League of Oregon Cities

101ST ANNUAL CONFERENCE

Cybersecurity for Cities Under Attack

SPONSORED BY:

COVENANT TECHNOLOGY SOLUTIONS

COVENANT TECHNOLOGY SOLUTIONS

Left of boom:
cyber crisis in city hall

An interactive leadership tabletop for Oregon city officials

IN PARTNERSHIP WITH

blackpoint

LOC 101st Annual Conference • Salem • October 15-17, 2026

Facilitated by Melissa Swann and Tom Choquette

BEFORE WE START

How this works

1

No perfect answers

Only choices and trade-offs. You'll decide with incomplete information — like the real thing.

2

It's a safe room

Play your role, take a few risks. This is practice, not a test.

3

AI is the backdrop

It's on both sides now — making attacks faster and more convincing, and making good defense more possible.

The hardest calls in a cyber incident aren't technical — they're leadership calls.

READINESS PULSE

4 quick questions — hands up

1. Whose job is it to declare a cyber incident in your city? Do you know the name?
2. If utility billing and email went down this morning, could you still serve residents by end of day?
3. In the last year, has your team practiced a cyber incident — even once?
4. Have you set ground rules for staff using AI tools with city data?

THE SCENARIO

Monday morning

Most of your staff isn't in yet. Your phone buzzes.

It's a notice from the vendor that runs your permitting and utility-billing software — one you trust and have used for years.

Read the notice on the next screen slowly. Let it land.

THE SCENARIO

The vendor notice

> **“Critical security notice:** the software update we released 9 days ago was compromised by an advanced threat actor who used **AI-assisted tooling** to slip malicious code past our review. If you installed version 8.4, your systems may be affected. We are working with federal authorities.”

You installed it 5 days ago — you followed good practice and waited. That's all you know.

THE SCENARIO

What you know / what you don't

What you know

- The software is widely used across your city
- You installed it 5 days ago
- CISA has issued a national alert
- Thousands of organizations are affected

What you don't know

- Whether attackers reached your systems
- What data may have been taken
- Whether they're still inside
- Whether your backups are clean

Meanwhile: utility billing is down, finance can't run payroll, email is shaky. Every hour it drifts, the impact to residents grows.

TABLE EXERCISE

Claim a role at your table

1 Mayor / council

Public trust and what the council must know.

2 City manager

Runs the response. Continuity vs. containment.

3 City attorney

Notification duties, records, evidence, liability.

4 Finance director

Billing, payroll, cost and the CIS claim.

5 IT / MSP liaison

Scope, containment and recovery.

6 Public information

Residents, media and AI-driven rumors.

TABLE EXERCISE — 10 MINUTES

Make 6 decisions together

1. **Immediate response to affected systems**
2. **Who to notify — and when**
3. **How to investigate what happened**
4. **Public communication — and who delivers it**
5. **Continuity: what must keep running**
6. **One change to prevent a repeat**

Curveball at the 5-minute mark: open the sealed AI complication card and adapt.

REPORT-OUT

Tell us three things

01 Your most critical decision — and why.

02 Where your roles disagreed the most.

03 Your AI complication — and how it changed the plan.

DEBRIEF

5 moves that decide the outcome

1	**Name the roles now**	Who declares and runs an incident — on paper, before you need it.
2	**Practice once a year**	A 60-minute tabletop is the cheapest readiness you can buy.
3	**Backups you can trust**	Ransomware can't reach them — and you've tested a restore.
4	**Someone always watching**	Round-the-clock monitoring turns months into hours.
5	**Draft the message early**	A resident and council update, written in calm times.

THE AI THROUGHLINE

AI is both the threat and the ally

Working against you

- Poisoned the trusted vendor update
- Wrote phishing with no telltale mistakes
- Cloned a familiar voice on a voicemail
- Spread a false rumor faster than facts

Working for you

- Spots the one unusual login among millions
- Flags the payment that doesn't fit
- Drafts a resident update in minutes
- Speeds a public records response

The difference is governance: AI helps a city only when you've decided what data is allowed near it.

HOW COVENANT HELPS

An ongoing partner, not a one-time project

Harden Microsoft 365

Identity, email, endpoints and data set up the way they were meant to be — our Fortify program.

Backups & monitoring

Backups you can trust and Blackpoint's round-the-clock detection, so an incident is caught in hours.

