathering checklist
6. Candidate criteria and applicability
7. Procedure starters and field boundaries
8. Reporting triggers
9. Recurring and event based duty calendar
10. Questions to resolve before scope is final
11. Sources
12. Talk to a senior examiner

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

1. How to use this set

What this set is for

This set prepares a New Jersey water, wastewater, electric or gas utility for a cybersecurity audit or assessment of its operational technology. The manual explains each record and why an examiner asks for it. The workbook is where your team assigns owners, planned dates and secure evidence references, and the CSV files carry the same registers for teams that work outside Excel.

Start with the entity and the facility

New Jersey duties attach to the legal owner or operator of a particular system, and one utility can sit under several regimes at once: the Board of Public Utilities cyber security order and reporting rule, the Water Quality Accountability Act, NJPDES permit conditions, the federal AWIA program, NERC CIP standards, pipeline safety rules, TSA security directives and the state breach and privacy laws. Record the facts that decide each one, such as service connections, population served, registered NERC functions and the gas operator identifier, before you assign a duty. Mark each criterion Applies, Excluded with reason or To decide in the Criteria sheet, with the basis and the person who decided.

Gather records before field work

Section 3 lists what to collect for an audit, a cybersecurity assessment, a physical security assessment and cyber or physical penetration testing, and who usually holds each record. Section 5 lists the records an examiner asks for first. Put secure references in the workbook rather than copying passwords, network diagrams, security sensitive information or personal data into it.

Keep the plant safe

Begin with documents, interviews and passive observation. Scanning, credential testing, configuration or logic changes, failover and any action that could affect the process proceed with written permission from the operating owner, operations and safety leads and the vendor where needed, with a named person who can stop the work and an agreed recovery plan.

Sources and currency

Every criterion, procedure, reporting trigger and calendar entry carries source identifiers, and section 11 lists each source with a link. The research behind this edition runs through October 17, 2026. The Water Quality Accountability Act, the Board reporting rule, the public agency reporting law, the breach notice law, the TSA pipeline directives and the NERC CIP versions were checked again on November 3, 2026. New Jersey agencies amend these rules often, so confirm the current text before you sign a scope decision.

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

2. Preparation tracks for the proposed engagement

Use this set to define the proposed engagement, gather and organize the records an examiner will ask for, list the information that is still missing and arrange the permissions an audit or assessment needs.

An audit, a control assessment, a physical review and an attempted intrusion are different engagements, so the tasks below are grouped by the work being proposed. Common tasks apply to every engagement.

Common preparation for every engagement

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP01	Define the preparation brief	An audit, control review and penetration test answer different questions; preparation identifies the requested work.	Requested service and decision; facilities or entities; intended users; proposed period; known exclusions; deliverables and assessment limitations.	Sponsor and GDF engagement lead	Before agreeing engagement scope
AP02	Identify owners and authority	Ownership, access and testing authority can belong to different parties.	Legal asset or site owners; operating authority; landlord or shared site rights; third party, cloud or vendor approval requirements; actual approvers.	Utility legal and operating owners	Before access or method approval
AP03	Organize one facility and system inventory	Reuse the same inventory for state, local, privacy, environmental and gas applicability work.	Entity or site IDs; utility functions; municipalities or counties; critical processes; asset and zone or conduit diagrams; dependencies and remote locations.	Utility PM and engineering	Before assessment planning
AP04	Gather governing instruments		Current rules, orders, permits or contracts; coverage facts; versions and effective periods; unresolved interpretation; independent review needs.	Compliance owner and qualified advisers	Before criteria approval
AP05	Prepare safe evidence access	Keep secrets, customer data, SSI and sensitive facility details in approved repositories; use references in the guide.	Evidence request index; record periods; custodians; redaction; approved secure transfer or supervised review; classification; retention or legal holds.	Evidence custodian and privacy or security lead	Before sharing records
AP06	Identify operations and safety constraints	Preparation sets the boundaries the safety review approves.	Service continuity limits; fragile or legacy systems; vendor restrictions; safety systems; change freezes; outage windows; emergency and stop contacts.	Operations, engineering and safety owners	Before approving any site visit or technical method

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

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP07	Arrange participants and escalation	Name the people and confirm their availability.	Sponsor; PM; operations or safety; IT/OT; physical security; legal; vendor contacts; deputies; available interview windows and escalation channels.	Utility PM	Before kickoff
AP08	Prepare an exceptions and open questions register	A missing record is a collection issue until substantive assessment establishes a finding.	Missing records; inaccessible sources; proposed exclusions with reasons; affected work; responsible owner; next action and planning target.	Utility PM and GDF engagement lead	During preparation and at scope review
AP33	Review the preparation handoff	Use a documented handoff. The appropriate qualified team decides what work can proceed and what limitations apply.	Missing information; owner or action list; agreed proposed scope and exclusions; approval documents to collect; secure evidence index and responsible reviewer.	Utility sponsor, PM and GDF engagement lead	Before agreeing or starting an assessment

Audit preparation

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP09	Confirm the audit basis		Audit purpose; criteria; period; populations; intended reliance; competence or independence; any actual regulator direction or appointment.	Sponsor, compliance and GDF audit lead	Before an audit engagement is represented as agreed
AP10	Assemble the audit evidence request	The auditor selects and evaluates the evidence you locate.	Policies; control ownership; relevant logs or tickets; prior findings; remediation evidence; sample populations and known missing periods.	Control owners and evidence custodians	Before assessor sampling is finalized
AP11	Identify specialist interfaces		Privacy, pipeline safety, electrical or process safety, environmental and other specialist criteria; actual boundaries and referrals.	Compliance and specialist leads	Before agreeing audit conclusions
AP12	Plan the audit handoff	The handoff supports the independent assessment and preserves unanswered questions.	Indexed records; open matters; interview schedule; agreed reporting recipients; factual review process; secure workpaper handling.	Utility PM and GDF audit lead	Before audit kickoff

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

Cybersecurity assessment preparation

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP13	Prepare the cyber architecture review	Identify proposed review boundaries and interfaces that need specialist attention.	Current IT/OT diagrams; data flows; zones or conduits; remote or vendor access; cloud or shared service interfaces; legacy and unsupported assets.	IT/OT and engineering owners	Before assessment scope review
AP14	Gather control and resilience records	The assessor will determine evidence sufficiency and whether demonstrations are appropriate.	Configuration exports through approved methods; access reviews; monitoring coverage; backups or restoration records; incident exercises and change history.	IT/OT control owners	Before evidence examination
AP15	Agree assessment methods	Arrange permission for passive access and method specific approval for active scans or demonstrations.	Proposed record review or interviews; passive observation access; tooling or connection restrictions; lab versus production; approval and safety contacts.	GDF technical lead and operations	Before any connection or technical activity
AP16	Define intended assessment outputs	The assessment report will reflect actual work; the preparation guide provides no security verdict.	Expected architecture or control observations; risk context; coverage limits; remediation planning and retest arrangements.	Sponsor and assessment lead	Before engagement agreement

Physical security assessment preparation

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP17	Prepare an escorted site review plan	An escorted walkthrough differs from an attempted physical intrusion.	Facility boundaries; lawful access and escorts; visitor or contractor rules; photography restrictions; restricted, hazardous and shared areas.	Facility security, operations and safety	Before a site visit
AP18	Gather protective system records	Provide sensitive plans through an approved secure channel.	Approved site plans; access or visitor records; key or badge management; alarm/CCTV coverage and retention; lighting, barriers, cabinets and guard arrangements.	Physical security and facilities owners	Before physical assessment planning
AP19	Map physical and cyber dependencies	Electronic protective systems can have OT and service continuity consequences.	Access control/CCTV networks; power and communications dependencies; control rooms and remote cabinets; incident escalation and outage effects.	Physical security and OT engineering	Before defining assessment boundaries
AP20	Arrange observation and specialist limits	The preparation plan authorizes no alarm activation, lock bypass, electrical work or safety system test.	Approved walkthrough times; escorts; safety induction; restricted observations; fire or life safety or engineering specialist referrals.	Facilities, safety and assessment lead	Before fieldwork scheduling

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

Cyber penetration test preparation

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP21	Define the proposed cyber test objective	List every target explicitly, including any adjacent IT, vendor or OT system in scope.	Business question; proposed target IDs and ownership; internal or external boundaries; exclusions; test environment; permitted proof limits.	Sponsor and GDF test lead	Before drafting rules of engagement
AP22	Gather written cyber testing authority	Penetration testing starts once written authorization is signed.	Signed engagement and asset specific authorization; third party or provider permissions; scope approvers; activity windows and revocation or stop authority.	Legal, system owners and test lead	Before any testing
AP23	Prepare rules of engagement	Keep an approved, versioned rules of engagement separate from unsigned preparation notes. This checklist supplies no exploitation procedure.	Approved and prohibited activities; target boundaries; source identifiers; credentials handling; rate or impact limits; contacts; incident versus test distinction; stop or recovery criteria.	GDF test lead, operations, security and legal	Before test plan approval
AP24	Separate IT testing from production OT	Keep IT testing inside the IT boundary agreed in writing. Live OT scanning, exploitation, denial of service and control changes are scoped separately and authorized in writing by the operating owner after qualified safety review.	Proposed lab or replica options; segmentation boundaries; fragile assets; vendor safety review; maintenance or outage plan and validated restoration arrangements where relevant.	OT operations, safety, vendor and test lead	Before authorizing any OT adjacent method
AP25	Plan test communications and evidence	Record what is intentionally undisclosed and to whom; retain an authorized emergency controller able to stop the work.	Monitoring or detection objectives; informed versus limited knowledge participants as expressly agreed; on call contacts; secure proof collection; data minimization and urgent escalation.	Security operations, privacy and test lead	Before test commencement
AP26	Prepare cleanup and follow up requirements	Preparation defines required follow up; actual cleanup and findings are documented by the authorized test team.	Agreed removal or revocation inventory; restoration ownership; proof handling; report recipients; validation and retest scope; acceptance records.	System owners and test lead	Before closing the agreed test plan

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

Physical penetration test preparation

ID	Task	Why it matters	Records to gather	Who usually holds them	Needed before
AP27	Define the proposed physical exercise	A physical penetration test is a separately authorized exercise with its own scope and escorts.	Named sites or owners; specific objectives; proposed areas or times; exclusions; participants; permitted proof and stop authority.	Sponsor, facility owner and GDF test lead	Before drafting physical test rules of engagement
AP28	Gather physical test authorization	Third parties sign their own authorizations. Legal review resolves the actual authority and limits.	Written property or operating owner authority; shared site or landlord permissions; approved activities; emergency verification contacts and carry documentation.	Legal, facilities and exercise controller	Before any attempted entry or interaction
AP29	Agree physical safety and exclusions	The exercise stays clear of damage, forced entry, alarm disablement, weapons, safety systems and live processes.	Restricted hazardous, energized, confined or process areas; life safety and emergency egress; public interaction limits; restricted items; environmental or service consequences.	Safety, operations, physical security and test lead	Before approving the exercise
AP30	Plan emergency deconfliction	Agree notification and disclosure decisions in writing before the exercise. You send any notification through your own channels.	Exercise controller; verified stop phrase or process; site, guard, police or emergency coordination where approved; unexpected real incident response and medical arrangements.	Exercise controller, legal and physical security	Before the exercise
AP31	Document permitted human interactions	Human interaction is covered where the signed scope lists it and the sponsor approves it. Record only the employee details the exercise needs.	Whether any social engineering interaction is proposed; specific consent or approvals, personnel protections, privacy or labor considerations, exclusions and escalation.	Legal, HR/privacy, sponsor and test lead	Before approving any interaction scenario
AP32	Prepare accountability and closeout	The authorized team records actual activities, recovery and findings after execution; preparation creates no successful test claim.	Participant or site access accountability; approved evidence limits; badge, key or item return; any equipment restoration; reporting, welfare and factual review arrangements.	Exercise controller and facility owner	Before approving the exercise plan

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

3. The New Jersey decisions that need particular care

Water: count connections and people separately

The Water Quality Accountability Act covers any person that owns a public community water system with more than 500 service connections (N.J.S.A. 58:31-2), so a system with exactly 500 connections is outside it. The federal AWIA risk and resilience assessment and emergency response plan duties apply to community water systems serving more than 3,300 people. Screen wastewater only service under its NJPDES permit conditions.

Sources: NJ03; F01

Water: a covered purveyor reports promptly

A covered water purveyor keeps a cybersecurity program that covers all of its industrial control systems and reasonably conforms to the NIST Cybersecurity Framework, the CIS Critical Security Controls or the ISO/IEC 27000 series, joins NJCCIC and keeps an incident reporting process (58:31-4 and 4.1). It reports a qualifying incident to NJCCIC promptly after an employee is made aware of it (58:31-4.2(a)). The 30 days in 58:31-4.2(b) is the period within which NJCCIC causes an independent audit of the program after receiving a report, at the purveyor’s expense. The DEP implementation page summarizes the reporting duty differently; plan around prompt notice and ask DEP to confirm in writing.

Sources: NJ03; NJ04

Every applicable clock runs on its own

The Board six hour report under N.J.A.C. 14:3-6.7(a), the prompt water report to NJCCIC, the 72 hour report a public agency or government contractor makes to the Office of Homeland Security and Preparedness, the resident breach notice (with the State Police report first under 56:8-163(c)(1)), permit and physical release notices, and federal or operator duties can all apply to one event. Each has its own trigger and recipient, so plan for the earliest applicable deadline.

Sources: NJ01; NJ02; NJ03; NJ05; NJ06; NJ12

Electric: name the NERC CIP versions in effect

FERC Order No. 919, effective May 26, 2026, approved CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3. They take effect on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after the order took effect, and entities may adopt them early, so record which version governs each audit period. CIP-015-1, approved by Order No. 907, requires internal network security monitoring from October 1, 2028 for high impact BES Cyber Systems and medium impact Control Centers, and 24 months later for other medium impact systems with External Routable Connectivity. Track the Board order duties alongside NERC compliance.

Sources: F02; F19; F20; NJ01

Gas: separate state, federal and TSA duties

Separate the New Jersey incident dates from the federal discovery, confirmed discovery, determination and exceedance dates. The state incident notice and follow up, the federal incident notice and update, safety related condition reports and MAOP reports have distinct triggers. Pipeline owners and operators notified by TSA are also subject to Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, and the reporting directive Pipeline-2021-01G.

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

Sources: NG01; NG02; NG03; F09

Gas: drill calendars

The adopted New Jersey distribution rule spaces district or division drills at least two weeks apart. Distribution and transmission drills have different cycles, field participation, notice and reporting conditions; the Calendar sheet keeps them as separate records.

Sources: NG01

Framework and audit distinctions

The water law names the NIST Cybersecurity Framework, the CIS Controls or the ISO/IEC 27000 family; NIST SP 800-82 supports the work as OT guidance. At a covered utility chemical facility, run the New Jersey TCPA annual audit on its annual cycle alongside the OSHA PSM three year cycle.

Sources: NJ03; NJ10; F03; F06

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

4. Project walkthrough and gates

Agree the objective, intended users, report basis, criteria and period, examiner competence and independence, deliverables and evidence handling before detailed audit design. Where a regulator directs an independent audit, record the direction and the trigger.

ID	Stage	Role to assign	Inputs	Exit condition	Timing	Procedures
M01	Initiate	Sponsor, legal or compliance, GDF engagement lead	Charters, instruments, engagement and independence	Agreed objective or assurance basis, accountable entity and scope; unresolved criteria named	Before detailed audit design	P01; P02
M02	Gather and resolve	PM and criteria owners	Checklist and Open questions	Every critical gap has an owner or evidence request; no unsourced coverage conclusion	Before criteria approval	P01; P09; applicable water, electric, gas and common procedures; P58 through P63 for gas
M03	Design	GDF engagement lead and operations or safety	Approved criteria, rules of engagement, population or sample design	Named approvers authorize actual methods; stop authority and repository ready	Before fieldwork	P02; P34
M04	Execute	Named examiners and collectors	Actual execution and evidence records	Contemporaneous observations, attribution, limits and evidence quality	Within approved window	Individually selected and authorized procedures from this set
M05	Review	Actual reviewer, legal or criteria specialists	Complete workpapers and facts	Criterion, condition, evidence or implication reconciled; missing/to be determined/future dates rejected	Before draft report	P34; P35; P43
M06	Correct and retest	Control owner, authorized retester, closure approver	Remediation and retest evidence	Chronological actual actions; remaining risk or mandatory duty distinguished	Agreed project dates	P35
M07	Handover	Sponsor, GDF engagement lead and signatories	Report, limitations, filing support, receipt	Every compliance statement is supported by evidence; open matters and recurring calendar assigned	Before engagement close	P14; P18; P35

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

5. Information gathering checklist

Every record starts as To gather in the Gathering sheet. Assign an owner, a planned date and a secure reference, and record the next action. Scope critical records decide which duties apply, so collect those first.

