# MOVEit Cyber Incident Briefing

Joint Legislative Committee on Information Management and Technology

September 27, 2023.

Thomas Amato, Chief Information Officer

Amy Joyce, DMV Administrator

Oregon Department of Transportation

# Agenda

- Use of MOVEit at ODOT
- Incident Overview (What Happened)
- Simplified Timeline
- Discovery and Notification
- Customer Service Response


Oregon Department of Transportation

# How is MOVEit Used at ODOT

- MOVEit is one of the most widely-used commercially available secure transfer tools available and has been used by ODOT since 2015.
- It is used by ODOT to encrypt, and transmit in a secure manner, agency data for business purposes.
- Example uses include data and file exchanges with other agencies, other governmental bodies, and vendors.


Oregon Department of Transportation

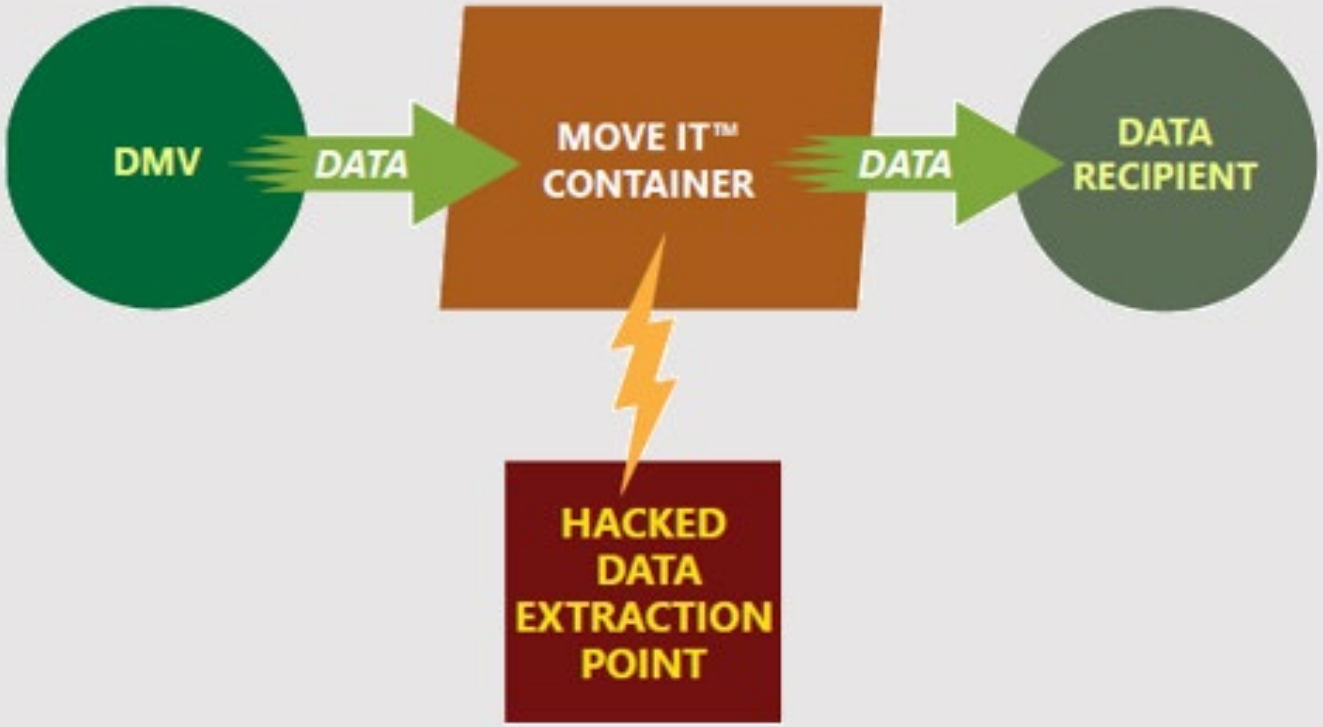
# What Happened at ODOT

- MOVEit CVE-2023-34362 was exploited on three internet facing ODOT MOVEit web servers at the state datacenter during the early morning hours of Sunday 5/28/2023.
- Based on the forensic report and our FBI field office briefing, the attacker was the CL0P ransomware group.
- Determinations of activity are from agency analysis, Cyber Security Services Security Operations Center analysis, and third-party forensic analysis.
- Forensic conclusion: the adversary's goal was data theft, and there was no unauthorized activity outside of CVE-2023-34362 exploitation.