Incident plan & roles

The decisions from today, written down and practiced — before the call comes.

AI readiness

Sensible rules so Copilot is useful without exposing resident data.

Microsoft-first, security-first — reducing risk without adding chaos.

Detection partner blackpoint

ONE CLEAR NEXT STEP

COVENANT TECHNOLOGY SOLUTIONS

Take a Security Score Assessment

A right-sized read on where your city stands and what to fix first. No obligation, no jargon.

Ask Tom or scan the card on your table.

COVENANT TECHNOLOGY SOLUTIONS

Questions

IN PARTNERSHIP WITH

blackpoint

Thank you.

Melissa Swann and Tom Choquette • Covenant Technology Solutions

Microsoft-first, security-first managed and co-managed IT for the Pacific Northwest

Cybersecurity Incident Notification
Legislative Concept – 2027 Session

League of Oregon Cities – Annual Conference | October 16, 2026

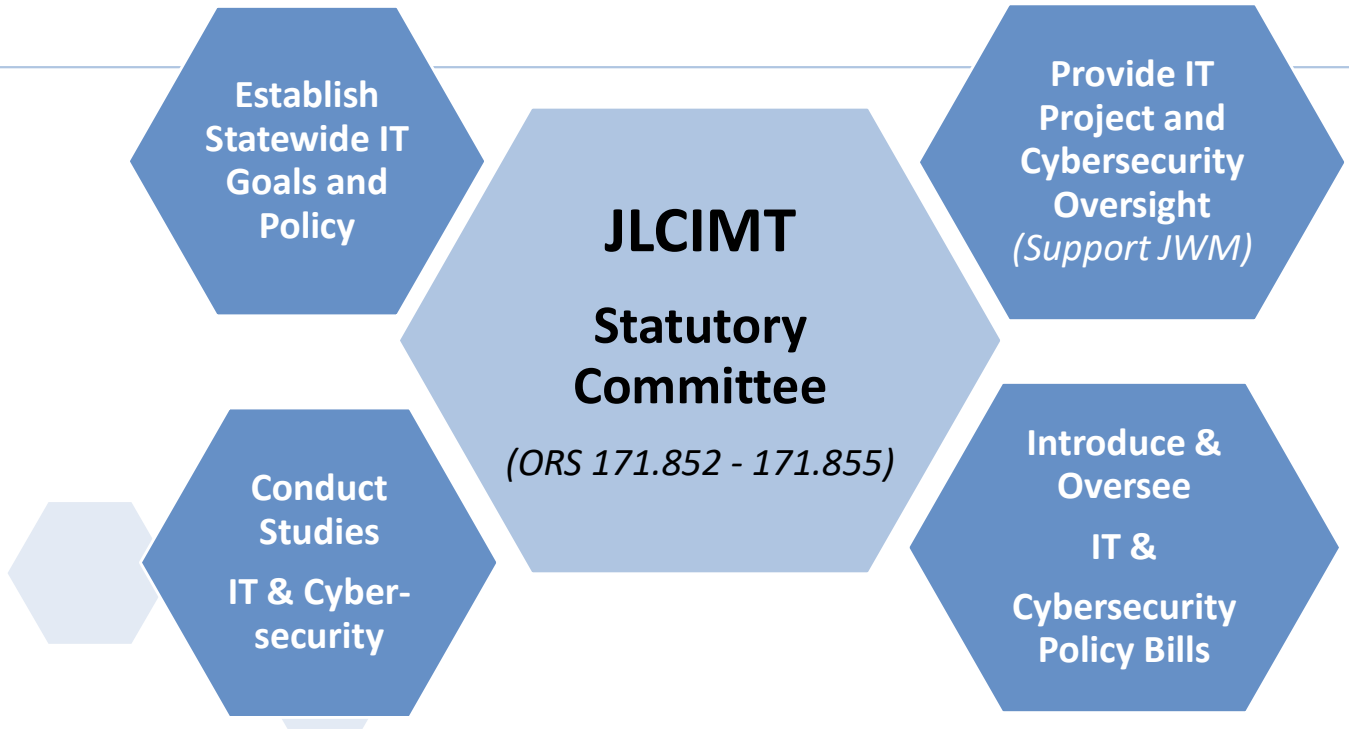
Nancy Nathanson, State Representative – District 13
Sean McSpaden, Principal Legislative IT Analyst
Committee Administrator – Joint Legislative Committee on Information Management and Technology