ID	Record to gather	Sector	Gate	Procedures
G01	Legal owner, operator, charter and affiliate or contract boundaries	All	Scope critical	P01
G02	Each facility, county, municipality, permit/registration/PWS ID	All	Scope critical	P01; P33
G03	BPU jurisdiction decision, operative orders and current rule text	Utilities	Criteria critical	P01
G04	Community classification, dated service connections and population as separate records	Water	Scope critical	P15
G05	Chosen framework, version or final publication date and revision or submission trail	Water	Criteria critical	P16
G06	NJCCIC membership, program or annual filing receipts and insurance review	Water	Evidence required	P17
G07	Full NJPDES permit or modifications and current reporting categories	Wastewater	Criteria critical	P20
G08	NERC registration or functions, categorization and separate control center scope	Electric	Criteria critical	P21
G09	Chemical/SDS inventory, threshold calculations, registration, TCPA/PSM/RMP criteria	Utilities	Criteria critical	P23
G11	Current local orders, permits or contracts, approved emergency contacts and notice channels	All	Criteria critical	P09; P33
G12	Customer/employee/AMI data map, resident roles or counts and processor contracts	All	Scope critical	P10; P32
G13	Signed engagement, competence or independence review and approved report basis	All	Fieldwork gate	P02
G14	Approved rules of engagement, operations, safety or vendor permissions, stop authority and rollback	All	Fieldwork gate	P02
G15	Current OT/IT inventory, zone or conduit map, legacy or protocol restrictions and dependencies	All	Evidence required	P03; P04
G16	Risk methodology, annual reviews or treatments and actual risk acceptance authority	All	Evidence required	P05
G17	Redacted monitoring, remote access, patch or change and training records	All	Evidence required	P06; P07; P08; P13
G18	IR/recovery plans, isolated restore evidence, exercises and corrective records	All	Evidence required	P11; P12
G19	Population, period, selection method or rationale and coverage limits for each procedure	All	Execution gate	P34
G20	Controlled repository, evidence IDs/classification/retention/collector and source times	All	Execution gate	P34
G21	Actual examiner or reviewer, observations, evidence, execution or review dates and disposition	All	Review gate	P34

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

ID	Record to gather	Sector	Gate	Procedures
G22	Findings, corrective owners or dates, authorized retest and independent closure approval	All	Handover gate	P35
G23	Approved identity or role, remote access, boundary, configuration and engineering change records	All	Evidence required	P36; P37; P38; P39
G24	Portable device or media inventory, critical supplier terms and shared service responsibilities	All	Evidence required	P40; P41
G25	Escorted physical walkthrough permission, access, power or environment records and specialist scope	All	Fieldwork gate	P42
G26	Workpaper cross reference, evidence integrity or custody, retention or legal holds and secure handover	All	Review gate	P43
G27	Actual nuclear license or status, exemptions or orders, approved cybersecurity plan and specialist criteria, where indicated	Electric	Criteria critical	P44
G28	Gas control room functions, full or limited applicability facts, current 192.631 paragraphs and lawfully accessed incorporated standards. Hazardous liquid operations require a separately scoped specialist review.	Gas	Criteria critical	P45
G29	EDC/AMI roles; meter to bill data lineage; validated or local data populations and actual PJM milestone	Electric	Scope critical	P46
G30	Current Board third party eligibility order or list, Common Release Form, MFA, consent, decline or revocation and onward recipient records	Electric	Criteria critical	P47
G31	AMI authorization or transmission timestamp exports, rolling history/API/portal records and data field map	Electric	Evidence required	P46; P47
G32	AMI release response recipients or sequence, developer change notices, nine metric semiannual instructions and receipts	Electric	Evidence required	P48; P49
G33	LDC/TPS role, current customer or error populations, reporting calculations and future supplier freeze project/EDI evidence	Utilities	Criteria critical	P50
G34	Actual drinking water emergency or planned change criteria, onset or call records, operator or engineer and asset program filings	Water	Criteria critical	P51
G35	Actual hazardous substance capacities, current appendices, major facility or pipeline determination and approved DPCC/DCR plans	All	Scope critical	P52
G36	Discharge detection, monitoring, prevention or safety device map, malfunction, knowledge, notice or two hour disposition records	All	Evidence required	P52
G37	TCPA current federal or state clause crosswalk, approved consent anniversary, annual audit or report and NJRMP change or ownership receipts	Utilities	Criteria critical	P56
G38	NJDPA purpose, data, age or acquisition map, actual exemptions, rights or appeal population and dated responses	All	Evidence required	P53; P54
G39	Consent, revocation or cessation records, high risk assessments, minimization or safeguard evidence and processor or subprocessor terms	All	Evidence required	P54; P55
G40	Calendar for each recurring or event based duty: applicable instrument, actual trigger or last event, owner or deputy, next due basis and receipt	All	Review gate	P09; P14; P49; P50; P51; P56

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

ID	Record to gather	Sector	Gate	Procedures
G41	DER/CIAP current chapter or readoption, Board orders, actual implementation or tariff, platform security, uptime or workflow evidence	Electric	Criteria critical	P57
G42	Exact 6.10 event category, receiving DTW, initial or revised oral notice, written follow up, bypass or serious violation records and actual permit	Wastewater	Evidence required	P20
G43	Legal gas operator/OPID, current gas service or pipeline instruments and interstate or intrastate, distribution/transmission/storage/LNG and CRM scope facts.	Gas	Resolve scope or current instruments before design; gather approved evidence before execution or review.	P58; P29; P45
G44	Gas event classifications, current reporting channels, distinct actual event, discovery, learning or confirmed discovery or determination times, initial, update or final receipts and deputy contacts.	Gas	Resolve scope or current instruments before design; gather approved evidence before execution or review.	P59
G45	Complete district or division, call or dispatch and transmission drill histories, field or tabletop locations, spacing, advance notices, evaluations and reports.	Gas	Resolve scope or current instruments before design; gather approved evidence before execution or review.	P60
G46	Secure gas pressure, temperature or alarm records, independent time or calibration corroboration, MAOP/device margin basis, approved changes and qualified safety reviewer.	Gas	Resolve scope or current instruments before design; gather approved evidence before execution or review.	P61
G47	Applicable state or federal filing inventory, current forms and thresholds, annual, leak or pressure test source data, reporting periods, actual receipts and corrections.	Gas	Resolve scope or current instruments before design; gather approved evidence before execution or review.	P62

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

ID	Record to gather	Sector	Gate	Procedures
G48	Gas interruption population, affected customer, season, road or critical facility facts, actual start and awareness times, contract exclusion basis, prompt written follow up and any incident corrective action amended report.	Gas	Before reporting matrix approval and historical event review.	P63; P59

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

6. Candidate criteria and applicability

These are the duties a New Jersey utility audit usually has to settle. Record each decision in the Criteria sheet as Applies, Excluded with reason or To decide, with the facts, the source, the person who decided and the date. Add clause level rows where your instruments require them.

