AFTER-ACTION REPORT

County Election Systems — Ransomware 14 Days Before the General

Discussion-based tabletop exercise conducted via Atlas. This AAR is structured to FEMA HSEEP and NIST SP 800-84 §3.4.3 and is formatted for direct submission to a state auditor, cyber-insurance underwriter, or SOC 2 CC7.5 evidence folder.

Exercise name	Conducted	Duration	Participants
County Election Systems — Ransomware 14 Days Before the General	04 Oct 2025 · 14:00 ET	60 minutes (plus 15-minute hot-wash)	7 · facilitator + 6 players
Scenario type	**Complexity**	**Sponsor**	**Exercise ID**
Discussion-based tabletop	Advanced	County Board of Elections	ATX-2025-0411-PUB-CE

Exercise overview

At 06:14 local time on the exercise date, the County Board of Elections' ePollbook vendor reported a confirmed ransomware encryption event across the hosted pollbook environment. The general election sat 14 days out. Players were asked to triage containment, decide on public-statement timing under conflicting CISA and state-CISO guidance, map a paper-pollbook contingency to precincts within procurement constraints, and produce an HSEEP-conformant AAR for state auditor review.

The exercise was facilitated by Atlas, the Annual Tabletop AI facilitator, with inject timing driven by the scenario's programmed Master Scenario Events List (MSEL). No real systems were touched.

Exercise objectives

- Activate COOP per ESF #2 within the first hour of a confirmed cyber event.
- Decide on public-statement timing under conflicting CISA / state-CISO guidance.
- Map a paper-pollbook contingency to affected precincts inside existing procurement authority.
- Produce an HSEEP-conformant AAR ready for state auditor review.

Participants

Role	Function	Represented by
Exercise Director	County Emergency Manager	[Redacted]
Lead Facilitator	Atlas (AI)	Annual Tabletop platform
Player	Board of Elections Director	[Redacted]
Player	County IT / CISO delegate	[Redacted]
Player	Public Information Officer	[Redacted]
Player	County Counsel	[Redacted]
Observer	State CISO liaison	[Redacted]

Timeline of decisions captured

T+	Inject	Player decision captured
00:00	ePollbook vendor reports confirmed ransomware encryption event; scope and strain unknown.	Activated county COOP per ESF #2. Established incident commander and decision log within 22 minutes.

T+	Inject	Player decision captured
00:22	State CISO phones: “Have you notified CISA yet?” State guidance conflicts with vendor contractual NDA.	Notified CISA Central and state CISO immediately; instructed counsel to review vendor NDA in parallel rather than serially.
00:45	Local press picks up vendor’s status page; first reporter call to the PIO desk.	Held the public statement pending verification. PIO issued a holding line; board chair briefed within 60 minutes.
01:30	County IT confirms BoE backups are 11 days stale; paper pollbook inventory unknown across 14 precincts.	Activated paper-pollbook contingency for 14 precincts. Tasked procurement with emergency 48-hour purchase authority.

Analysis

Strengths. Incident command was established in 22 minutes — inside the county's own COOP target of 30. Counsel reviewed the vendor NDA in parallel with the CISA notification decision rather than serially, which preserved the state's preferred early notification window.

Areas for improvement. Backups were 11 days stale at the moment of the exercise — not a player failure but a planning gap surfaced under pressure. The PIO had no pre-approved holding line for cyber events, which forced on-the-spot drafting while the reporter was already holding. Paper-pollbook inventory is not centrally tracked at the county level.

Framework crosswalk

Each row below maps a player decision or captured artifact to the underlying framework control. This crosswalk is the core of the AAR for audit consumers: the left column answers "which control?" and the right column answers "show me the evidence."

Framework	Control / capability	Evidenced by
NIST CSF 2.0	RC.RP-1 · Recovery plan executed during / after event	COOP activation timestamp + decision log
NIST CSF 2.0	RS.CO-2 · Incidents reported consistent with criteria	CISA + state CISO notification log
NIST SP 800-84	§3.4.3 · Tabletop exercise documentation	This AAR in full
FEMA HSEEP	Capability Target #4 · Public Information & Warning	PIO holding-line decision at T+00:45
CISA Election Security Toolkit	§2 · Continuity for election infrastructure	Paper-pollbook contingency for 14 precincts

Improvement Plan (IP)

Four findings were converted into tracked recommendations with owners and due dates. Atlas will generate a follow-up reminder two weeks before each due date.

Finding	Recommendation	Owner	Due
Backups 11 days stale at time of exercise.	Restore nightly BoE backup cadence. Add quarterly restore test with timed metric captured in CSF RC.RP-1 evidence folder.	County IT	Q1 2026
Vendor NDA conflicted with CISA notification expectation.	Counsel to add disclosure-carveout clause to vendor template; renegotiate at next renewal.	County Counsel	Pre-Nov 2026
Paper-pollbook inventory not centrally tracked.	Quarterly precinct-level inventory; state-level mutual-aid stockpile evaluated against ESF #2.	BoE Director	Q2 2026
PIO had no pre-approved holding-line for cyber events.	Draft + approve three holding-lines (unknown scope, confirmed incident, resolved). Rehearse with board chair.	PIO	Q1 2026

Exercise director sign-off

I certify that this discussion-based tabletop exercise was conducted as described, that the decisions captured above reflect the consensus of the players named, and that the Improvement Plan has been entered into the county's corrective-action tracker.

_____	_____	_____
Exercise Director County Emergency Manager	**BoE Director** Board of Elections	**Date**

Sample artifact. This document is a redacted example AAR produced by Atlas for the purposes of demonstrating the Annual Tabletop output format. It is structurally identical to AARs generated during real exercises, except that participant names, jurisdiction, and specific vendor references have been replaced with placeholders. A real AAR downloads as PDF + editable DOCX inside your Annual Tabletop account. Run your own exercise at annualtabletop.com.