LFO
LEGISLATIVE FISCAL OFFICE

Table of Contents

- Oregon Joint Legislative Committee on Information Management and Technology
- Representative Nancy Nathanson – What Public Health Reporting Teaches Us About Cybersecurity Incident Notification
- Cybersecurity Incident Notification – 2027 Legislative Concept
- Questions & Contact Information

Joint Legislative Committee on Information Management and Technology



- https://www.oregonlegislature.gov/bills_laws/ors/ors171.html
- https://olis.oregonlegislature.gov/liz/2025I1/Committees/JLCIMT/Overview

JLCIMT Members & Staff

Senate Members

- **Senator Khanh Pham (Co-Chair)**
- Senator Mark Meek
- Senator Christine Drazan

House Members

- **Representative Willy Chotzen - Co-Chair**
- Representative Nancy Nathanson
- Representative Daniel Nguyen
- Representative Darcey Edwards
- Representative Ed Diehl

Staff

Sean McSpaden, Committee Administrator

- Authorizing Statute: https://www.oregonlegislature.gov/bills_laws/ors/ors171.html
- JLCIMT Website: https://olis.oregonlegislature.gov/liz/2025I1/Committees/JLCIMT/Overview

Available - Agendas, Materials, Recording Logs and Recorded Content for all meetings during the 2025-26 Legislative Interim

Representative Nancy Nathanson

What Public Health Reporting Teaches Us About Cybersecurity Incident Notification

Public Health & Cybersecurity Incidents

Public Health Incident / Emergency Reporting ORS Chapter 433 · OAR 333-018 — protecting Oregonians for decades		Cybersecurity Incident / Emergency Notification 2027 Legislative Concept — all Oregon public bodies
Infectious diseases spread quickly, escalate quietly, and cause severe harm if not contained early	THREATS SPREAD →	Attackers move from one city, county, or school to the next using the same tools and stolen passwords
Immediate, 24-hour, or one-working-day reporting based on disease severity	SPEED MATTERS →	Notify the State CIO within 48 hours of discovery — or sooner
Suspected cases are reported, not only confirmed ones, so intervention starts early	DON'T WAIT FOR CERTAINTY →	Notify on discovery or reasonable belief — even while details are still emerging
Reports go to local public health, then to the Oregon Health Authority	ONE CENTRAL POINT →	Notifications go to the State CIO through a secure, confidential portal
Reporters are protected with immunity from liability	REPORT WITHOUT FEAR →	Safe harbor and good-faith protections for public bodies that notify
Statewide awareness drives outbreak detection and deployment of support	STATEWIDE AWARENESS →	Statewide attack patterns, shared alerts, coordinated assistance, and stronger resilience

LIKE CALLING 911 "**This happened here** — please help me, please help my neighbors, and please make sure it doesn't happen to anyone else."

Cybersecurity Incident Notification – Background



Joint Legislative Committee on Information Management and Technology
Potential Legislative Concept - 2027 Legislative Session

Topic: Cyber Incident Notification Requirement - all public bodies

While all 50 states (including Oregon) have data breach notification laws requiring covered entities to inform individuals when their personal information or personal health information is compromised, these laws primarily focus on notifying affected individuals rather than mandating cybersecurity incident notifications to a central state government entity for real time information sharing, analysis, coordination, and response. In Oregon, a breach notification is required within 45 days of the discovery of the incident.

Oregon's executive branch state agencies are required to report information security incidents to the State Chief Information Officer per ORS 276A.300 and associated rules and policies. Oregon's state agencies, including the constitutional offices, the Attorney General, and the Judicial and Legislative Branches are also required to notify and report information security incidents to the Legislative Fiscal Office per ORS 276A.306.

Currently, there is no requirement in Oregon for cyber incident notification by local governments, local service districts, and special government bodies to a central state government entity.

However, the trend of statutorily requiring public bodies to report cybersecurity incidents to a central state government entity is growing, as states across the nation recognize the importance of centralized information collection, analysis, and sharing to combat cyber threats effectively. To date, at least 17 states have enacted mandatory cyber incident reporting laws for local government and schools - California (2022), Florida (2022), Georgia (2021), Indiana (2021), Kansas (2024), Maryland (2024), Minnesota (2024), New Jersey (2023), New Mexico (2024), North Carolina (2021), North Dakota (2021), New York (2025), Ohio (2025), Texas (2023), Virginia (2023), Washington (2005), and West Virginia (2024).