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C01	Board jurisdiction	Electric, gas, water or wastewater entities potentially within BPU jurisdiction	Determine the legal entity, regulated service, governing orders and system boundary before assigning NJ01 duties.	Legal entity charter; BPU docket or order history; service territory; ownership; affiliate or shared service map.	NJ01; NJ14 (Order scope and critical system definition)
NJ-C02	Critical system inventory	NJ01-covered entity or systems	Review critical ICS/SCADA and customer personal information systems inventory annually and document changes.	Dated inventory, responsible owner, customer data classification, annual review and changes.	NJ01 (Requirements 1(a))
NJ-C03	Annual risk process	NJ01-covered entity or systems	Conduct and document annual risk assessment or prioritization, methodology and review, including physical risk, vulnerabilities, current threats and recovery or continuity considerations.	Risk assessment, criteria, methodology review, treatment decisions and annual records.	NJ01 (Requirements 1(b)-(d))
NJ-C04	Monitoring and threat review	NJ01-covered entity or systems	Use risk based critical system log monitoring and a process to evaluate relevant internal, external or vendor threat and vulnerability information.	Log sources, monitoring rationale, review records, threat advisories and applicability decisions.	NJ01 (Requirements 2(a)-(b))
NJ-C05	Patch decisions	NJ01-covered entity or systems	Review vendor patches in a timely manner and implement as appropriate; record risk, compatibility and compensating controls. Set patch timing through the order's risk based process.	Vendor notices, OT test or maintenance approvals, deferment rationale and safeguards.	NJ01 (Requirements 2(c))
NJ-C06	ICS event notices	NJ01-covered entity with qualifying ICS event	Evaluate the order defined access, unauthorized code or commands and extortion events; reporting path through NJCCIC to designated Board staff is within six hours of detection.	Detection facts, defined event match, time zone, current recipients or channel, receipt.	NJ01 (Requirements 3(a)(i)-(iv))
NJ-C07	Other cyber and customer data notices	NJ01-covered entity	Evaluate unusual cyber activity with potential critical system compromise and Board copies of statutorily required customer-PI law enforcement notices as separate duties.	Event scope, law enforcement notice determination, Board copy and acknowledgement.	NJ01; NJ06 (Requirements 3(b)-(c); 56:8-163)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C08	Response and exercise	NJ01-covered entity or systems	Maintain response lifecycle and forensic log retention arrangements; exercise at least once every 24 calendar months, with documented lessons and program updates. A qualifying actual incident may satisfy the order exercise provision.	Plan, recovery roles, retention rationale, exercise or incident evidence, lessons and closure.	NJ01 (Requirements 4(a)-(b))
NJ-C09	Training and awareness	NJ01-covered personnel	Review general awareness, continuing communications, role training and new personnel training. The order uses biannually for program review; obtain a written interpretation rather than silently choosing a frequency.	Training matrix, course records, credential holder coverage, actual review frequency and clarification.	NJ01 (Requirements 5(a)-(d))
NJ-C10	Annual executive certification	NJ01-covered entity	Annual authorized executive certification is due December 31 after historical implementation. NERC certification may satisfy the annual certification for the overlapping CIP covered critical systems, and the other NJ duties and systems keep their own certification.	Signed certification, scope, receipt; exact NERC overlap and Board acceptance if used.	NJ01 (Accountability 1-3)
NJ-C11	Service impact cyber reporting	Public utility within operative Chapter 14:3 scope	2022 adopted 14:3-6.7(a)6-7 requires Board reporting within six hours of awareness for listed cyber attacks and attempted intrusions with the specified service impact conditions. Authenticate current code and later amendments.	Actual intrusion or outage facts, awareness timeline, consolidated rule, recipients, receipts.	NJ02; NJ14; NJ15 (14:3-6.7(a)6-7)
NJ-C12	WQAA threshold	Owner of a public community water system with more than 500 service connections	Use service connections and system classification; coverage starts at 501 connections. Apply the WQAA connection count on its own, separate from the AWIA population test, and screen wastewater only systems separately.	PWS ID, community classification, owner and dated service connection count or source.	NJ03 (58:31-2)
NJ-C13	Program coverage and accountability	WQAA covered purveyor	Maintain accountable cybersecurity program, risk management, threat awareness, exercised response or recovery and coverage of all ICS. Former internet connected system exemption was deleted.	Chief responsible individual; program; full ICS boundary; risk or treatment and exercise records.	NJ03 (58:31-4(a)-(c); -4.1(a))
NJ-C14	Chosen framework and revision	WQAA covered purveyor	Reasonably conform to at least one listed framework family: NIST CSF, CIS Critical Security Controls or ISO/IEC 27000. A final revision to the chosen framework triggers revision and NJCCIC submission within 180 days.	Selected framework or version, final publication date, controls mapping, revision decisions and submission receipts.	NJ03; F12 (58:31-4.1(a)-(b))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C15	Membership, reporting process and insurance	WQAA covered purveyor	Confirm NJCCIC membership, incident reporting process and cyber insurance meeting applicable Board standards; verify historic compliance rather than restarting expired 2017/2021 transition periods.	Membership receipt, current reporting instructions, policy, declarations, limits or exclusions, applicable insurance standard.	NJ03 (58:31-4(b),(d))
NJ-C16	Annual certification and portal deliverables	WQAA covered purveyor	Annual cybersecurity certification has ownership specific signers. DEP currently lists annual controls assessment and annual certification December 31; confirm current forms, recipients and acceptance receipts.	Corporate officer or authority executive director or municipal mayor or CEO authority; filings and dated portal instructions.	NJ03; NJ04 (58:31-4.1(c); agency deliverables table)
NJ-C17	Prompt qualifying incident report	WQAA covered purveyor with statutory incident facts	Report a qualifying incident to NJCCIC promptly after an employee is made aware of it. The 30 day period in 58:31-4.2(b) is the time within which NJCCIC causes an independent audit after receiving the report.	Employee awareness timeline, affected functions, physical effects, notification route and receipt; written resolution of conflicting guidance.	NJ03; NJ04 (58:31-4.2(a)-(b))
NJ-C18	Independent triggered audits	WQAA covered purveyor meeting audit trigger	A reported qualifying incident, or a missing program, revision or certification, leads NJCCIC to cause an audit by a qualified and independent cybersecurity company at the purveyor's expense, followed by the audit and corrective action submissions.	NJCCIC direction, trigger facts, auditor competence or independence, agreed scope, audit and corrective action submissions.	NJ03 (58:31-4.1(d); -4.2(b))
NJ-C19	Engineering and noncyber WQAA interfaces	WQAA covered purveyor	Track noncyber annual certification, asset management, engineering and operator duties with the appropriate specialists.	Licensed operator or engineer records; annual certification; capital or asset reports; separate ownership of noncyber work.	NJ03; NJ04 (58:31-3; -6 to -8)
NJ-C20	AWIA federal applicability	Community water system serving more than 3,300 persons	Assess whole federal risk or resilience and emergency plan obligations separately from NJ service connection threshold; ERP certification follows actual RRA certification within six months.	Population source, RRA/ERP scope, EPA certification receipts and actual cycle dates.	F01 (AWIA Section 2013)
NJ-C21	NJPDES and physical consequence reporting	Actual wastewater permit or operator	Determine applicable discharge, bypass, noncompliance and emergency notice categories from the current rule and permit; the two hour and 24 hour windows apply to the listed discharge events.	Complete NJPDES permit or modifications; current 7:14A-6.10; event classification; commencement or awareness timestamps; receiving treatment works where applicable; initial, update or written report receipts.	NJ12; NJ24 (7:14A-6.10; permit specific provisions)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C22	NERC CIP scope and versions	Registered functions and applicable systems	Determine registered functions, BES Cyber System categorization and Control Center communications scope, then assign the standards in effect for each period. FERC Order No. 919 approved CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3, effective on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after May 26, 2026. CIP-015-1 internal network security monitoring takes effect October 1, 2028 for high impact systems and medium impact Control Centers. The NJ BPU requirements are a separate screen.	Registration, BES system categorization, control center map, compliance dates and approved requirement inventory.	F02; F19; F20; NJ01 (Current CIP versions and implementation plans, including CIP-012 and CIP-015-1 scope)
NJ-C23	Energy safety and service interfaces	Gas, electric, generation, storage or other actual energy operations	Inventory applicable safety, environment or service rules, permits and emergency orders. Assign cyber duties asset by asset.	Asset types, utility orders, pipeline classifications, generation permits, interconnections and emergency plans.	NJ01; NJ14; F02; F09 (Entity instruments; controlled operator directives as applicable)
NJ-C24	TCPA chemical or process coverage	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. Facility potentially subject to NJ TCPA	Resolve substances, quantities, mixtures, processes, thresholds, exemptions and registration under current N.J.A.C. 7:31 before assigning program duties.	Chemical inventory/SDS, threshold calculations, process map, registration and current rule or consent orders.	NJ10; NJ11 (N.J.S.A. 13:1K-19 et seq.; N.J.A.C. 7:31)
NJ-C25	TCPA audit frequency and completeness	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. TCPA covered facility	For covered Program 3 processes, 7:31-4.1(c)13 replaces the federal three year compliance audit interval with every year and adds as built or as operated verification against process safety information. Audit report includes scope, techniques, methods and participant names, plus a written corrective action implementation schedule or completed action statement. The agency checklist alone is insufficient.	Program or coverage decision; current federal or state crosswalk; annual audit and as built review; named participants; scope or methods; findings or actions schedule; evidence of completion.	NJ10; NJ20; NJ21; NJ22 (7:31-4.1(c)13,14,23; incorporated 40 CFR 68.79)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C26	PSM and RMP integration	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. Actual OSHA PSM or EPA RMP covered process	Determine each program independently; OSHA PSM compliance audit cycle is at least every three years when applicable. Run the NJ TCPA annual audit on its own annual cycle. Cyberinduced process hazards require safety team review.	Coverage decisions, process safety information, hazard analysis, MOC, audits, RMP program level or current rule dates.	F06; F07; NJ11 (1910.119; 40 CFR 68; NJ incorporation)
NJ-C30	Gas utility pipeline jurisdiction	Actual utility owned or operated gas pipeline, storage or LNG assets; jurisdiction and coverage unresolved	Determine the legal operator, interstate or intrastate status and asset boundaries. Separate BPU gas service and intrastate pipeline requirements from PHMSA minimum safety rules and from TSA security directives. Pipeline owners and operators notified by TSA are subject to SD Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, and to the reporting directive SD Pipeline-2021-01G.	Legal operator/OPID, system maps, utility or franchise status, interstate or intrastate determination, distribution/transmission/storage/LNG functions, current agency or operator instruments.	NJ01; NJ14; F09; F14; NG01; NG06 (Actual orders, certification or jurisdiction records, 14:6/14:7 and applicable 49 CFR Parts 191/192/193)
NJ-C32	72 hour public agency and contractor reporting	Public agency or qualifying government contractor	Report a cybersecurity incident to the New Jersey Office of Homeland Security and Preparedness, which operates NJCCIC, within 72 hours of reasonably believing it occurred. A government contractor is defined by its access to or hosting of public agency networks, systems, applications or information.	Entity charter; contracts or access scope; reasonable belief timeline; current submission route and receipt.	NJ05 (52:17B-193.2; -193.3(a))
NJ-C33	NJ resident breach analysis	Covered NJ resident personal information and entity role	Evaluate actual personal information definition, access or use, exemptions and notice duties. Notify State Police before customer disclosure; customer notice is expedient without unreasonable delay subject to statutory conditions.	Data elements, resident scope, encryption or key status, controller or maintainer role, law enforcement correspondence, decision and notices.	NJ06 (56:8-161; -163(a)-(c))
NJ-C34	Breach exceptions and special notice paths	Actual breach facts	Document no reasonable possibility of misuse exception for five years if used; evaluate maintainer immediate notice to owner, law enforcement delay, over 1,000 person CRA notices and credential only notification rules.	Written exception analysis, delay authorization, recipient counts, account or email role and exact notice sequence.	NJ06 (56:8-163(a)-(g))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C35	NJDPA threshold and exclusions	Actual controller conducting NJ business or targeting residents	Screen 100,000 consumers excluding sole payment transactions, or 25,000 consumers plus sale revenue or discount. Evaluate government and other statutory exemptions and household consumer definition.	Entity classification, annual consumer counts or method, processing purpose, sale or discount flows, statutory exemptions.	NJ07 (56:8-166.4 to -166.5; -166.13)
NJ-C36	NJDPA operational controls	NJDPA covered processing	Use the enacted operational criteria NJ-C64 through NJ-C70 for rights, notice, consent, reasonable security, assessments, processor contracts and opt out mechanisms. Apply the enacted duties now and add implementing rule detail as it is adopted.	Data inventory, request workflow, processor terms, sensitive data practices, risk assessments, current adopted rule status.	NJ07; NJ08; NJ09; NJ25 (56:8-166.6 through -166.16)
NJ-C37	Local instruments and simultaneous notices	Actual facility and municipality or county	Identify permit, consent order, municipal or authority, OEM/LEPC, fire or health, insurer, contractual and operator duties. Distinguish binding instrument from voluntary coordination and calculate each trigger independently.	Exact facility locations, permits, orders or contracts, emergency plan, adopted local instruments and current recipients.	NJ01; NJ03; NJ05; NJ12 (Engagement specific local, permit or contract record required)
NJ-C38	Technical method and authority	All assessed OT systems	Use approved passive first examination. The operating owner authorizes any scan or control command in writing.	Rules of engagement, owner or operations approval, vendor restrictions, test method, stop conditions and rollback.	F03; F04; F05 (Engagement method; binding only when expressly adopted)
NJ-C39	Nuclear specific cybersecurity scope	Actual licensee subject to 10 CFR 73.54	Screen actual NRC license conditions, exemptions or orders, approved cyber plan and protected digital system functions. Review 73.55(m) program review and 73.77 notification interfaces through NRC specific criteria.	Actual license or status, exemptions or orders, approved plan, digital asset scope, current review or notice criteria, qualified specialized reviewer and authorized information handling.	F13 (10 CFR 73.54; actual license and approved plan)
NJ-C40	Gas pipeline SCADA control room management	Actual gas pipeline facility with controller/SCADA functions; evaluate the exact 192.631(a) coverage and limited activity provisions	Apply 192.631 scope before assigning full duties. Control rooms limited to distribution with fewer than 250,000 services or transmission without a compressor station implement only paragraphs (d), (i) and (j). Other covered operations require the applicable full procedure set, including SCADA information, alarms, change management and training.	Current 192.631, controller or control room functions, service count, compressor station facts, written applicability decision, CRM records and actual paragraph level calendar.	F14; NG04 (49 CFR 192.631(a)-(j))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C42	AMI scope and data lineage	Actual EDC/AMI operation within 14:5-10 scope	Identify EDC owned smart meter usage or demand data and distinguish validated data from local nonvalidated data. Bill only from validated data. These are specific AMI duties, independent of NERC CIP categorization.	EDC status; meter or data flow inventory; validation and billing lineage; third party roles.	NJ16 (14:5-10.1; -10.2; -10.5(a))
NJ-C43	AMI collection and availability	Actual EDC/AMI operation within 14:5-10 scope	Make validated readings available within 48 hours of capture and collect usage in intervals no greater than 15 minutes at watt level precision. Requested billing intervals tied to Order 2222 follow the applicable PJM implementation date in the adopted rule.	Capture, validation or availability timestamps with zones; interval settings and precision; actual PJM milestone and request evidence.	NJ16 (14:5-10.3(a)1-2)
NJ-C44	Local nonvalidated AMI access	Actual EDC/AMI operation within 14:5-10 scope	On customer request provide access through the customer owned energy monitoring device as close to real time as the meter allows. Document the rule distance or multiunit dwelling inability exception from actual facts.	Requests; supported meter or device capabilities; response and configuration records; specific inability rationale.	NJ16 (14:5-10.3(b))
NJ-C45	AMI authorized sharing and performance	Actual EDC/AMI operation within 14:5-10 scope	Use the Green Button Data Standard and required access channels. Supplier portal datasets include rolling 14 days delivered daily with automated API access. Transmit to authorized third parties within 60 seconds of customer authorization. Include required billing, meter or rate, multisite address and account fields, and provide access free of charge.	Authorized recipient or data field map; portal/API/EDI records; authorization and transmission times; rolling history evidence; fee schedule.	NJ16 (14:5-10.4(a)-(h))
NJ-C46	AMI consent and eligible third parties	Actual EDC/AMI operation within 14:5-10 scope	Coordinate the Common Release Form. Its web access and confirmation require MFA; disclose third party name, field, time or account scope and authorized use, with one click consent or decline. Let consumers revoke consent at any time, free of penalty. Obtain the Board eligibility order or approved party list under subsection (b).	Current common form; MFA design or evidence; consent, decline or revocation records; Board eligibility order or list and recipient verification.	NJ16 (14:5-10.6(a)-(d))
NJ-C47	AMI third party protection	Third party receiving described customer information	Take appropriate steps to protect the customer information described in -10.4(g) according to industry cybersecurity or customer information protection standards. Adopt and justify the criteria for this platform.	Actual recipient or onward transfer inventory; adopted security criteria; contracts; access, storage and transfer evidence; exceptions.	NJ16 (14:5-10.6(e))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C48	AMI unauthorized release notice	EDC, third party or onward recipient responsible for qualifying unauthorized release	Within 48 hours of discovery notify its customers, the supplying EDC, NJ State Police and BPU Division of Reliability and Security. Keep this duty separate from six hour cyber events and ITPA State Police before customer notice sequencing where both apply.	Release or discovery facts and times; information and affected customers; recipient or channel verification; legal sequencing analysis; each submission and receipt.	NJ16; NJ06; NJ01 (14:5-10.6(f); 56:8-163 as independently applicable)
NJ-C49	AMI permitted use and research access	Actual EDC/AMI operation within 14:5-10 scope	Use validated data for activated-AMI billing and customer load for peak load contribution. Use customer AMI data only for the purposes the rule permits. Examine noncore use competition, anonymized noncommercial academic access and additional use case exploration under their actual clauses.	Billing or settlement lineage; uses and sale inventory; authorized party treatment; academic request, anonymization and purpose evidence.	NJ16 (14:5-10.5(a)-(e))
NJ-C50	AMI application change and fairness	Actual EDC/AMI operation within 14:5-10 scope	Give application developers 90 days notice of technical changes adversely affecting functionality unless necessary for an immediate cyber concern or system vulnerability. Document nondiscriminatory access, the limits on surveillance or reverse engineering, and the web issue tracking system.	Developer notices or timestamps; actual emergency rationale; access comparisons; application review authority; issue records.	NJ16 (14:5-10.7(a)-(d))
NJ-C51	AMI semiannual metrics	Actual EDC/AMI operation within 14:5-10 scope	Report the nine adopted metric categories to the Board and Division of Clean Energy semiannually. Preserve the specified historical, monthly or tariff class detail. The adopted rule moves the reporting cycle from quarterly to semiannual; take the filing date from the Board's current instructions.	Nine field reporting crosswalk; usage or demand history; access, withdrawal, onboarding or login metrics; actual reporting instructions, submissions and receipts.	NJ16 (14:5-10.8(a)1-9)
NJ-C52	TPS billing integrity incident reporting	Actual licensed TPS with qualifying billing error population; distinguish electric or gas supplier and distribution company roles from ordinary water or wastewater operations	For fewer than 60 customers: report 15 or more incorrectly billed within 30 days or less. For 60 or more: apply the lesser of 25 percent of customer base or 100 customers within 30 days or less. Report within 10 business days of awareness to the listed recipients, describing impact, cause and correction. Examine residential interest or refund rules separately.	TPS status; dated full customer population; overcharge or error population and window; calculation; awareness; report or copies; refund, credit or interest records.	NJ17 (14:4-7.2 billing error definition; -7.14(a)-(d))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C53	Supplier freeze future implementation	Actual LDC/TPS customer enrollment systems; distinguish electric or gas supplier and distribution company roles from ordinary water or wastewater operations	The adopted freeze provisions specify September 8, 2027 applicability; plan changes now, then verify the actual operative date before concluding a violation. Trace direct customer authority, separate switching authorization, one business day implement or lift, two business day confirmation and rejected order notice/EDI rules, including merger or default service exceptions.	Approved implementation plan; EDI/vendor dependencies; actual rule or date interpretation; authorization or notice and nonproduction acceptance scenarios.	NJ17 (14:4-2.6(d)-(e); -2.6A(a)-(n))
NJ-C54	Drinking water emergency notice	Supplier of water with qualifying quality or pressure emergency	Notify DEP by telephone within six hours of the occurrence of an emergency tending to lessen delivered quality or pressure or increase likelihood of nonstandard water. This occurrence trigger is distinct from cyber detection, employee awareness and reasonable belief.	Emergency onset; quality, pressure or process records; licensed operator review; current daytime or after hours channel; call or receipt evidence.	NJ19 (7:10-2.4(b))
NJ-C55	Planned treatment change notice	Supplier planning a qualifying treatment plant or operational change	Written DEP notice is required at least five working days before a planned change tending to lessen water quality or increase the likelihood of nonstandard water. Have the operator determine whether an OT change falls within the clause and send the regulatory notice it requires.	Change/MOC; operator engineering consequence review; proposed date; working day basis; notice and receipt; permit review.	NJ19 (7:10-2.4(a))
NJ-C56	Water asset program and signatory interfaces	Public community water system within 7:10-6 scope	Coordinate the asset inventory, criticality, revision, funding and certification work with the responsible operator or engineer. Rule copy specifies annual March 15 capital report, asset plan certification every three years or ownership or status change, ownership specific annual compliance signers and annual designated training. Annual water loss audit is specified effective March 31, 2027. These are distinct from the WQAA cyber certification.	Actual 7:10-6.1 scope; asset plan and prior certification; capital report; signatory or training records; current water loss criteria; qualified engineering lead.	NJ19 (7:10-6.1; -6.3(b)9,(c)-(g); -6.4)
NJ-C57	Physical hazardous substance discharge notice	Actual person responsible for a qualifying NJ discharge	Immediate notice under 7:1E-5.3 is measured from knew or reasonably should have known facts; receipt within 15 minutes is considered immediate. Evaluate the specific transformer and motor vehicle conditions, other reporting laws and the 5.6 delay justification.	Substance or current Appendix A; discharge or pathway facts; actual knowledge timeline; exception clause or facts; hotline or backup; notification content and receipt.	NJ18; NJ26 (7:1E-5.3(a)-(f); -5.6)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C58	Discharge detection or safety malfunction notice	Owner or operator of an actual major facility under 7:1E	Immediately report malfunction of discharge detection or other discharge monitoring, prevention or safety system or device. Receipt within 15 minutes of knew or should have known is considered immediate. Within two hours after initial notice report repair, alternate detection activation or protected equipment out of service. This malfunction duty applies on the malfunction itself, before any spill.	Major facility determination; covered detection, prevention or safety devices; fault or awareness timeline; initial call; actual follow up disposition or time; authorization for operations actions.	NJ18 (7:1E-5.5(a)-(c); -5.6)
NJ-C59	DPCC/DCR plan and OT dependency screen	Actual major facility or transmission pipeline under applicable 7:1E provisions	Screen capacity, substances, exemption facts and approved DPCC/DCR plans with the environmental owner. Trace detection, alarms, remote valves, response communications, changes, training and exercises into actual plan requirements. Agency requires covered plan submissions through its online service from June 1, 2026. Engineering and plan certification follow their own process alongside the OT audit.	Capacity calculations; current appendices; registration; approved plans; change or renewal history; PE/offsite response signoffs; online submission receipts.	NJ18; NJ22; NJ26 (Applicable 7:1E-1.6; -2 through -4; actual approved plans)
NJ-C60	TCPA annual audit design	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. TCPA Program 3 covered process	Use the state every year interval and verify as built or as operated equipment and process technology against process safety information. Include actual audit scope, techniques, methods and participant names; assign competent process safety reviewers for elements outside OT competence.	Current incorporation crosswalk; full applicable program index; prior audit or date; PSI/as built evidence; team competence and actual workpapers.	NJ20; NJ21; NJ22 (7:31-4.1(c)13-14)
NJ-C61	TCPA corrective action report	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. TCPA Program 3 audit with findings	Include written corrective action implementation schedule or completed action statement in the audit report. Reconcile other open related program findings. Close on evidence of completion that meets each mandatory duty.	Audit findings and prior related findings; response basis; owners or dates; schedule; remediation and retest or reviewer evidence.	NJ10; NJ20 (7:31-4.1(c)23; incorporated 68.79(d))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C62	TCPA annual report and anniversary	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. Actual covered Program 3 owner or operator	Report the prior 12 month risk management activity within 90 days of the approval or consent anniversary. Include required updates or no change statements, management changes, applicable PHA/risk assessment, event summaries, compliance audit or corrections and IST reports. Use the facility's approved anniversary date for the audit cycle.	Signed initial consent or order and approved anniversary change; annual report or checklist; audit and required attachments; submission receipt.	NJ20; NJ21 (7:31-4.9(a)-(b))
NJ-C63	NJRMP refresh and transfer	Utility facility only if its actual chemicals, quantities, process and applicable program establish coverage. Actual TCPA covered facility or process	Reconcile full NJRMP five year cycle, event driven resubmission or corrections and owner transfer requirements against actual facts. State and federal chemical scope differ. Current federal amendments are incorporated subject to state conflict or stricter rule treatment; read them with the current consolidated text.	Last full submission or receipt; process and chemical changes; Program Level; new owner agreement; current federal or state crosswalk and actual dates.	NJ20; NJ21; NJ22; NJ23 (7:31-7.1(c)5,11; -7.4; incorporated Part 68)
NJ-C64	Privacy rights and response record	NJDPA covered controller or processing after actual threshold and exemption review	Provide applicable access, correction, deletion, portability and opt out rights. Verified requests use 45 days from receipt; a reasonably necessary 45 day extension requires notice or reason in the first period. Refusal notice and appeal response have separate 45 day windows. Authentication restrictions and documented fraudulent opt out handling are distinct.	Request or appeal inventory; receipt dates; authentication or minimization method; decisions and extension or refusal notices; portability or deletion scope; actual exceptions.	NJ07 (56:8-166.7; -166.10)
NJ-C65	Privacy notice and contact	NJDPA covered controller or processing after actual threshold and exemption review	Publish reasonably accessible, meaningful notice covering categories, purposes, third parties, shared data, rights or appeals, material changes or effective date and contact channel. Clearly disclose applicable sale or targeted advertising or profiling and opt out. Let consumers exercise their rights through existing accounts or a simple request.	Versioned notices and effective dates; actual data, use or recipient mapping; working channels; rights and appeal workflows; account prerequisites.	NJ07 (56:8-166.6)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C66	Sensitive data, young consumers and consent	NJDPA covered controller or processing after actual threshold and exemption review	Obtain required sensitive data consent and apply COPPA to known child processing. Apply the enacted actual knowledge or willful disregard test for consumers at least 13 but younger than 17 in the listed uses. Provide equally easy consent revocation and cease the relevant processing as soon as practicable, no later than 15 days after receipt. AMI is excluded from the precise geolocation definition only, and the other personal and sensitive data rules apply.	Data element or age purpose map; actual consent or revocation records; scope of processing stopped; COPPA/specialist analysis; precise geolocation decision.	NJ07 (56:8-166.4 sensitive data or precise geolocation; -166.12(a)4,6,7)
NJ-C67	Privacy minimization and reasonable security	NJDPA covered controller or processing after actual threshold and exemption review	Limit collection to adequate, relevant, reasonably necessary data; control incompatible use and specify purposes. Apply administrative, technical and physical safeguards appropriate to data volume or nature during storage or use. Document exceptions and necessity rather than asserting utility operation purposes waive every privacy safeguard.	Purpose, collection or retention map; legitimate exception basis; access, encryption or recovery controls; risk and safeguard evidence; deletion or return rules.	NJ07 (56:8-166.12(a)1-3,8; -166.15)
NJ-C68	Privacy data protection assessment	NJDPA covered controller or processing after actual threshold and exemption review	Before heightened risk processing, conduct or document the required assessment for personal data acquired on or after the effective date. Evaluate listed profiling or targeted advertising risks, sale and sensitive data; weigh benefits, rights risks, safeguards, expectations and context. Retain availability for DCA request. Record each workpaper's confidentiality basis individually.	Processing inventory and acquisition dates; risk trigger; actual assessment; benefits, risks or safeguards; approvals or changes; controlled location.	NJ07 (56:8-166.12(a)9,(b)-(d))
NJ-C69	Processor terms and assessment route	Actual NJDPA controller or processor relationship	Binding processor terms specify instructions, purpose, data, duration, confidentiality, subcontractors, security allocation, deletion or return subject to law, and compliance information or assessment access. The independent annual assessor route is an alternative with controller consent, at processor expense.	Actual role facts; executed DPA and subprocessor terms; allocation; return or deletion; assessment access or consented independent report, scope, period or competence.	NJ07 (56:8-166.16(a)-(g), especially (e)4(b))
NJ-C70	Universal opt out and authorized agents	NJDPA covered controller or processing after actual threshold and exemption review	For covered targeted advertising or personal data sale, the statutory universal opt out mechanism start is no later than six months after January 15, 2025. Review actual signals or agent authority and conflict or consent handling against enacted criteria and the applicable rules.	Sale or advertising applicability; supported user selected mechanism; agent verification; signal or consent conflict records; dated functional evidence.	NJ07; NJ09; NJ25 (56:8-166.11(a)-(c))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C71	CIAP authentication and secure data exchange	Actual EDC CIAP within current 14:8 scope	The January 2026 adopted text requires MFA/secure login, role based access, secure file viewing or transfer and confidentiality, integrity and accessibility within a privacy, security or risk assessment framework. Resolve current chapter status, later orders, tariffs and implementation before treating this dated amendment as currently enforceable.	Current chapter or readoption and orders; actual CIAP implementation or tariff; role or tenant map; MFA and transfer design; independent evidence and exceptions.	NJ27; NJ14 (14:8-5.13(d)1-2; source currency dependency NJ-Q17)
NJ-C72	CIAP availability, workflow and data quality	Actual EDC CIAP within current 14:8 scope	Adopted text specifies at least 99 percent uptime during stated weekday 8 AM-8 PM EST hours, quarterly public uptime metrics, listed workflow timestamps, payment or status visibility, validation and notifications or opt choices. Verify current operative text and measurement or time zone interpretation. Hosting maps have separate updates and disclosure limits; treat operational security information as protected.	Current instruments; uptime definition or window and raw periods; outage exclusions basis; fourteen timestamp events; validation or status records; map publication or security approvals.	NJ27 (14:8-5.13(d)3-4; -5.11; NJ-Q17)
NJ-C73	NJPDES oral categories and revision notice	Actual permittee with 6.10(a) qualifying facts	Subsection (c) uses two hour hotline notice for (a)1i iv health or environment exceedances and (a)2 unpermitted listed toxic or hazardous discharge, with receiving DTW if applicable; revisions to that information within 24 hours of awareness of the need. Subsection (d) uses 24 hour notice for (a)1v listed toxic daily maximum exceedance, (a)3 other upset or unanticipated bypass and (a)5 residual standard noncompliance. Apply actual commencement or awareness facts and permit.	Exact event or permit category; discharge, awareness or revision times; listed pollutants or limits; receiving DTW; initial and revision content or receipts.	NJ24; NJ12 (7:14A-6.10(a)-(d))
NJ-C74	NJPDES written and anticipated bypass duties	Actual permittee with applicable 6.10 category	For (a)1-3 and 5, subsection (e) requires written information within five days of commencement or awareness unless already submitted, and immediate correction of missing or incorrect facts; upset or unanticipated bypass has additional (f) evidence. Anticipated bypass uses (g) notice at least ten days before if possible. Serious violation has separate (i) 30 day written report; other noncompliance is reported with regular MRFs under (j).	Exact permit or category; contemporaneous signed logs; cause, duration, response or evidence; planned bypass, necessity or alternatives; serious violation decision; current recipient; reports and receipts.	NJ24 (7:14A-6.10(e)-(j))