Oregon Department of Transportation

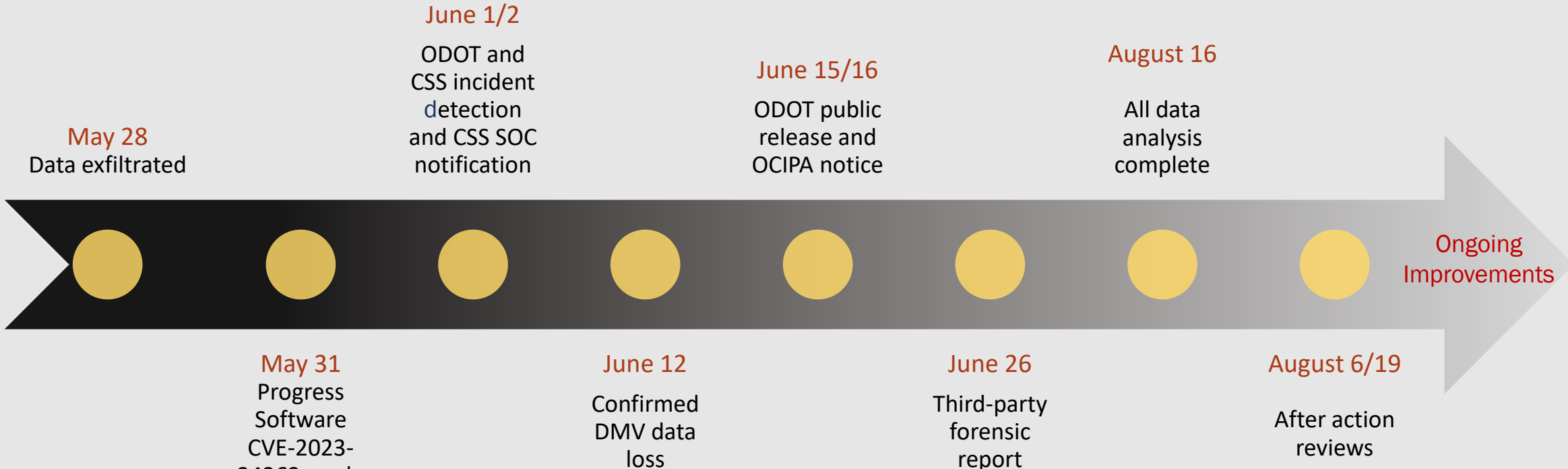
# Relationship to Systems of Record

MOVEit is not a system of record for data




Oregon Department of Transportation

# Simplified Timeline




Oregon Department of Transportation

# Discovery and Notification Complete

- The single largest data set was the DMV related information, and notification per the Oregon Consumer Identity Protection Act was completed on 6/16/2023.
- All affected data has been analyzed for personally identifiable information (PI), health information and financial information.
- Where data was exposed, we have completed notification as required by law.

Oregon Department of Transportation

# Customer Service Response

- Web site

- Call center overtime and long holiday weekend
  - Low call volume over the weekend
  - Few calls about MOVE It attack
  - Specialty call center contract explored, rejected due to low volume

- Very low call volume about MOVEit attack
  - June 16 - day after news conference – 56 calls answered by DMV
  - 6 weeks total – less than 600 calls / web inquiries to DMV or ODOT

# Thank You

Questions

Oregon Department of Transportation