LEGISLATIVE AUDITOR GENERAL

AUDIT SUMMARY

REPORT 2026-32 | October 2026

Office of the Legislative Auditor General | Kade R. Minchey, Auditor General

PERFORMANCE AUDIT

ELECTRICITY AND NATURAL GAS CYBERSECURITY

AUDIT REQUEST

The Legislative Audit Subcommittee prioritized an audit of cybersecurity readiness of public utilities throughout the state in its October 2024 meeting. This audit focuses on electricity and natural gas cybersecurity, while previous and future audits will look at other critical public utilities.

BACKGROUND

The adoption of networked technology has made critical infrastructure increasingly vulnerable to attack. Cyberattacks on electricity and natural gas distribution have the potential to disrupt services foundational to modern society. Past cyberattacks demonstrate the need for robust cybersecurity controls. The capabilities of state-sponsored groups and changes in geopolitics increase the risk of future cyberattacks.

KEY FINDINGS

- **Finding 1.1**
  Municipal power systems have opportunities to improve cybersecurity.
- **Finding 1.2**
  Cybersecurity controls at the state's largest electricity provider are mature.
- **Finding 2.1**
  Natural gas in Utah appears to be well protected from cyberattacks under existing federal regulations.

KEY RECOMMENDATIONS

- 1.1 The Legislature should consider whether additional state involvement is necessary to encourage municipal power systems to improve cybersecurity practices. This could include such things as having the Cybersecurity Commission or Cyber Center help develop model incident response plans, requiring municipalities to adopt baseline cybersecurity controls, or encouraging adoption of best practices by reducing potential liability for those that do adopt best practices.
- 1.2 The Legislature should consider whether additional oversight is necessary for Rocky Mountain Power's distribution network cybersecurity, and, if so, designate an appropriate entity to provide oversight.
- 2.1 The Legislature should consider whether changes to Utah's oversight of natural gas cybersecurity are necessary given current levels of risk.

REPORT SUMMARY

Municipal Power Systems Have Opportunities to Improve Cybersecurity

We found municipal power systems have opportunities to improve in fundamental areas of cybersecurity, such as incident response planning and third-party assessments. This finding is concerning because cyberattacks have the potential to disrupt the delivery of electricity such as that seen in Ukraine in 2015. Cyberattacks can also affect related systems and open the door to future attacks on power systems.

Cybersecurity Controls at the State's Largest Electricity Provider Are Mature

Work completed on this audit demonstrates that Rocky Mountain Power has mature cybersecurity controls. Currently, the Public Services Commission appears to be the only state-level agency that provides general oversight of cybersecurity for Rocky Mountain Power's distribution network. However, this oversight is reportedly limited to the electricity rate-setting process.

Natural Gas in Utah Appears to Be Well Protected from Cyberattacks Under Existing Federal Regulations

Utah's natural gas provider, Enbridge, has mature cybersecurity controls with some opportunities for improvement. From a regulatory standpoint, Utah relies solely on the federal government to ensure Enbridge is adequately protecting natural gas infrastructure from cyberattacks. Utah could do more to provide additional assurance.

Municipal Power Systems Have Not Fully Implemented Key Cybersecurity Practices. As part of our audit, we interviewed five municipal power systems from across the state about baseline cybersecurity controls that are proven to reduce the risk of a cyberattack. This infographic displays the controls most frequently needing improvement.