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C75	Gas utility jurisdiction and complete criteria	Actual gas utility or operator and asset functions	Separate retail gas service, intrastate pipeline safety, interstate federal oversight and actual controlled security instruments. Obtain current full 14:6/14:7 and applicable 49 CFR Parts 191/192/193 with amendments.	OPID; owner or operator; franchise or tariff; maps; pipeline class; distribution/transmission/storage/LNG boundaries; jurisdiction instruments; current code and incorporation history.	NJ14; NG01; NG05; NG06 (14:7-1.1; actual 14:6 and federal scope; orders or agreements)
NJ-C76	NJ gas incident reporting and follow up	Gas operator with a reportable event under 14:7-1.17	The selected final state rule requires immediate notice, no later than one hour after learning of a reportable incident. Its event definition includes federal incident coverage and additional listed state categories. Preserve new information updates and the separate follow up report within 15 days after the incident. Run the state gas incident clock on its own, separate from the federal confirmed discovery clock and the six hour cyber window.	Actual event classification and learning time; full state definition; current division or channel; initial or update receipts; incident date and 15 day follow up evidence.	NG01; NJ01 (14:7-1.17(b)-(h); current full text and later history)
NJ-C77	Gas distribution drills and spacing	Actual distribution operator subject to 14:7-1.9(f)-(g)	Plan each district or division and call or dispatch center for two year coverage, with district or division drills spaced at least two weeks apart. Reconcile the initial field or training site transition and subsequent four year field site cycle, with permitted tabletop limits. Keep the five business day advance notice, narrow weather exception and final audit report within two months as separate tasks. Record the BPU cyber exercise separately from this operational drill.	Districts or divisions; call and dispatch centers; prior drill dates, type or location; two week spacing; actual field cycle; notice and final report receipts; weather exception basis if used.	NG01 (14:7-1.9(f)-(g), final adopted text)
NJ-C78	Gas transmission emergency closure drill	Actual transmission operator subject to 14:7-1.10(f)	Review the annual calendar year drill and maximum 15 month interval together. The adopted provision also requires a field site drill at least every three calendar years, normal business hour timing at least once every three years, and limits tabletop use to no more than two of three calendar years. Obtain unchanged surrounding paragraphs before final program approval.	Transmission closure plan; previous actual dates; three year type or location calendar; operating permissions; drill evaluation and corrective records.	NG01 (14:7-1.10(f) and current complete section)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C79	Gas state filings and source data integrity	Actual gas operator and applicable state report or asset class	Reconcile selected state filings: applicable prior year annual report copies by March 15; leak classification inventory by January 31; gas transmission pressure test records within one month after test; and transmission direct assessment or examination excavation notice at least five business days beforehand. Verify current full section, forms and applicability.	Report or asset class matrix; current forms; prior year source systems; leak status and municipality records; pressure or temperature charts; test dates; excavation schedule; submission receipts.	NG01; NG05 (14:7-1.26(c), (d)1 and 8, (f); current full section)
NJ-C80	Gas MAOP state and federal notice distinction	Actual qualifying overpressure event and relevant pipeline class	The adopted state 14:7-1.26(g) requires immediate notice upon discovery of the specified MAOP exceedance beyond the allowed device margin and a formal report under 191.25. Federal 191.25(b) separately addresses a qualifying gas transmission MAOP exceedance with a five calendar day report. Confirm the exact trigger, exclusions and current channels for this federal category.	Actual pressure or time series integrity; MAOP and device margin; asset class; discovery or exceedance timestamps; current trigger decision and state or federal receipts.	NG01; NG03 (14:7-1.26(g); 191.23(a)(10); 191.25(b)-(c))
NJ-C81	Federal gas incident initial and 48 hour update	Operator or event covered by Part 191 and current 191.3 definition	Section 191.5 requires notice at the earliest practicable moment following discovery and no later than one hour after confirmed discovery of a qualifying incident. Within 48 hours after confirmed discovery, revise or confirm the initial notice to the extent practicable; unchanged estimates also require confirmation. Keep discovery and confirmed discovery timestamps distinct.	Complete current incident definition or exclusions; event date monetary notice (NG07 verifies July 2026-June 2027 only); discovery and confirmed discovery evidence; current NRC instructions; initial and 48 hour receipts.	NG02; NG07 (191.5(a)-(c); current 191.1/.3)
NJ-C82	Federal gas safety related condition reporting	Actual condition covered by 191.23(a)(1)-(9), after exclusions	Under 191.25(a), the written report is due within five working days after the day an operator representative first determines the condition exists, and no later than ten working days after the day of discovery. Saturday, Sunday and federal holidays are excluded. This differs from the five calendar day transmission MAOP category. Preserve discovery, determination and receipt dates separately.	Current 191.23 trigger or exclusion decision; discovery or determination dates; applicable working day calendar; required report fields and receipt; corrective action schedule.	NG03 (191.25(a),(c); applicable 191.23)

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

ID	Topic	Applies to	What to determine	Facts to gather	Sources
NJ-C83	Gas safety telemetry and specialist interfaces	Utility pressure control, alarms, leak detection, storage or LNG interfaces	Trace OT evidence into the actual pipeline safety program and qualified specialist boundaries. Confirm current operating or emergency procedures, control room requirements, integrity programs, operator qualification and any actual LNG/storage criteria. Live valve operation, pressure tests and alarm injection proceed only under the operator's written procedures.	Approved procedures, safety or engineering specialists, pressure or temperature provenance, calibration, control changes and incident reconstruction; actual specialist program or permit limits.	F14; NG01; NG04; NG05; NG06 (Actual 192/193 program, 14:7 and operator procedures)
NJ-C84	Gas service interruption and amended report branches	Actual gas operator and qualifying interruption or incomplete incident follow up	Keep service interruptions and reportable incidents as separate records. Under the selected 14:7-1.17(j), qualifying interruptions are reported within 30 minutes after awareness that service has been interrupted for 30 minutes: the listed heating season 100-customer, defined healthcare facility and designated airport categories. Subsection (k) separately uses awareness of one hour of interruption for nonheating season 100-customer, listed highway lane closure and specified critical customer categories. Contract provided interruptions have an exclusion under (l); prompt detailed written follow up is required under (m). Where the incident follow up lacked corrective measures or recommendations, (i) requires an amended report within 30 days of the incident. Obtain exact current category definitions, exclusions, forms and later amendments.	Affected customer count or type and season; actual interruption start and awareness timestamps; road or critical facility facts; contract exception decision; current reporting forms; written follow up and corrective action availability.	NG01 (14:7-1.17(i)-(m), (p)-(r); current complete section)

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

7. Procedure starters and field boundaries

Select procedures after the criteria are agreed, then tailor the objective, population, period, sample and depth to the engagement. Each safety boundary is a rule for the field team.