During the 2026 session, the JLCIMT sponsored the introduction of a measure on this topic - HB 4055. Ultimately, based on written and in-person public testimony, the Co-Chairs felt more work on the measure and an extended period of stakeholder engagement during the legislative interim was required. We have shared a scaled back version of the concept with the Oregon Cybersecurity Advisory Council and other stakeholders and are currently reviewing and adjusting the concept based on the feedback received to date.

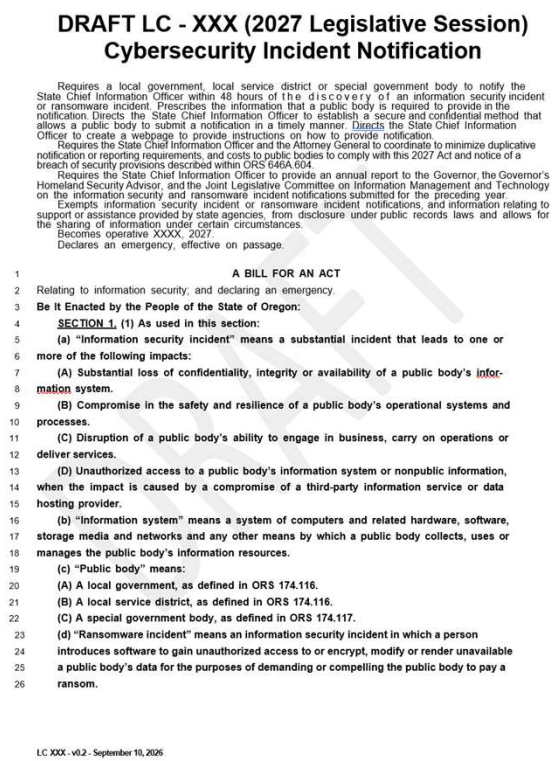
States with Mandatory Cyber Incident Reporting Laws for Local Governments and Schools

1. **Georgia** - Utilities, state agencies, local entities, including school districts, must report all cyber incidents that render critical business systems unavailable.
   Reporting Timeline: For state agencies (within 1 hour of discovery). For local government entities - required to contact local emergency management agency within 1 hour of discovery. For Utilities, within 2 hours of notification to the U.S. government.
   - House Bill 156 (2021)
     https://www.legis.ga.gov/api/legislation/document/20212022/196159
   - GEMA: Report Util/Agcy Cybersecurity Incident | Georgia Emergency Management and Homeland Security Agency

Legislative Fiscal Office - October 2026 Page 1 of 5

- **Concept:** Cyber incident notification requirement for all public bodies
- **Purpose:** Better information collection and analysis, threat assessment, resource allocation, and coordinated information sharing and response to cybersecurity incidents that may affect all public bodies throughout the state
- **As of 2025 - Seventeen (17) Other States** with Mandatory Cyber Incident Notification and Reporting Laws for Local Governments and Schools
  - California (2022), Florida (2022), Georgia (2021), Indiana (2021), Kansas (2024), Maryland (2024), Minnesota (2024), New Jersey (2023), New Mexico (2024), New York (2025), North Carolina (2021), North Dakota (2021), Ohio (2025), Texas (2023), Virginia (2023), Washington (2005), West Virginia (2024)

Cybersecurity Incident Notification – All Public Bodies 2027 Legislative Concept Overview



DRAFT LC - XXX (2027 Legislative Session)
Cybersecurity Incident Notification

Requires a local government, local service district or special government body to notify the State Chief Information Officer within 48 hours of the discovery of an information security incident or ransomware incident. Prescribes the information that a public body is required to provide in the notification. Directs the State Chief Information Officer to establish a secure and confidential method that allows a public body to submit a notification in a timely manner. Directs the State Chief Information Officer to create a webpage to provide instructions on how to provide notification.

Requires the State Chief Information Officer and the Attorney General to coordinate to minimize duplicative notification or reporting requirements, and costs to public bodies to comply with this 2027 Act and notice of a breach of security provisions described within ORS 646A.604.