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P01	Resolve entity and facility scope (All)	Assign duties to a documented legal entity and system boundary. 1. Obtain charter, ownership and operator agreements. 2. Record each facility, county, municipality and legal owner or operator. 3. Identify service, PWS/permit/registration IDs and shared IT/OT providers. 4. Have qualified compliance counsel or authority resolve disputed coverage; retain exclusion reasons.	Charter; ownership evidence; site list; contracts; applicable orders.	Signed scope decision names systems, exclusions, decision maker, date and source. Each unknown has an owner and a next evidence request.	Assign regulatory coverage from documented entity and facility facts.
P02	Approve audit plan and safety boundary (All)	Establish authority, criteria, competence and site safety before fieldwork. 1. Agree audit objective and assurance or report basis, period, users and limitations. 2. Assess examiner competence, conflicts and independence. 3. Agree evidence handling, sampling and escalation. 4. Obtain owner, operations, safety and vendor approvals. 5. Approve rules of engagement, stop authority, recovery and communications.	Engagement letter; independence or competence records; signed plan/rules of engagement; safety contacts.	Named approvers authorize precise methods, assets and windows; all scope critical criteria or evidence gaps are resolved or scope is expressly limited.	Active discovery, credential use, write operations and production tests after explicit method authorization.
P03	Reconcile critical inventory (Utilities)	Find omissions between operating systems and the regulated critical system inventory. 1. Obtain dated asset or configuration exports and drawings. 2. Reconcile ICS controllers, RTUs, HMIs, historians, engineering stations, telecom and customer-PI systems. 3. Trace additions or removals and review approval. 4. Record population, source or date and discrepancies.	Inventory; diagrams; changes; annual review; customer data inventory.	A documented reconciliation covers agreed populations; unresolved omissions become findings rather than assumed absence.	Network probes and new capture ports only with written approval from the operating owner.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P04	Map dependencies and protocols (All)	Understand process consequences, legacy constraints and external paths. 1. Walk through physical process with operator. 2. Mark safety, power, time, communications, cloud or vendor and remote access dependencies. 3. Identify actual protocols, versions and supported methods from approved records or passive observations. 4. Record unsupported or unseen assets and vendor safety restrictions.	Validated zone or conduit diagram; dependency register; protocol or vendor records.	Operators validate boundaries and consequence paths; assumptions and unknown protocol coverage are explicit.	Promise all protocols are tested; no packet injection, failover or controller polling only with separate approval.
P05	Assess risk and treatment (All)	Connect cyber failure modes to safety, service, environment and financial exposure. 1. Agree risk scales and decision authority. 2. Examine current risk methodology and annual review where required. 3. Trace credible access and failure paths, dependencies and physical risks. 4. Examine controls or compensations and residual decisions. 5. Link each finding to consequence and accountable owner.	Method; risk register; threat inputs; treatment approvals; BIA/continuity records.	Evidence supports risk ratings and treatment; risk acceptance is an authorized decision with an expiry date, and each mandatory duty is tracked to completion on its own record.	Review hazardous process states through records and approved observation.
P06	Examine monitoring and time (All)	Establish whether relevant events can be detected and reconstructed. 1. List sources and retention rationale. 2. Examine representative authentication, remote access, configuration and boundary logs from approved exports. 3. Check time zone or time synchronization and gaps. 4. Trace one authorized alert through triage or escalation.	Source inventory; redacted logs; time settings; alert or ticket trail; retention policy.	Coverage and missing sources are recorded against agreed objectives; collector, collection time and source system are attributable.	Use approved historical events or a lab example as evidence; use approved historical event or lab example.
P07	Trace threat and vulnerability handling (Utilities)	Test whether relevant intelligence leads to timely documented action. 1. Define assessment period and advisory population. 2. Select high consequence and routine examples with rationale. 3. Trace receipt, applicability, owner, disposition and follow up. 4. Examine omitted suppliers or assets.	Vendor/ISAC advisories; intake queue; tickets; risk decisions.	Document the full population, selected sample, exceptions and coverage limits, and support interviews with records.	Keep sensitive intelligence in authorized repository.
P08	Review patch and legacy safeguards (All)	Assess risk decisions with production kept stable. 1. Match approved vendor notices to asset versions. 2. Examine compatibility or lab validation and outage coordination. 3. Sample applied or deferred patches and compensating controls. 4. Review unsupported assets, isolation and replacement plans.	Version exports; vendor notices; MOC/maintenance tickets; deferment approvals; compensating controls.	Decisions are traceable to actual systems and approved criteria; no invented patch SLA is used.	Patching, restart, exploit or active vulnerability scan only with written approval from the operating owner.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P09	Build and rehearse reporting decision tree (All)	Keep simultaneous legal triggers and clocks distinct. 1. Gather current source text and applicable instruments. 2. Record detection, employee awareness, Board awareness, reasonable belief and incident consequence times separately. 3. Map each matched duty to trigger, clock, owner, deputy and current official recipient. 4. Rehearse with synthetic scenario and evidence preservation plan. 5. Retain actual submission or receipt trail separately from rehearsal.	Notices register; approved decision tree; current portal instructions; tabletop record; receipts.	Each applicable duty keeps its own deadline, earliest first; prompt reporting has no invented number. Unknown law or channel is escalated before fieldwork.	Real incident: activate the approved response and legal escalation immediately and report on time.
P10	Review customer and employee information (All)	Determine breach and privacy handling using actual data and legal roles. 1. Inventory resident data, online credentials, AMI and vendor processing. 2. Record controller or maintainer roles and affected population. 3. Evaluate each legal definition or exception and exact sequence with counsel. 4. Review notices, law enforcement communications and exception retention. 5. Use redacted evidence and keep personal data out of workbooks.	Data inventory; processor contracts; legal decision record; redacted notice or receipt trail.	Conclusions cite operative criteria and facts for each data element; all exceptions have evidence and authorized decision.	Keep raw customer data, keys and credentials in the utility's secure systems.
P11	Examine incident response and recovery (All)	Verify executable roles and recovery arrangements. 1. Review cyber, operations or safety incident integration. 2. Trace communications, containment authority, forensic preservation and manual operating limits. 3. Examine approved backup, configuration or logic recovery scope. 4. Review isolated restore evidence and actual recovery objectives.	Approved plans; role or deputy roster; immutable or offline backup design; restore records; manual limits.	Recovery claims are supported by relevant observed records; untested restores remain untested.	Production restore, failover, interlock bypass or manual operation demonstration only with separate safety authorization.
P12	Evaluate exercise record (Utilities)	Distinguish actual execution from a planned exercise. 1. Establish applicable cycle and last qualifying date. 2. Review scenario, participants, actual chronology, decisions and observations. 3. Trace lessons to owners and closure. 4. Verify whether claimed actual incident satisfies stated criteria.	Exercise plan; attendance; contemporaneous notes; after action report; action or retest evidence.	Cycle, scope and evidence meet the adopted criterion; attendance or future calendar entry alone is insufficient.	Use a tabletop or an approved low impact exercise.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P13	Review training coverage (Utilities)	Assess general, role specific and new personnel coverage. 1. Reconcile personnel or credential holder populations to training records. 2. Sample new staff and high privilege roles. 3. Examine recurring communications and program review. 4. Record how the Board interprets "biannually" and the authorized interim plan.	Role or credential roster; training matrix; completion records; awareness messages; written interpretation.	Coverage and exceptions use actual populations and dates, with a source for each interpretation.	Collect only the employee information the review needs.
P14	Reconcile certifications to evidence (Utilities)	Prevent unsupported executive sign off. 1. Identify exact required certification and signer. 2. Reconcile assertions to scope, open findings and evidence. 3. Verify authority and dates. 4. Check filing recipients and receipts. 5. For NERC overlap, identify exact systems or duties accepted by BPU.	Signed certification; authority record; supporting index; exception or legal decisions; receipts.	The authorized signatory approves the certification separately.	The authorized signatory signs and submits each regulatory certification through the official channel.
P15	Separate NJ and federal water scope (Water)	Record service connections, population and ownership as separate facts. 1. Obtain PWS identity and community status. 2. Record more than 500 service connection screen separately from AWIA more than 3,300 person screen. 3. Validate owner and all ICS. 4. Record BPU and public agency screens independently.	PWS records; dated counts; charter; service or asset map; EPA certifications.	Each applicable or excluded decision has source, facts and reviewer, with wastewater only systems screened separately.	Record an unknown count as To decide until the count is confirmed.
P16	Test framework revision trail (Water)	Connect chosen framework to control and submission evidence. 1. Identify chosen listed framework(s), final edition and publication date. 2. Review requirement or control mapping and treatment. 3. Reconcile final revision changes and 180 day submission duty where triggered. 4. Verify actual program revision and receipt.	Chosen framework decision; licensed text where needed; change map; revised program; NJCCIC receipt.	Final framework versions and change dates support the conclusion, naming the CSF, the CIS Controls or ISO/IEC 27000 as the chosen framework.	Cite licensed standards by clause number in exports and keep their text in licensed copies.
P17	Assemble NJCCIC and insurance records (Water)	Prepare current program delivery and insurance evidence. 1. Obtain membership or program submission receipts. 2. Verify current annual portal instructions and deliverables. 3. Review policy period, named insured, exclusions, limits and applicable Board standards with insurance or legal owners. 4. Capture open coverage questions.	Membership or filing evidence; insurance declarations and review; current instructions.	Coverage and submission status use actual records and receipts.	Insurance adequacy opinion only with the relevant policy or standards and qualified review.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P18	Prepare for independent triggered audit (Water)	Recognize statutory triggers and qualified independent auditor requirements. 1. Determine missed submission or incident trigger and NJCCIC direction. 2. Preserve incident and program records. 3. Confirm auditor competence, independence and scope. 4. Track audit, corrective plan and submission responsibilities.	Trigger record; NJCCIC correspondence; engagement or independence records; audit/CAP/receipts.	Regulator required deliverables are planned and accepted separately, and a qualified independent company performs any statutory audit.	Record the engagement terms and independence review in the signed engagement.
P19	Coordinate engineering and AWIA work (Water)	Keep OT evidence connected to broader resilience within the agreed scope. 1. Inventory AWIA RRA components and ERP linkage. 2. Coordinate with operator or engineer for WQAA noncyber certifications and asset plans. 3. Assign deliverable owners and exact actual dates. 4. Expose work outside the cyber engagement.	RRA/ERP scope; licensed specialist records; asset or capital reports; responsibility matrix.	Whole program conclusions combine cyber testing with the other program evidence; specialist dependencies and omissions are visible.	Leave engineering certification and valve or hydrant operation to the utility's engineers and operators.
P20	Map cyberto discharge consequences (Wastewater)	Integrate cyber incident handling with permit based response. 1. Obtain complete current permit or modifications, 6.10 text and actual emergency plan. 2. Map pump, treatment, aeration, disinfection and telemetry failure consequences with permit owner. 3. Classify each scenario into the exact (a) category and independent (c), (d), (e), (f), (g), (i) or (j) duties. 4. Review commencement, awareness, revision, initial call and written report records separately, including receiving DTW and signed contemporaneous logs where applicable. 5. Verify current recipients or channels and rehearse synthetic communications in a tabletop.	NJPDES permit; current rule; process diagrams; emergency contacts; reporting tree.	Reporting categories cite actual permit or rule sections and facts, with cyber and physical clocks tracked separately.	Bypass, discharge, process upset or chemical dosing test only with written approval from the operating owner.
P21	Reconcile NERC and NJ programs (Electric)	Build a requirement level inventory from confirmed CIP coverage. 1. Verify registered entity or functions and systems. 2. Examine categorization and separate control center communications screening. 3. Obtain current effective standards or implementation plans. 4. Map evidence and NJ duties, including any accepted certification overlap.	Registration; categorization; current standards; system or evidence map; overlap decision.	A qualified owner approves the exact applicable requirements and versions.	Relay, protection, dispatch or generation command testing only with separate approved method.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P22	Review energy operating interfaces (Utilities)	Cover gas, electric, generation and emerging asset boundaries. 1. Identify substations, DER, storage, plants, gas assets and outsourced control. 2. Map safety, dispatch or interconnection and permits. 3. Assign regulatory specialist owners. 4. Review communications loss or manual operations using records.	Asset or interface list; approved operating and emergency plans; permits; vendor agreements.	Each asset type has a documented governing program screen and unresolved specialist work.	Switching, trip, synchronization, gas flow or storage safety test only with written approval from the operating owner.
P23	Screen covered processes (Utilities)	Resolve TCPA, PSM and RMP applicability with process safety personnel. 1. Obtain chemical quantities, mixtures, process boundaries and exemptions. 2. Reconcile NJ and federal threshold methods separately. 3. Obtain registration or program levels or consent orders. 4. Authenticate current rule or incorporation dates.	Inventory/SDS; calculations; registration; current rules or orders; process engineer approval.	Safety or compliance owner signs a factual utility site coverage decision; selecting a utility group establishes none.	Calculate chemical thresholds from inventory records.
P24	Integrate safety audit and OT findings (Utilities)	Keep audit cycles and whole program coverage distinct. 1. Build applicable TCPA annual, PSM three year and RMP criteria or calendar separately. 2. Reconcile prior audits and open related findings. 3. Trace OT related safeguards through process hazard analysis and MOC. 4. Record excluded safety elements and specialist owners.	Current criteria; audit reports; PHA/MOC; corrective records; complete program index.	OT findings inform the applicable safety program and its full audit report.	Safety integrity, mechanical integrity and process safety certification stay with the facility's certified specialists.
P25	Review utility process and safety system separation (Utilities)	Assess controller or recipe access and safety dependencies through records and observation. 1. Examine design or configuration records for BPCS/SIS and engineering access. 2. Review recipe or logic change approval and vendor access. 3. Examine backups, provenance and restore validation. 4. Trace one historical approved change with safety owner.	Architecture; logic or recipe change records; MOC; backups; vendor approvals.	Actual boundaries and shared dependencies are recorded; independence claims require evidence.	Logic download, interlock test, setpoint or recipe change or safety bypass only with written approval from the operating owner.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P29	Resolve gas utility operator instruments (Gas)	Establish gas operator jurisdiction and controlled criteria before designing the audit. 1. Obtain legal operator, OPID, ownership and system or function maps. 2. Resolve distribution, transmission, gathering, storage and LNG boundaries with pipeline compliance staff. 3. Obtain current BPU, PHMSA and any actual TSA operator instruments through authorized channels. 4. Record applicability, versions, effective dates, exclusions and outstanding specialist decisions.	Operator or jurisdiction records, current rules and orders, controlled criteria register and actual decision evidence.	Each instrument has its effective revision and applicability evidence.	Flow, valve, compressor, leak detection or emergency shutdown actuation only with written approval from the operating owner.
P31	Screen public agency contractors (All)	Apply the access or hosting definition to actual contracts. 1. Identify public agency and contractor legal entities. 2. Read contract scope and actual network, system, application or information access. 3. Record current incident process and 72 hour reasonable belief trigger. 4. Review supplier flow down supplier by supplier.	Contracts; access or service records; legal coverage decision; current reporting process.	Decision distinguishes qualifying access or hosting from ordinary supply and records actual facts.	Keep agency information in authorized repositories.
P32	Screen privacy and customer data controls (All)	Assess NJDPA coverage and actual processing duties. 1. Confirm legal entity or exclusions. 2. Reconcile annual household consumer counts and sole payment exclusions. 3. Review sale, revenue or discount facts and processors. 4. Authenticate adopted rules. 5. Map applicable rights, security and assessment duties to evidence.	Entity or data inventory; count method; contracts; current rules; request, security or assessment records.	Draw conclusions data set by data set for AMI, utility and employee data; each exclusion has exact legal basis and facts.	Take final rule status from the adopted rule.
P33	Collect local and contractual instruments (All)	Turn local uncertainty into specific collection tasks. 1. List every facility, municipality or county and owner. 2. Obtain permits, consent orders, franchise, lease or compact terms and regulator directions. 3. Identify binding local enactment versus voluntary emergency coordination. 4. Record exact section, current status, trigger, recipient and responsible specialist.	Complete instrument copies; adoption or effective evidence; current emergency plan; contractual duty register.	Every local duty or exclusion is traceable; a missing instrument stays on the Open questions sheet until it is obtained.	Collect the municipal instruments for each facility.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P34	Execute traceable field records (All)	Produce reproducible evidence through safe work. 1. Record examiner, collector, permission, population or sample method and rationale. 2. Execute only approved examine, interview or test steps. 3. Record observations, exceptions, actual times and evidence IDs. 4. Separate criterion, condition, cause and consequence. 5. Have reviewer evaluate records and limits.	Execution record; evidence manifest; rules of engagement; sampling basis; observations; review trail.	Evidence supports only the stated population or method; untested, missing and inaccessible are distinguished.	Stop on safety concern, unexpected process behavior, unauthorized access or scope or method change; notify named stop authority.
P35	Close findings and hand over (All)	Deliver an honest report and actionable remediation trail. 1. Validate factual findings with owners while the examiner keeps the final judgment. 2. Agree corrective owners or dates and evidence. 3. Retest relevant correction with authorized safe methods. 4. Record retester or date and closure approver or date. 5. Reconcile exclusions, open questions and source currency; deliver controlled report or records.	Findings; treatment or acceptance; retest; closure approvals; final report and receipt.	Closure follows actual remediation and retest; no future or reversed actual dates or to be determined evidence accepted. Open scope or criteria prevent unsupported whole program assurance.	
P36	Examine identities and privileged access (All)	Assess actual access paths and lifecycle from records and configuration. 1. Reconcile approved account exports to named people, services and vendor roles. 2. Sample joiner, mover or leaver and privileged approvals. 3. Examine remote access MFA, session approval, emergency access and service account safeguards. 4. Record legacy constraints and compensating controls against the adopted criterion.	Redacted account or role exports; access reviews; approvals; remote access settings; termination tickets.	Population and sample rationale support least privilege or lifecycle conclusions.	Password guessing, login trials and account disabling only with written approval from the operating owner; secrets stay in their vault.
P37	Examine segmentation and remote conduits (All)	Verify documented boundary intent against approved configuration evidence. 1. Reconcile zones or conduits and vendor, cloud, wireless or cellular paths. 2. Examine authorized firewall, routing and jump host exports. 3. Trace selected necessary flows and denied path design, including actual Modbus, DNP3, EtherNet/IP, IEC 61850, OPC UA or other site protocols. 4. Document unobserved paths and protocol specific limitations.	Current drawings; sanitized configurations; authorized passive records; vendor connection lists.	Each sampled path has a documented purpose or owner, an adopted control objective and test evidence.	Connectivity probes, packet injection, port mirroring or firewall changes only with separate method approval.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P38	Examine configuration and endpoint safeguards (All)	Assess approved hardening against platform and process constraints. 1. Establish vendor supported baselines and actual platform or firmware versions. 2. Examine approved exports for services, access, logging, application controls and endpoint protections. 3. Review exceptions and legacy compensations. 4. Compare selected systems to the adopted baseline with owner validation.	Baseline; version or configuration exports; exception approvals; platform compatibility evidence.	Observed deviations and coverage limits are recorded, with an OT appropriate benchmark for each device.	Agent installation, service stopping, hardening changes or unsupported endpoint query only with written approval from the operating owner.
P39	Trace engineering and logic change integrity (All)	Establish authorization and recoverable provenance of control changes. 1. Identify approved engineering tools, project repositories and logic, firmware or recipe baselines. 2. Sample actual changes from request through review, safety/MOC, implementation and validation. 3. Compare approved stored revisions or checksums where safe and meaningful. 4. Review rollback and vendor handover.	Change requests; approved logic or project revisions; MOC; checksums or provenance records; validation results.	Actual changes and exceptions are attributable and reproducible within the approved evidence scope.	Online logic comparison, upload or download, firmware or setpoint change only with specific operations or vendor authorization.
P40	Examine portable devices and removable media (All)	Review maintenance and transfer paths into isolated or legacy systems. 1. Inventory engineering laptops, portable media and temporary vendor equipment. 2. Review approval, custody, scanning or transfer station and configuration practices. 3. Sample maintenance entry or exit records and exceptions. 4. Check restoration and contamination response arrangements.	Device or media register; vendor procedures; custody and maintenance records; approved transfer design.	Known temporary paths and exceptions are recorded against adopted policy; evidence avoids malware introduction.	Examine media controls through records and observation.
P41	Review supplier and shared service controls (All)	Connect outsourced access and responsibilities to actual evidence. 1. Identify critical integrators, MSPs, telecom or cloud services and OEMs. 2. Examine responsibilities, incident notice, access approval, support or patch, recovery and evidence access terms. 3. Sample access termination and supplier changes. 4. Resolve public agency contractor scope separately.	Contracts; responsibility matrix; service inventory; assurance reports with scope or period; supplier access records.	Third party claims are evaluated for scope, exceptions and period, alongside evidence of the operator's own controls.	Outreach or supplier disclosure only with engagement authorization; retain confidential contracts securely.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P42	Review physical and environmental dependencies (All)	Check whether cyber safeguards depend on unexamined physical access or utilities. 1. Conduct an authorized nonintrusive walkthrough with escort. 2. Review panel or control room access, cabling, remote cabinets, environmental and backup power dependencies. 3. Sample authorized access or maintenance records. 4. Record safety and engineering specialist dependencies.	Escort or permission; observations; access records; power or environment drawings; maintenance evidence.	Recorded observations identify time, location, escort and limitation.	Cabinet opening, electrical contact, lock bypass and alarm triggering only with written approval from the operating owner; site access is escorted.
P43	Review workpaper quality and information handling (All)	Make the result reproducible, controlled and candid. 1. Reconcile criteria to procedures, executions, evidence and findings. 2. Verify examiner, collector or reviewer and actual chronology. 3. Treat to be determined, pending, unknown, unexplained n/a and absent records as open items. 4. Check evidence origin, capture time or time zone, classification, integrity and custody; hash where appropriate, recording method. 5. Check retention or legal holds, access, versioning, secure transfer and destruction approval.	Cross reference index; quality review; evidence manifest or custody; controlled report; actual acceptance receipt.	A qualified reviewer checks that the evidence is sufficient for each conclusion.	Keep secrets, raw PII, SSI and exploitable configurations in controlled storage, and preserve held evidence.
P44	Resolve nuclear criteria and specialist authority (Electric)	Keep nuclear cybersecurity review within actual approved license or program boundaries. 1. Obtain current license status, orders or exemptions and approved cybersecurity plan through authorized access. 2. Have qualified nuclear compliance personnel establish 73.54 scope and protected functions or assets. 3. Obtain actual 73.55(m) review and 73.77 reporting criteria and program records. 4. Agree specialized competence, independence, safety and protected information handling. 5. Limit generic OT work to expressly approved objectives.	License or status; exemptions or orders; approved plan; protected asset and criteria inventory; specialist approval and actual program review or notice records.	Governing instruments and qualified specialized review support the agreed scope.	Plant connection, testing and any disclosure of protected information proceed only within a qualified, authorized nuclear engagement and its criteria.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P45	Review gas control room safety records (Gas)	Examine the applicable gas control room management program and its OT evidence through records and observation. 1. Obtain current 49 CFR 192.631 and decide full or limited paragraph coverage from actual functions, service counts and compressor facts. 2. Reconcile controller roles, shift or fatigue records, SCADA displays, alarm or change management, operating experience and training to the applicable paragraphs. 3. Trace record samples and every applicable review or test cadence to the applicable criteria and recorded timestamps. 4. Preserve gaps, permitted deviations and corrective work for qualified review. Apply 192.631 to gas control rooms; 195.446 covers hazardous liquid lines.	Written CRM scope, current rule, procedures, alarm, shift, change or training records, sample rationale, reviewer and criteria specific calendar.	Evaluate only the applicable paragraphs. Production tests proceed under written authorization; a complete pipeline safety inspection runs as its own engagement.	Live alarm inhibition, forced values, point actuation, backup switching, fatigue experiment or manual operation test only with written approval from the operating owner; examine approved historical records.
P46	Trace AMI meter to bill lineage (Electric)	Establish complete data lineage and the adopted collection or availability measures. 1. Confirm actual EDC, meter population, platform and third party boundaries. 2. Obtain approved stored exports for capture, validation, release and billing for a defined period. 3. Select normal, delayed, corrected, multisite and customer request examples with a recorded selection basis. 4. Compare actual precision, intervals, elapsed times and billing sources to each adopted clause. 5. Examine clock or zone and missing record limits; separate local nonvalidated access and PJM milestone evidence.	Meter or system population; sanitized timestamp, interval or validation exports; billing lineage; request and exception records; actual PJM criterion.	Trace each sample to source and criterion; report untested populations and actual measured intervals. Sample customer portal displays across the population.	Meter reconfiguration, HAN pairing, disconnect or reconnect, live query load or production billing change only with written approval from the operating owner.
P47	Review AMI authorization and onward access (Electric)	Determine whether customer instructions and recipient controls match adopted AMI duties. 1. Obtain common form or version, Board eligibility order or list and recipient or data field map. 2. Examine MFA access or confirmation design and approved historical records. 3. Sample consent, decline, historical or ongoing scope, revocation and onward transfer, including exceptions. 4. Trace authorization to transmission time and API/portal history. 5. Review security criteria, use restrictions, prohibited sale and anonymized academic access handling.	Forms; actual approved party record; permissions and revocations; redacted transfer logs; contracts or security controls; academic data release basis.	Evidence links named recipient, authorized account, field or time scope and actual delivery or revocation handling. Record any absent Board implementation order as an unresolved criterion dependency.	Use authorized nonproduction or sanitized records for every test of customer permissions and exports.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P48	Rehearse simultaneous AMI and breach notices (Electric)	Prepare accurate separate event classifications, recipients and time records. 1. Use a synthetic unauthorized release scenario. 2. Resolve 14:5-10.6(f) party or information scope and discovery time. 3. Independently screen BPU six hour, WQAA, public agency and ITPA triggers. 4. Record current recipient or channel and sequencing for every applicable duty. 5. Review escalation, deputies, evidence preservation, legal decisions and receipt capture.	Scenario or classification; separate clock register; current official channels; approved templates; escalation or receipt procedure.	Each duty has its own notice and window. ITPA State Police before customer sequence is evaluated where applicable; unanswered classification stops a readiness conclusion.	The exercise uses synthetic notices, customer communications and regulator submissions.
P49	Review AMI changes and semiannual reporting (Electric)	Verify developer impact controls and reproducible adopted metrics. 1. Build a nine metric source or definition crosswalk from final 10.8 text. 2. Reconcile reporting period, historical detail, counts and login measures to approved system records. 3. Obtain actual filing instructions or date and receipts. 4. Sample a developer affecting change, 90 day notice or evidenced immediate cyber exception and issue tracking. 5. Review nondiscriminatory access and authorized application analysis limits.	Metric dictionary or population; query lineage and reconciliations; filed reports or receipts; notices; change, exception or issue records.	Semiannual duty is distinguished from any quarterly language retained within metric detail; take the filing day and reporting period from the current instruction.	Production API change, code reverse engineering or third party application testing only with specific authority.
P50	Assess energy customer data integrity changes (Utilities)	Separate current TPS reporting from future supplier freeze implementation. 1. Confirm LDC/TPS roles, effective amendments and the explicit September 8, 2027 freeze applicability date. 2. Reconcile actual TPS customer or error populations and 30 day window; calculate applicable reporting threshold from final text. 3. Review historical qualifying reports, copies and correction or refund treatment. 4. Review freeze project design, direct customer authority, separate switch consent, EDI rejections, notices and merger or default exceptions using nonproduction cases. 5. Assign implementation owners or dates and vendor dependencies.	Role or license facts; adopted text; dated population or error calculations; report or credit records; project and nonproduction acceptance records.	Use the adopted customer threshold and the adopted implementation date for the supplier freeze. Report data integrity findings within the approved scope.	Supplier switches, freezes, customer notices and billing adjustments only with written approval from the operating owner; customer records stay with authorized staff.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P51	Coordinate OT changes with water safety duties (Water)	Link OT consequences to actual operator notices and asset program work. 1. Confirm system or rule scope independently of WQAA connection count. 2. With the licensed operator classify quality or pressure emergencies and planned treatment changes. 3. Review occurrence to call and planned change written notice records. 4. Reconcile asset plan certification, March 15 capital report, signatory training and future water loss audit interface. 5. Record engineering tasks outside the cyber engagement and current recipients or receipts.	PWS/system status; operator decision; change or emergency records; notice receipts; asset plan, report or calendar; specialist responsibility.	Cyber evidence supports defined interfaces; the operator or engineer owns water quality, asset engineering and certification determinations. Actual event onset differs from cyber detection.	Treatment changes, dosing or pressure manipulation, valve or hydrant operation, water sampling certification and engineering conclusions stay with the utility's licensed operators and engineers.
P52	Review spill prevention OT and reporting interfaces (All)	Prepare environmental response with malfunction, discharge and cyber triggers kept distinct. 1. Have environmental lead determine major facility or pipeline and substance or plan scope with current appendices. 2. Map detection, monitoring, prevention and safety devices to actual approved plans. 3. Review synthetic or authorized historical discharge and device malfunction cases, preserving knew or should have known times separately. 4. Trace immediate notice, two hour malfunction disposition and applicable written follow up to exact clauses; assess only current specific exceptions. 5. Reconcile DPCC/DCR submissions, changes, specialist signoffs and independent federal or local duties.	Capacity and coverage calculations; current rules or appendices; plans; device or alarm map; awareness, call or disposition timeline; exception evidence; submission receipts.	The 5.5 malfunction duty applies to the malfunction itself, whatever happens after it. Discharge notification applies to major facilities as well. Delays rest on actual evidence and regulator or legal assessment.	Spill simulation, detector disabling, alarm inhibition, valve operation, protected equipment shutdown or real emergency call only with written approval from the operating owner.
P53	Examine privacy rights and notice operations (All)	Verify enacted consumer rights using traceable safe records. 1. Confirm actual legal coverage, role, household consumers and exemption basis. 2. Reconcile notice versions to processing or recipient facts. 3. Select requests, refusals, extensions, appeals, portability or deletion and opt out or agent cases from a defined population. 4. Calculate each receipt or response window and check the notices the rule calls for and its permitted exceptions. 5. Review universal mechanisms with authorized synthetic or nonproduction evidence; record final rule status separately.	Coverage decision; data map; notices; redacted request or appeal population and timestamps; response and signal records; exception analysis.	Show response performance with records as well as policy, and explain missing populations, untested rights and unsupported exemptions.	Submit real consumer requests, erase data, expose PII, override legal holds or test live customer accounts only with authority.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P54	Examine privacy consent, safeguards and risk assessments (All)	Evaluate actual processing decisions and safeguards against enacted provisions. 1. Reconcile purpose, data, age or acquisition date inventory to sensitive data and high risk screens. 2. Examine required consent, equally easy revocation and actual cessation chronology. 3. Review minimization, incompatible use controls and safeguards proportionate to data nature or volume. 4. Trace heightened risk assessments to processing before it starts, benefits or risks, safeguards and authorized decisions. 5. Review restricted retention, regulator access and precise legal privilege basis with counsel.	Data or purpose map; actual consent or revocation records; age/COPPA decision; safeguard evidence; assessments and changes; retention or hold instructions.	Separate ordinary utility necessity, data specific exceptions and full entity exemptions; no assumption every AMI use is exempt or every assessment privileged.	Production consent withdrawal, destructive deletion, young consumer profiling test or public export of sensitive data only with written approval from the operating owner.
P55	Examine processor contract and assurance evidence (All)	Verify actual allocation and permitted assessment route. 1. Determine controller or processor roles from actual purposes or instructions. 2. Compare executed contract and subprocessor terms to each 166.16 requirement. 3. Review confidentiality, security allocation, request or breach assistance and end of service disposition. 4. Verify assessment access or actual controller consented annual independent route, qualified assessor, period, scope and exceptions. 5. Trace material gaps to corrective owners and evidence requests.	Executed terms or instructions; subcontractor register; allocation; service exit or assistance records; assessment rights or consented report; exceptions or actions.	Confirm contract terms and scope from the signed agreement.	Supplier outreach, contract disclosure, data transfer or deletion only with engagement specific authority.
P56	Reconcile TCPA full program audit and report (Utilities)	Connect OT findings to the actual annual process safety program. 1. Establish facility, process or program and approved anniversary from actual consent or order. 2. Reconcile state modifications, 2022 readoption, current federal amendments and their dates in a clause crosswalk. 3. Allocate every applicable full program element to competent reviewers; examine as built or operated PSI verification and actual audit participant or method records. 4. Reconcile corrective schedules and other open related findings. 5. Trace 12 month report contents, 90 day filing and receipt, plus NJRMP event or ownership changes.	Coverage or anniversary; complete current criteria crosswalk; team competence; PSI/audit/workpapers; findings or actions; annual report/NJRMP and receipts.	OT work is a defined contribution. A complete safety program conclusion rests on all applicable elements and qualified reviewers.	Process operation, chemical handling, SIS or interlock actuation, startup authorization and process safety certification stay with qualified process safety staff.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P57	Review interconnecti on portal control evidence (Electric)	Assess CIAP data protection, availability and workflow only against the applicable criteria. 1. Resolve Chapter 14:8 status or readoption, effective orders or tariffs and implementation with utility compliance. 2. Map CIAP/applicant/EDC/vendor boundaries and actual assigned responsibilities. 3. Examine authorized historical or nonproduction MFA, role, secure transfer and account separation records. 4. Reconcile uptime definition, stated hours, time zone and daylight saving treatment and public metrics to source records. 5. Sample workflow timestamps, validation, payment or status and notification preferences, plus approved map disclosure controls.	Current chapter or status and orders; actual tariff or implementation; architecture or roles; redacted access or transfer records; uptime and workflow populations; map approvals.	Each noncompliance finding rests on the reconciled current amendment. Report actual tested population or method and unresolved criteria precisely.	Live interconnection approval, grid control setting, production file upload, account cross access or public release of operational maps only with written approval from the operating owner.
P58	Resolve gas jurisdiction and operative instruments (Gas)	Approve the gas specific criterion inventory before execution. 1. Reconcile operator/OPID, legal entity and asset or function maps. 2. Obtain current Chapters 14:6/14:7, federal scope and actual TSA/agency instruments through authorized channels. 3. Resolve distribution/transmission/storage/LNG and full or limited CRM coverage with specialists. 4. Record each clause or version, effective dates, exclusions, owner and missing evidence before criteria approval.	Jurisdiction decision; current criteria and amendment history; specialist scope; actual authorization.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.
P59	Rehearse gas notice decisions in a tabletop (Gas)	Validate classification, distinct clocks and recipient readiness from historical or controlled tabletop records. 1. Select an actual authorized historical event or clearly labeled tabletop. 2. Have pipeline compliance staff classify the current state or federal triggers and exclusions. 3. Record event, discovery, learning, confirmed discovery and determination times separately with zone. 4. Calculate each applicable window using its own calendar and reconcile initial, update or final receipts. 5. Record missing fields, current channels, deputy and escalation; send no actual notice during the preparation test.	Trigger decisions; timeline; separate deadline calculations; current channels; historical receipts or clearly labeled tabletop observations.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P60	Reconcile gas drill coverage and calendar (Gas)	Check district, dispatch, field site, notice and report requirements against actual history. 1. Obtain current rule and all operator districts or divisions, call and dispatch centers. 2. Reconstruct actual drill dates, locations or types and attendance. 3. Check two year distribution coverage, prohibited two week proximity, field or tabletop cycles and the separate transmission annual/15 month or three year provisions. 4. Reconcile advance notices, any narrow exception and final report receipts. 5. Assign gaps and planned corrective work, and schedule any field drill through its own approval.	Complete drill population or history, attendance, current criteria, calendar, notices, evaluations and corrective records.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.
P61	Trace gas safety telemetry to operating records (Gas)	Assess integrity and availability of OT records used by qualified pipeline specialists. 1. Select an approved asset or event sample and safety objective. 2. Compare SCADA pressure, temperature or alarm timestamps and configuration to independent approved records and calibration evidence. 3. Trace approved control changes, operator qualifications and incident reconstruction to the owning safety program. 4. Record inconsistencies, evidence custody and process implications with the specialist. 5. Propose changes only through the actual safety or change approval process.	Asset or sample rationale; raw secure evidence references; clock, calibration or configuration records; independent confirmation; specialist review.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.
P62	Reconcile gas filings and supporting data (Gas)	Test the relationship between required reports, source records and actual submission evidence. 1. Determine applicable report types from the current full rule and asset classification. 2. Reconcile annual, leak or pressure test source systems and reporting periods to submitted records. 3. Verify actual dates, report content and receipts separately for each state or federal recipient. 4. Check known corrections, missing source data and the applicable event or working day or calendar day basis. 5. Assign open items and have the qualified compliance owner review the conclusion.	Applicable filing matrix; source to report reconciliation; current forms or criteria; period and timestamp evidence; receipts; corrections.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.

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

ID	Procedure	Objective and steps	Evidence to request	Review basis	Safety boundary
P63	Reconcile gas service interruption branches (Gas)	Check the separate interruption categories, awareness thresholds and follow up records in a tabletop rehearsal. 1. Reconcile the actual interruption population, start times, customer counts or types, season, road and critical customer facts. 2. Apply exact current 14:7-1.17(j)-(l) categories and exclusions with the compliance owner. 3. Keep awareness of 30 minutes or one hour of interruption separate from the subsequent 30 minute notice window. 4. Trace actual notice and prompt written follow up records. 5. For reportable incidents, test whether the separate 30 day amended corrective action report is triggered. 6. Record forms, receipts, source gaps and reviewer.	Interruption or event records; season, customer or road classifications; actual timestamps; contract exception decision; receipts; written and amended follow up records.	Evaluate the applicable clauses against the evidence. Each conclusion rests on a confirmed trigger, source and record. Record examiner, reviewer and limitations.	Records or interviews and authorized passive evidence only. Pause and escalate to the operating owner on a jurisdiction dispute, unsafe access or any request to actuate valves, pressure, logic or safety systems.

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

8. Reporting triggers

Confirm the current recipient and channel for each duty before an incident, record the event, trigger and submission times with the time zone, and keep each receipt. In a real incident, escalate immediately; this register supports a fast, correct decision.

ID	Who	Qualifying event	Trigger	Window	Basis
N01	NJ01-covered utilities	Defined ICS events	Detection	Within 6 hours	NJ01 Requirements 3(a)
N02	Covered public utility	Listed cyber attack or attempt with adopted service impact conditions	Becoming aware	Within 6 hours; confirm the current code	NJ02 14:3-6.7(a)6-7
N03	WQAA covered water purveyor	Statutory business information compromise or specified ICS effects	Employee made aware	Promptly; no numeric grace period asserted	NJ03 58:31-4.2(a)
N04	Public agency or government contractor	Cybersecurity incident reported to NJOHSP	Reasonable belief occurred	Within 72 hours	NJ05 52:17B-193.3(a)
N05	Covered holder of NJ resident PI	Breach meeting actual statutory conditions	Discovery and applicable statutory analysis	Expedient without unreasonable delay; State Police before customer disclosure	NJ06 56:8-163
N06	Maintainer on behalf of another	Covered breach in maintained records	Discovery	Immediately notify owner or licensee as specified	NJ06 56:8-163(b)
N07	Actual wastewater operator	Permit or rule defined discharge, bypass or noncompliance	Exact permit or rule trigger to determine	Applicable 2 hour or 24 hour discharge category	NJ12 and actual permit or current rule
N08	Actual facility or operator	Physical safety, environmental, federal, contract or insurer and local events	Instrument specific trigger to determine	Set from the current criteria	Actual utility facility, permit, federal or operator, local and contract instruments; see NJ-C23, NJ-C26, NJ-C30 and NJ-C37
N09	Covered AMI EDC/third party or onward recipient	Unauthorized release of covered customer information	Discovery	Within 48 hours; required recipients separately; coordinate independently applicable earlier or sequence duties	NJ16 14:5-10.6(f)
N10	Supplier of water	Qualifying emergency affecting quality, pressure or standards	Occurrence of emergency	Within 6 hours by telephone; distinct from cyber detection or awareness triggers	NJ19 7:10-2.4(b)

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

ID	Who	Qualifying event	Trigger	Window	Basis
N11	Responsible person for qualifying NJ hazardous discharge	Discharge under actual 7:1E scope and exceptions	Knew or reasonably should have known	Immediate; receipt within 15 minutes considered immediate. Applies to small spills as well; actual 5.6 delay basis requires review.	NJ18 7:1E-5.3; -5.6
N12	Actual major facility owner or operator	Discharge detection, monitoring, prevention or safety system or device malfunction	Knew or reasonably should have known of malfunction	Immediate; 15 minute measure, then disposition notice within 2 hours after initial notification	NJ18 7:1E-5.5(a)-(c)
N13	Actual TPS meeting adopted customer or error threshold	Incorrect billing incident meeting actual population or window tests	TPS became aware of incident	Written report within 10 business days to specified Board recipients and utility if consolidated billing	NJ17 14:4-7.14(a)-(b)
N14	Actual NJPDES permittee with 6.10(c) event	6.10(a)1i iv exceedance or (a)2 listed unpermitted discharge	Discharge commencement or permittee awareness; actual facts required	Initial telephone notice within 2 hours; revisions within 24 hours after awareness of need to revise	NJ24 7:14A-6.10(c)
N15	Actual NJPDES permittee with 6.10(d) event	6.10(a)1v toxic daily maximum, (a)3 other upset or bypass or (a)5 residual noncompliance	Discharge commencement or permittee awareness; actual facts required	Telephone notice within 24 hours; verify no earlier independently applicable category	NJ24 7:14A-6.10(d)
N16	NJPDES (a)1-3 or 5 category	Required written information pending submission	Discharge commencement or awareness; actual applicable basis	Within 5 days; immediately correct missing or incorrect required facts; additional (f) documentation where applicable	NJ24 7:14A-6.10(e)-(f)
N17	Actual NJPDES serious violation	Serious violation as defined by applicable rule	Violation	Separate written report within 30 days, in addition to earlier oral or written duties	NJ24 7:14A-6.10(i)
N18	Applicable NJ gas operator	Reportable state gas incident	Operator learns of the reportable incident	Immediately; no later than one hour after learning. Verify the current state event categories and channel.	NG01: 14:7-1.17(b)-(f)

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

ID	Who	Qualifying event	Trigger	Window	Basis
N19	Applicable NJ gas operator	Follow up report of each reportable state incident	Actual incident date	Within 15 days after the incident; additional new information notices have separate as soon as practicable requirements.	NG01: 14:7-1.17(e), (g)-(h)
N20	Actual Part 191 covered gas operator or event	Qualifying current 191.3 incident	Discovery; retain separate confirmed discovery time	Earliest practicable moment following discovery; no later than one hour after confirmed discovery. Use the current adjusted dollar threshold.	NG02: 191.5(a)-(b); NG07
N21	Actual Part 191 covered gas operator or event	Revision or confirmation of initial incident notice	Confirmed discovery of qualifying incident	Within 48 hours after confirmed discovery, to extent practicable. Confirm unchanged estimates too.	NG02: 191.5(c)
N22	Operator with actual 191.23(a)(1)-(9) condition after exclusions	Ordinary safety related condition written report	Day first determined; separate day first discovered	Received within five working days after determination day, and no later than ten working days after discovery day. Exclude Saturdays, Sundays and federal holidays.	NG03: 191.25(a),(c)
N23	Qualifying gas transmission MAOP exceedance	191.23(a)(10) category	Actual qualifying exceedance	Federal written report received within five calendar days of exceedance. Resolve exact trigger and current channel.	NG03: 191.25(b)-(c)
N24	Applicable NJ pipeline operator	Specified MAOP exceedance beyond allowed device margin	Discovery of qualifying exceedance	State notification immediately upon discovery; formal report under 191.25 separately classified.	NG01: 14:7-1.26(g)
N25	Actual 14:7-1.17(j) gas interruption category, subject to (l)	Heating season 100-customer interruption, defined healthcare facility or designated airport category	Operator awareness that service has been interrupted for 30 minutes	Report to Board no later than 30 minutes from that awareness. Resolve exact categories, definitions and contract exclusion; prompt detailed written follow up under (m) separately.	NG01: 14:7-1.17(j), (l)-(m)

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

ID	Who	Qualifying event	Trigger	Window	Basis
N26	Actual 14:7-1.17(k) gas interruption category, subject to (l)	Nonheating season 100-customer interruption, listed highway lane closure or specified critical customer	Operator awareness that service has been interrupted for one hour	Report to Board no later than 30 minutes from that awareness, in addition to any applicable (j) notice. Resolve exact categories, definitions and contract exclusion; prompt detailed written follow up under (m) separately.	NG01: 14:7-1.17(k)-(m)
N27	Reportable state gas incident whose corrective measures or recommendations came after the follow up	Conditional amended corrective action report	Incident date; retain evidence of when measures or recommendations became available	File amended report within 30 days of the incident, stating corrective measures and recommendations. The initial and 15 day follow up deadlines stay as set.	NG01: 14:7-1.17(i)

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

9. Recurring and event based duty calendar

Use the Calendar sheet to record whether each duty applies, the owner and deputy, the last event, the next due date and how it was calculated.