Requires the State Chief Information Officer to provide an annual report to the Governor, the Governor's Homeland Security Advisor, and the Joint Legislative Committee on Information Management and Technology on the information security and ransomware incident notifications submitted for the preceding year.

Exempts information security incident or ransomware incident notifications, and information relating to support or assistance provided by state agencies, from disclosure under public records laws and allows for the sharing of information under certain circumstances.

Becomes operative XXXX, 2027.

Declares an emergency, effective on passage.

A BILL FOR AN ACT

Relating to information security; and declaring an emergency.

Be It Enacted by the People of the State of Oregon:

SECTION 1. (1) As used in this section:

(a) "Information security incident" means a substantial incident that leads to one or more of the following impacts:

(A) Substantial loss of confidentiality, integrity or availability of a public body's information system.

(B) Compromise in the safety and resilience of a public body's operational systems and processes.

(C) Disruption of a public body's ability to engage in business, carry on operations or deliver services.

(D) Unauthorized access to a public body's information system or nonpublic information, when the impact is caused by a compromise of a third-party information service or data hosting provider.

(b) "Information system" means a system of computers and related hardware, software, storage media and networks and any other means by which a public body collects, uses or manages the public body's information resources.

(c) "Public body" means:

(A) A local government, as defined in ORS 174.116.

(B) A local service district, as defined in ORS 174.116.

(C) A special government body, as defined in ORS 174.117.

(d) "Ransomware incident" means an information security incident in which a person introduces software to gain unauthorized access to or encrypt, modify or render unavailable a public body's data for the purposes of demanding or compelling the public body to pay a ransom.

LC XXX - v0.2 - September 10, 2026

- Requires a local government, local service district or special government body to notify the State Chief Information Officer within 48 hours of the discovery of an information security incident or ransomware incident.
- Directs the State Chief Information Officer to create a webpage to provide instructions on how to provide notification and establish a secure and confidential method that allows a public body to submit a notification in a timely manner.
- Requires the State Chief Information Officer and the Attorney General to coordinate to minimize duplicative notification or reporting requirements, and costs to public bodies to comply with this 2027 Act and notice of a breach of security provisions described within ORS 646A.604.
- Requires the State Chief Information Officer to provide an annual report to the Governor, the Governor's Homeland Security Advisor, and the Joint Legislative Committee on Information Management and Technology on the information security and ransomware incident notifications submitted for the preceding year.
- Exempts information security incident or ransomware incident notifications, and information relating to support or assistance provided by state agencies, from disclosure under public records laws and allows for the sharing of information under certain circumstances.

Cybersecurity Incident Notification – All Public Bodies 2027 Legislative Concept Overview

Stakeholder Issues and Concerns – Feedback received to date

- Definition of an Information Security Incident – request to narrow definition of "substantial" incident requiring notification
- Notification Timeframe – Currently 48 hours
  - Notification providers have asked for 72 hours or longer
  - Notification receivers have asked for 24 hours
  - Request for consideration of an "acting in good faith clause" if notifications can't be provided within the required timeframe.

    Note: No penalty provisions are included within the Legislative Concept
  - Reliance on third party technology providers who may not notify affected public bodies of their discovery of an incident or attempt to inhibit/delay covered entity notifications to the State CIO.
- Detail to be provided within the Notifications. Only the information that is absolutely necessary should be required.
- Need for assurance of security and confidentiality of information contained within the notifications. Requests for anonymization of information prior to secure sharing
- Requests to be exempted from Notification Requirements altogether; lack of alignment/duplication with federal requirements for electric utilities (Form DOE-417) and/or CIRCIA.

Questions?

Legislative Fiscal Office

900 Court Street NE, Room H-178, Salem, Oregon 97301

Oregon State Capitol | (503) 986-1828 | www.oregonlegislature.gov/lfo

Contact Information

Representative Nancy Nathanson

District: 13 - View District Map

Capitol Phone: 503-986-1413

Capitol Address: 900 Court St NE, H-279, Salem, OR 97301

Email: Rep.NancyNathanson@oregonlegislature.gov

Website:
https://www.oregonlegislature.gov/nathanson

Sean McSpaden, Principal Legislative IT Analyst

Oregon Legislative Fiscal Office

JLCIMT Committee Administrator

Email: Sean.L.McSpaden@oregonlegislature.gov
Phone: 503-986-1835