ID	Duty	Applies to	Trigger	Timing	Prepare	Basis
D01	Critical system inventory and risk or method review	NJ01 covered entity	Prior actual annual review	Annual; establish actual review period	Inventory or change reconciliation, risk assessment or treatment and methodology review with owners.	NJ01 Requirements 1
D02	Executive cyber certification	NJ01 covered entity	Annual cycle	December 31 after historical implementation; verify current instructions	Actual authorized signer, scope, evidence and receipt; document limited NERC overlap if used.	NJ01 Accountability
D03	Cyber response exercise	NJ01 covered entity	Last qualifying actual exercise or incident	At least once every 24 calendar months under order conditions	Actual date, scenario or coverage, lessons and corrective actions.	NJ01 Requirements 4
D04	Awareness program review	NJ01 covered entity	Actual review or Board interpretation	Biannually is ambiguous; obtain the Board's written interpretation	Record actual interim management practice and written clarification separately.	NJ01 Requirements 5
D05	WQAA framework revision and submission	Covered purveyor or chosen framework	Final chosen framework revision publication	Within 180 days of publication; establish actual edition or date	Current chosen framework, revised program or control mapping and NJCCIC receipt.	NJ03 58:31-4.1(b)
D06	Annual cyber certification and assessment filings	Actual WQAA purveyor and current instructions	Annual reporting cycle	DEP lists December 31; confirm current portal or form instructions	Ownership specific signer, controls assessment, current program and receipt.	NJ03; NJ04
D07	Planned treatment change notification	7:10-2.4(a) qualifying change	Actual planned change	Written notice at least 5 working days before change	Operator or engineer consequence decision; schedule or notice and receipt.	NJ19 7:10-2.4(a)
D08	Asset plan and capital reporting	Actual 7:10-6 scope	Annual cycle; last plan certification; ownership or status change	March 15 annual capital report; plan certification every 3 years or ownership or status change	Qualified operator or engineer and responsible individual signoffs; separately track annual compliance or training.	NJ19 7:10-6.3(c); -6.4(a)
D09	Water loss audit interface	Actual applicable water system scope	Future operative provision and actual cycle	Rule specifies effective March 31, 2027; authenticate 7:19-6.4	Assign engineering or data owners; acquire current actual audit method and scope before stating a completion date.	NJ19 7:10-6.3(b)9

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

ID	Duty	Applies to	Trigger	Timing	Prepare	Basis
D10	AWIA RRA and ERP cycle	Community system over 3,300 people	Actual RRA certification and prior review cycle	ERP certification within 6 months of actual RRA certification; review or update at least every 5 years	Actual population, full RRA/ERP scope and EPA certification receipts, kept apart from the WQAA connection count.	F01 AWIA Section 2013
D11	AMI reporting metrics	14:5-10 covered EDC	Actual reporting period	Semiannual; obtain current specific filing instructions	Nine metric crosswalk, monthly or history detail, current recipients and receipt; no invented filing day.	NJ16 14:5-10.8
D12	AMI developer impact notice	Covered EDC technical change	Planned adversely affecting technical change	90 days before change unless necessary for immediate cyber concern or vulnerability	Actual impact assessment, developer population, notice receipt or documented emergency basis.	NJ16 14:5-10.7(b)
D13	Supplier freeze implementation	Actual LDC/TPS scope	Explicit adopted future applicability	14:4-2.6(d) for requests on or after September 8, 2027; -2.6A states after September 8, 2027	Resolve exact operative wording before edge date cases; plan EDI, authorizations, exceptions and notices.	NJ17 14:4-2.6(e); -2.6A(a)
D14	TCPA compliance audit	Actual TCPA Program 3 covered process	Last actual covered annual audit	Every year; separate from OSHA PSM three year interval	Full program, as built or operated verification, actual participants or methods and corrective schedule.	NJ20 7:31-4.1(c)13
D15	TCPA annual report	Actual Program 3 owner or operator	Approved consent or order anniversary	Within 90 days of anniversary, covering prior 12 months	Obtain signed approval or anniversary changes; report and required attachments or receipt.	NJ20 7:31-4.9
D16	NJRMP resubmission and changes	Actual TCPA scope	Last full RMP; actual process, level or ownership change	At least every 5 years plus actual earlier event driven requirements	Separate resubmission from correction; actual state or federal chemicals and transfer approvals.	NJ23; NJ20 7:31-7
D17	Privacy rights and consent revocation	Actual NJDPA covered processing	Verified request, appeal or consent revocation receipt	Request or appeal 45 day duties; properly justified request extension 45 days; consent cessation no later than 15 days	Separate clocks or notice requirements and actual response evidence; exceptions need actual statutory basis.	NJ07 56:8-166.7; -166.12(a)6
D18	Optional independent processor assessment route	Actual NJDPA processor using alternative with controller consent	Chosen permitted contractual assurance route	At least annually at processor expense when this alternative is selected	Actual consent, qualified independent assessor, accepted criteria, report scope or period and access on request.	NJ07 56:8-166.16(e)4(b)(ii)

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

ID	Duty	Applies to	Trigger	Timing	Prepare	Basis
D19	Other program specific calendars	Actual NERC, NRC, gas operator, permit, local or contract scope	Actual governing instrument and qualifying facts	Set from the current instrument and the last or trigger dates	Create separate rows for every applicable clause, submission, review, training, test and notice.	F02; F09; F12; F13; F14; NJ-C37
D20	Anticipated bypass prior notice	Actual NJPDES anticipated bypass	Planned bypass date and actual conditions	At least 10 days before if possible; the operator determines the exact applicable conditions	Necessity, alternatives, signed statements and current agency channel or receipt; record the written authorization for any production bypass.	NJ24 7:14A-6.10(g)
D21	Gas distribution drill coverage	Applicable distribution operator, district or division and call or dispatch center	Actual prior drills and covered organizational units	At least every two years, with district or division drills spaced at least two weeks apart. Reconcile initial transition, later four year field site cycle and tabletop limits from the actual rule.	Unit population, actual dates, types or locations, attendance and gap plan.	NG01: 14:7-1.9(f)
D22	Gas drill notice and final audit report	Actual drill under 14:7-1.9(f)	Planned drill and actual drill occurrence	Notice at least five business days before; narrow rainy day or similar weather exception requires as soon as possible notice no later than two hours before. Final audit report within two months after. Track separate records.	Approved schedule, exception evidence if used, notice or report receipts and responsible people.	NG01: 14:7-1.9(g)
D23	Gas transmission emergency closure drill	Actual applicable transmission operator	Actual prior drill dates and calendar years	At least once each calendar year with no interval over 15 months; field site and normal business hour conditions at least once every three calendar years; tabletop no more than two of three years.	Current full section, actual dates, type or location and permissions; specialist review.	NG01: 14:7-1.10(f)

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

ID	Duty	Applies to	Trigger	Timing	Prepare	Basis
D24	Gas state annual report copies	Applicable operator and asset or report class	Close of actual calendar reporting year	Selected state copies due no later than March 15 for the preceding calendar year. Review the federal filing classification, exceptions and the complete current state section.	Current forms, asset applicability, period reconciliation and state or federal receipts.	NG01: 14:7-1.26(c); NG05
D25	Gas state leak classification inventory	Applicable pipeline operator	Close of actual calendar reporting year	January 31 for the preceding calendar year under the selected adopted clause.	Open unrepaired leaks by grade, district or division and municipality; current Bureau format; receipt.	NG01: 14:7-1.26(d)1
D26	Gas test records and excavation notice	Applicable gas transmission test or integrity examination	Actual test date or planned qualifying excavation	Pressure test records within one month after test; direct assessment or examination excavation notice at least five business days before. Keep separate event records.	Pressure or temperature charts, test dates, current complete reporting fields, location and notice or receipt.	NG01: 14:7-1.26(d)8,(f)
D27	Gas CRM paragraph level review calendar	Actual 192.631 coverage after full or limited scope determination	Authenticated applicable paragraph and last actual activity	Set from current 192.631 paragraph timing. Set the interval for each CRM activity from its own paragraph.	Current rule; full or limited coverage decision; actual past records and individual approved deadline calculations.	F14; NG04; NJ-Q19

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

10. Questions to resolve before scope is final

Each question names the information to obtain, the records that answer it, a question you can send to the agency or the record holder, and who should own it. Close a question in the Open questions sheet once the answer, its authority and the resulting scope change are recorded.

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q01	Current BPU code and orders (All utilities)	Obtain current 14:3-6.7, relevant amendments, operative utility orders and entity jurisdiction determination. Obtain full current 14:3 and all amendments or orders; reconcile entity jurisdiction and system boundary. Build a clause, version or effective date table, retaining older wording and supersession evidence.	Full code or source notes; later Register items; utility charter; tariff or franchise and relevant BPU orders.	For each named utility or entity and facility, which current 14:3-6.7 provisions and later BPU orders govern, and what instrument supports each inclusion or exclusion?	Compliance or legal; Before final criteria approval
NJ-Q02	WQAA guidance conflict (Water)	Reviewed enacted text verifies prompt qualifying incident reporting, the separate agency audit clock and the more than 500 definition. Reconcile conflicting current guidance, any additional controlling authority and actual system facts. Retain supported subanswers separately from unresolved interpretation. Place exact enacted 58:31-4.2 and current DEP/NJCCIC guidance side by side; isolate prompt reporting versus 30 day audit language and more than 500 versus 500-or more screening. Draft a focused question for review before it is sent.	Exact statute or guidance versions; responsible recipient instructions; system classification and independently supported connection count.	For 58:31-4.2, please reconcile prompt employee awareness reporting with the DEP 30 day summary and distinguish the separate agency audit clock. Which enacted provision supports coverage at exactly 500 connections, and which recipients or channels apply?	Legal or incident lead; Before approving reporting tree
NJ-Q03	WQAA implementation and filings (Water)	Obtain current NJCCIC implementing requirements, portal instructions, actual framework, version or final publication dates, filing receipts and applicable insurance standards. Obtain current NJCCIC program, portal, form or signatory instructions and insurance standards. Reconcile actual framework final publication or revision date, controls assessment and submission receipts.	Current official instructions or forms; entity or signatory facts; actual framework or version; membership, filing and insurance records.	Which current program, framework version, publication or revision dates, signatory rules, portal or form and adopted insurance standards apply to this purveyor, and can the owner supply submission receipts and policy evidence?	Water compliance; Before certification support

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

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q04	Biannually (All covered utilities)	Obtain Board written interpretation of 2016 awareness program review frequency. Document any interim frequency as management practice. Locate the exact awareness program review phrase and any later authoritative interpretation. Ask whether biannually means twice per year or every two years in this order. Keep interim management practice separately labeled.	Original signed order; later orders or correspondence; actual training review history and documented interim decision.	For the awareness program review provision in order AO16030196, does biannually mean twice each year or once every two years? Please identify any controlling later order or written interpretation and its effective application.	Utility compliance; Before closing training criterion
NJ-Q05	Privacy codification (Covered utility or customer processing)	Authenticate current privacy statute or history, actual utility and processing coverage or exemptions, and any final 13:45L adoption. Obtain filed text and effective or compliance dates before privacy sign off. Authenticate current statute, any final 13:45L adoption, Register history, effective or compliance dates and amendments. Separate proposals from enacted duties and actual governmental or processing exemptions.	Current statute, rule or source notes; filed adoption if present; entity and personal data processing map; contracts and supported exemption analysis.	What filed adoption, Register citation, complete current 13:45L text and effective or compliance dates exist, if any, and which entity or processing exemptions actually apply to this utility?	Privacy counsel; Before privacy criteria sign off
NJ-Q06	Utility chemical or process safety coverage (Utility chemical or process interfaces)	Determine whether actual utility treatment chemicals, fuel storage or processes trigger TCPA, PSM or RMP. Obtain operative state or federal instruments, inventory or quantity calculations, registration and approved plans. Collect actual chemicals or mixtures, quantities and process boundaries; calculate coverage under current TCPA, incorporated federal RMP and PSM independently, including public worker jurisdiction. Reconcile conflicting or stricter state provisions.	Inventory/SDS; quantity and process calculations; current state or federal clauses and compliance dates; registrations, consent orders and approved program records.	For each listed utility process and maximum intended inventory, which TCPA, RMP and PSM provisions apply, what calculation and current incorporated version support that result, and who has public or private worker jurisdiction?	Process safety or legal; Before utility process safety criteria approval

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

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q07	Wastewater operative criteria (Wastewater)	Agency current NJPDES index and Chapter 6 copy are available. Obtain the actual complete permit or modifications and reconcile current reporting clauses, event categories, receiving treatment works and local conditions. Obtain complete current NJPDES permit and modifications, local or receiving treatment works conditions, current 6.10 text and channels. Build separate event category and follow up branches from actual clauses.	Complete permit or modifications; discharge or process and DTW facts; approved emergency contacts; current forms; past notice or receipt samples.	Please provide the complete current NJPDES permit and modifications, local or receiving treatment works conditions, event categories and current notice channels. Which exact clauses require each immediate, oral, written and follow up notice?	Permit owner or legal; Before approving reporting tree
NJ-Q08	Current controlled gas operator security criteria (Gas)	Obtain any current TSA gas pipeline operator directives, amendments, approved plans and applicability instructions through authorized operator channels. Confirm the actual designated operator and effective version. Keep SSI and other controlled materials out of public downloads. Have the actual operator establish designation and provide controlled current TSA instruments, amendments and approved plans through its authorized repository. Record version and access authority, keeping SSI in controlled storage.	Designation or applicability evidence; controlled instrument index; approved plan or version; amendments; authorized specialist access and handling rules.	Through the operator's authorized security repository, can the designated owner confirm current TSA applicability, exact directive or amendment versions, approved plan and authorized reviewer access or handling restrictions? Send SSI only through approved secure channels.	Operator security lead; Before gas criteria approval or applicable tests
NJ-Q10	Local and bistate instruments (All; facility dependent)	Collect actual municipal, county, authority or compact, permit, consent order, franchise or contract, OEM/LEPC and insurance records. Create one inventory per legal entity and site: municipality or county, authority or compact, franchise, permits, contracts, consent orders, emergency or insurance duties. Search only the actual jurisdictions and obtain signed or current documents.	Entity or site IDs; charters or compacts; permits; local ordinances; tariffs or franchises; contracts; insurance and emergency plan records.	For each legal entity and site, which municipality or county, authority or compact, franchise, permit, consent order, contract, insurance and emergency plan instruments govern, and who can supply the signed current versions?	Facility/legal/PM; Before final facility scope approval

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

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q11	Assurance basis and auditor appointment (All)	Agree engagement standard or basis, competence, independence, intended users, regulator direction and GDF appointment before calling any work a statutory independent audit. Agree objective, users, audit or assurance basis, period, criteria, competence, independence, deliverables and limitations. Obtain actual regulator direction or appointment where required. Define examiner or reviewer responsibility and safety authority.	Signed engagement or scope; qualifications and independence record; actual regulator direction; rules of engagement; reporting and secure evidence agreement.	What decision will the audit support, for whom and for which period? Which criteria and assurance basis are agreed; is a regulator directed independent audit or appointment required; and who approves independence, evidence access and safe fieldwork authority?	Engagement sponsor/GDF; Before fieldwork
NJ-Q12	Other actual federal or contract duties (All; federal or operator dependent)	Identify actual additional federal, license, contract and regulator duties. Recheck published final instruments and actual coverage before criteria approval. Check the published final CIRCIA text, effective date, coverage and any exceptions once it issues. Separately resolve actual nuclear licenses, federal or operator and contract duties.	Federal Register/CISA instruments and effective dates; actual licenses, operator designation, contracts and qualified specialist decisions.	Which actual federal licenses, registrations, operator designations and contracts add obligations? Before any CIRCIA conclusion, what published final instrument, effective or compliance date and coverage analysis support it?	Sector legal or compliance; Before final criteria approval
NJ-Q14	AMI implementation instruments (Electric/EDC and actual third parties)	Obtain the actual Board third party eligibility order or list, current common form, utility specific implementation and semiannual reporting instructions. Take approved recipients, the filing day, the revocation service level and the PJM implementation date from the current instruments. Locate the actual 14:5-10.6(b) implementation order, process or list, common release form and semiannual filing instructions. Obtain actual EDC implementation, authorization or revocation and reporting records.	Current Board order or list; common form or version; EDC instructions; AMI data lineage; consent and recipient records; metrics and receipts.	For 14:5-10.6(b), what current implementing order, eligibility or approval process, recipient list, common customer release form and semiannual filing instructions govern this EDC? Please identify current versions and effective dates.	EDC compliance or data owner; Before AMI criteria acceptance

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

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q15	Environmental and water source reconciliation (Water or wastewater and conditional utility facilities)	Obtain later amendment histories, actual current permits or plans, Chapter 7:1E Appendices A/B and actual water system or major facility facts. Obtain omitted 7:1E appendices and later amendments; reconcile current water or environmental rules, chemical or capacity exceptions and actual approved plans. Keep reporting scope distinct from major facility plan coverage.	Current complete rules or appendices and histories; storage capacities or chemicals; actual permits and approved DPCC/DCR, water and emergency plans.	Please provide complete 7:1E Appendices A/B, intervening amendments, current water or environmental rules and this site's capacities, permits and approved DPCC/DCR/emergency plans. Which reporting duties apply independently of major facility plan coverage?	Environmental or water specialist; Before reporting and fieldwork approval
NJ-Q16	2027 implementation calendar (Water, electric or gas as applicable)	Verify applicable supplier freeze date wording, actual PJM Order 2222 milestone and water loss audit scope. Assign implementation projects separately from currently due operational duties. Verify supplier freeze wording at the exact boundary date, operative PJM/FERC Order 2222 implementation instrument and actual water loss audit scope or method. Separate effective date, compliance date and operator project milestone.	Final instruments, current PJM/FERC tariff or order schedule and EDC program, actual water system scope and planned projects.	Which final instrument fixes each 2027 supplier freeze boundary, current PJM/FERC Order 2222 implementation milestone and applicable water loss audit method or date? Is the date an effective date, compliance deadline or internal project milestone?	PM and sector compliance; Before approving future duty schedule
NJ-Q17	DER/CIAP operative status and measurement (Electric/EDC)	Board approval of Chapter 14:8 readoption is evidenced in QX25080483 minutes. Obtain the filed readoption or current chapter and later orders or tariffs. Use QX25080483 minutes and June 2026 final publication as leads to the filed Chapter 14:8 readoption. Obtain full current chapter, later orders and tariffs. Separately obtain actual CIAP deployment and clarify EST/daylight saving, availability window and measurement rules.	Filed readoption or effective history; current chapter; orders or tariffs; actual platform or developer agreements; uptime or time zone and exception evidence.	For QX25080483, what filed readoption notice or current 14:8 text and later implementation orders govern? For CIAP availability, is stated EST fixed standard time or local civil time, and what window, denominator, maintenance exclusions and outage evidence govern measurement?	EDC compliance or legal and platform owner; Before CIAP criteria acceptance

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

ID	Question	What to obtain	Records to gather	Question to ask	Owner and timing
NJ-Q18	Complete current NJ gas rules and jurisdiction (Gas)	Obtain current full Chapters 14:6 and 14:7, later amendments, federal incorporation editions, agency or operator orders and jurisdiction records. The 2023 final amendments omit unchanged paragraphs. Determine actual intrastate or interstate and distribution/transmission/storage/LNG boundaries, current reporting instructions and specialist review before treating the selected clauses as operative engagement criteria. Obtain current full 14:6 and 14:7, later changes and incorporated federal editions. Resolve legal operator, OPID, interstate or intrastate and distribution/transmission/gathering/storage/LNG functions with specialists. Crosswalk selected adopted clauses to current text.	Current full chapters or source notes; actual orders or jurisdiction instruments; OPID/operator maps; functions; permitted specialist access.	Please provide complete current Chapters 14:6/14:7, source notes and later orders, and confirm the legal operator, OPID, interstate or intrastate status and distribution/transmission/gathering/storage/LNG functions with supporting jurisdiction records.	Gas compliance or legal owner and qualified pipeline safety specialist; Before gas criteria approval and any field method authorization
NJ-Q19	Current federal gas definition, reporting and CRM detail (Gas)	The official 2026 property damage amount and effective period are verified (NG07); January 2026 transmission, gathering or storage instructions are identified (NG08). Obtain licensed incorporated standards lawfully and actual operator facts. Controlled TSA criteria remain under NJ-Q08. Use the verified 2026 monetary notice and current identified instructions, then authenticate complete Part 191 definitions, exclusions, asset specific report sections or forms and actual 192.631 full or limited paragraph scope and timing. Obtain incorporated standards lawfully and retain licensed access or version.	Current complete rule or history; official annual threshold notice; asset specific current forms or instructions; CRM functions, service or compressor facts and actual program records; licensed incorporated standards.	For the actual gas facilities, what current Part 191 clauses, exclusions, asset specific forms and 192.631 full or limited paragraph duties apply? Please supply service, compressor or controller facts and lawful access to each incorporated standard. Keep controlled TSA review separate under Q08.	Pipeline compliance owner with legal and control room specialists; Before gas reporting decision tree, calendar approval or an audit conclusion

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

11. Sources

Official legal, regulatory and standards sources used in this set. Technical guidance such as NIST publications becomes binding when an instrument adopts it.

ID	Source	Where to look	What it says
NJ01	BPU Cyber Security Program order AO16030196 (signed order) https://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6AJD.pdf	Requirements 1-5; Implementation; Accountability	Adopted March 18, 2016; effective March 28, 2016.
NJ02	BPU 2022 readoption and adopted amendments https://www.nj.gov/bpu/pdf/rules/R.2022%20d.102%20%2854%20N.J.R.%201612%28a%29%29.pdf	Adopted N.J.A.C. 14:3-6.7(a)6-7; distinguish final text from comments	Adopted rule, 54 N.J.R. 1612(a), August 15, 2022. N.J.A.C. 14:3-6.7(a) requires a report to the Board within six hours of becoming aware of listed incidents, including a cyber attack resulting in outages or service issues or a confirmed breach. Checked November 3, 2026.
NJ03	Water Quality Accountability Act amendments, P.L. 2021, c. 262 https://pub.njleg.gov/bills/2020/PL21/262_.HTM	N.J.S.A. 58:31-2, -4, -4.1, -4.2, -6 to -8	Enacted law. Covers owners of public community water systems with more than 500 service connections; cybersecurity program, NJCCIC membership, prompt incident reporting and NJCCIC triggered audits. Checked November 3, 2026.
NJ04	DEP WQAA implementation page https://dep.nj.gov/watersupply/drinking-water-systems/water-quality-accountability-act/	Deliverables; cybersecurity; FAQs	Agency implementation guidance; the statute controls where the two differ.
NJ05	Public agency and qualifying government contractor incident reporting https://pub.njleg.state.nj.us/Bills/2022/PL23/19_.HTM	P.L. 2023 c.19; N.J.S.A. 52:17B-193.2 and -193.3	Enacted law, N.J.S.A. 52:17B-193.3(a). Public agencies and government contractors report a cybersecurity incident to the New Jersey Office of Homeland Security and Preparedness within 72 hours of reasonably believing it occurred. Checked November 3, 2026.
NJ06	Identity Theft Prevention Act 2019 amendments https://pub.njleg.state.nj.us/Bills/2018/PL19/95_.HTM	N.J.S.A. 56:8-161 and -163	Enacted law, N.J.S.A. 56:8-163. Customer notice in the most expedient time possible and without unreasonable delay; report to the Division of State Police before customer disclosure under 56:8-163(c)(1). Checked November 3, 2026.
NJ07	New Jersey Data Privacy Act enacted chapter https://pub.njleg.state.nj.us/Bills/2022/PL23/266_.HTM	56:8-166.4 through -166.16; enacted rights, security, consent, assessments and processor provisions	Enacted P.L. 2023 c.266 read, including operational provisions; effective January 15, 2025.
NJ08	NJ Consumer Affairs privacy law FAQ https://www.njconsumeraffairs.gov/ocp/Pages/NJ-Data-Privacy-Law-FAQ.aspx	Scope; rights; implementation dates	Agency explanatory guidance.
NJ09	NJ Consumer Affairs proposals https://www.njconsumeraffairs.gov/Proposals	Privacy rule status and adoption follow up	

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

ID	Source	Where to look	What it says
NJ10	DEP Toxic Catastrophe Prevention Act program https://dep.nj.gov/brp/tcpa/	N.J.S.A. 13:1K-19 et seq.; N.J.A.C. 7:31; compliance audit guidance	
NJ11	DEP TCPA rule index https://dep.nj.gov/rules/current-rules-and-regulations/njac7_31-2/	N.J.A.C. 7:31 and incorporated 40 CFR Part 68	
NJ12	DEP wastewater emergency response guidance https://dep.nj.gov/dwq/erp/	N.J.A.C. 7:14A-6.10; actual NJPDES permit	Agency guidance distinguishes two hour and 24 hour reporting categories.
NJ14	BPU current rule index https://www.nj.gov/bpu/agenda/rules/	Chapter 14:3 readoptions and amendment history	Official index points to OAL/Lexis and later adopted amendments.
NJ15	OAL public code access https://www.nj.gov/oal/rules/accessp/	Public Administrative Code and New Jersey Register access	OAL identifies the free public code as unofficial and updated semimonthly.
F01	EPA AWIA Section 2013 https://www.epa.gov/waterresilience/awia-section-2013	Risk and resilience assessment and emergency response plan	Federal program: community water systems serving more than 3,300 people; six month ERP interval follows actual RRA certification.
F02	NERC CIP reliability standards https://www.nerc.com/standards/reliability-standards/cip	Current applicable CIP versions, implementation plans and registration	FERC Order No. 919 (effective May 26, 2026) approved CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3. FERC Order No. 907 (effective September 2, 2025) approved CIP-015-1.
F03	NIST SP 800-82 Rev. 3 https://csrc.nist.gov/pubs/sp/800/82/r3/final	Guide to Operational Technology Security	Final technical guidance.
F04	NIST SP 800-115 https://csrc.nist.gov/pubs/sp/800/115/final	Assessment planning, rules of engagement and reporting	
F05	NIST SP 800-53A Rev. 5 https://csrc.nist.gov/pubs/sp/800/53/a/r5/final	Examine, interview and test assessment methods	
F06	OSHA process safety management https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119	1910.119 applicability; management of change; (o) compliance audits	Federal safety rule; three year audit requirement when applicable.
F07	EPA risk management rule https://www.ecfr.gov/current/title-40/chapter-I/subchapter-C/part-68	Current Part 68, covered processes and applicable amendments	Official federal eCFR route.
F09	TSA security directives for pipelines and rail https://www.tsa.gov/sd-and-ea	SD Pipeline-2021-02G; SD Pipeline-2021-01G	SD Pipeline-2021-02G is effective May 3, 2026 through May 2, 2027. Reporting directive SD Pipeline-2021-01G posted January 15, 2026. Checked November 3, 2026.
F12	NIST Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework	Final CSF; chosen framework and organizational profile	Voluntary framework, with potential adoption by WQAA or other binding instruments.

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

ID	Source	Where to look	What it says
F13	NRC digital systems cybersecurity rule https://www.ecfr.gov/current/title-10/chapter-I/part-73/subpart-F/section-73.54	10 CFR 73.54; incorporated 73.55(m) review and 73.77 notifications	
F14	PHMSA gas pipeline control room management https://www.ecfr.gov/current/title-49/subtitle-B/chapter-I/subchapter-D/part-192/subpart-L/section-192.631	49 CFR 192.631(a)-(j); incorporated standards in 192.7	
NJ16	AMI data access adopted rules, R.2026 d.085 https://www.nj.gov/bpu/pdf/rules/R.2026%20d.085%20(58%20N.J.R.%201845(a)).pdf	14:5-10.1 through -10.8; final adopted text, Register pages 1860-1861	Adopted June 30, 2026; effective August 3, 2026. Final operative text read, including changes from proposal.
NJ17	Energy competition adopted amendments, R.2026 d.102 https://www.nj.gov/bpu/pdf/rules/R.2026%20d.102%20(58%20N.J.R.%202169(a)).pdf	14:4-2.6(d)-(e), -2.6A, -7.14; final adopted text	September 21, 2026 Register, 58 N.J.R. 2169(a); selected operative amendments read.
NJ18	DEP DPHS rule text, January 20, 2026 https://dep.nj.gov/wp-content/uploads/brp/dphs/njac-7-1e-1.20.26.pdf	7:1E-1.6, -2, -3, -4, -5.3 through -5.8	
NJ19	DEP Safe Drinking Water Act rule text https://dep.nj.gov/wp-content/uploads/rules/rules/njac7_10.pdf	7:10-2.4; -6.1 through -6.4; selected operative sections	
NJ20	DEP TCPA state rule courtesy copy https://dep.nj.gov/wp-content/uploads/rules/rules/njac7_31.pdf	7:31-1.1; -4.1(c)13,14,23; -4.9; -7.4	Copy itself is dated February 1, 2016.
NJ21	TCPA notice of readoption https://dep.nj.gov/wp-content/uploads/rules/readopt/readopt-20221107b.pdf	Readoption notice, both pages	Notice states effective September 24, 2022 and expiration September 24, 2029; November 7, 2022 Register publication.
NJ22	DEP release prevention program updates https://dep.nj.gov/brp/program-updates/	March 2024 TCPA update; April or September 2026 DPHS updates	
NJ23	DEP NJ Risk Management Plan instructions https://dep.nj.gov/brp/tcpa/rmp/	Resubmission, correction and ownership instructions; 7:31-7.1(c)5,11	Agency guidance distinguishes five year full resubmission from event driven changes and corrections.
NJ24	DEP NJPDES conditions applicable to all permits https://dep.nj.gov/wp-content/uploads/dwq/pdf/n.j.a.c/njac714a_sub06.pdf	7:14A-6.10; actual permit and modifications	
NJ25	Consumer Affairs adoption index https://www.njconsumeraffairs.gov/Pages/adoptions.aspx	Adoption listing reviewed October 16, 2026; newest visible entry October 5, 2026	

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

ID	Source	Where to look	What it says
NJ26	DEP DPHS program and current appendices https://dep.nj.gov/brp/dphs/	Scope; current rules, Appendix A/B and 2026 plan instructions	Current agency program page read; last update September 23, 2026.
NJ27	DER interconnection and CIAP adopted amendment https://www.nj.gov/bpu/pdf/rules/R.2026%20d.010%20(58%20N.J.R.%2072(a)).pdf	14:8-5.13(d); selected -5.8 and -5.11; final text Register pages 98-99	Adopted November 21, 2025; effective January 5, 2026. Selected final clauses read.
NG01	NJ natural gas pipeline readoption and final amendments https://www.nj.gov/bpu/pdf/rules/R.2023%20d.071%20%2855%20N.J.R.%201201%28a%29%29.pdf	14:7-1.1, -1.9(f)-(g), -1.10(f), -1.17, -1.24 and -1.26; Register pages 1207-1210	Adopted April 26, 2023; readoption effective May 3, amendments effective June 5, 2023. Final adopted clauses read; printed expiration May 3, 2030.
NG02	Federal gas incident immediate notice https://www.ecfr.gov/current/title-49/subtitle-B/chapter-I/subchapter-D/part-191/section-191.5	191.5(a)-(c); current 191.3 and Part 191 scope	
NG03	Federal gas safety related condition and MAOP reporting https://www.ecfr.gov/current/title-49/subtitle-B/chapter-I/subchapter-D/part-191/section-191.25	191.25(a)-(c), distinguished from 191.23 triggers or exclusions	
NG04	PHMSA control room management program https://www.phmsa.dot.gov/pipeline/control-room-management/control-room-management	Gas 192.631 versus hazardous liquid 195.446; operator or control room functions	
NG05	PHMSA Part 191 reporting index https://www.phmsa.dot.gov/regulations/title49/part/191	191.1/.3/.5/.7/.9/.11/.15/.17/.23/.25 and current forms	
NG06	BPU pipeline and utility cybersecurity oversight https://nj.gov/bpu/about/divisions/reliability/	Bureau of Pipeline Safety; Cyber Security Unit; actual jurisdiction and orders	
NG07	PHMSA 2026 gas property damage threshold notice https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2026-09/Dollar%20Reporting%20Threshold%20for%20Gas%20Incidents_0.pdf	April 2026 notice; effective period history table	The property damage threshold is $153,600 from July 1, 2026 through June 30, 2027. Take the effective date from the adopted rule.
NJ28	BPU minutes: Chapter 14:8 readoption approval https://www.nj.gov/bpu/pdf/boardminutes/2025/20251217/December%2017%202025%20Minutes.pdf	PDF pages 15-16; docket QX25080483	
NJ29	Final June 2026 Chapter 14:8 solar amendments https://www.nj.gov/bpu/pdf/rules/R.2026%20d.077%20%2858%20N.J.R.%201681%28a%29%29.pdf	Publication header; Chapter 14:8-13 amendments	Final publication effective June 15, 2026; printed chapter expiration December 17, 2032.

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

ID	Source	Where to look	What it says
NG08	PHMSA current gas transmission, gathering or storage incident instructions https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2026-01/Current_GT_GG_UNGS_Incident_Instructions_PHMSA%20F%207100%202_1-2026%20and%20Beyond.pdf	Page 1 version and form routing; Parts A and D as applicable	
F16	OIRA CIRCIA regulatory review record https://www.reginfo.gov/public/do/eoDetails?rrid=1550967	RIN 1670-AA04; received October 1, 2026; pending review record	
F18	NIST SP 800-115 full technical guide https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf	Assessment planning and Appendix B rules of engagement template	
F19	FERC Order No. 919, virtualization and CIP standard revisions https://www.govinfo.gov/content/pkg/FR-2026-03-24/html/2026-05716.htm	91 FR, March 24, 2026; effective May 26, 2026	Standards take effect on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after the order took effect, with early adoption permitted. Checked November 3, 2026.
F20	FERC Order No. 907 and CIP-015-1 implementation plan https://www.govinfo.gov/content/pkg/FR-2025-07-02/html/2025-12309.htm	Order effective September 2, 2025; NERC Project 2023-03 implementation plan	CIP-015-1 takes effect on the first day of the first calendar quarter 36 months after the order took effect (October 1, 2028) for high impact BES Cyber Systems and medium impact Control Centers; medium impact BES Cyber Systems with External Routable Connectivity follow 24 months later. Checked November 3, 2026.

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

Talk to a senior examiner

Global Digital Forensics has examined digital evidence and tested security programs since 1992. Our examiners have testified in federal and state courts, and we scope every OT assessment around your operating windows and safety boundaries.

On the first call we review the utility groups and facilities in scope, the duties you have already identified in the workbook, the records that are still missing and the testing depth that fits your operating constraints.

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.

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