Alberta Energy and Alberta Energy Regulator

IT Security for Industrial Control Systems in Alberta's Oil and Gas Industry

October 2017

Introduction

Alberta's oil and gas industry relies on critical infrastructure to extract and refine its products and safely deliver those products to provincial, national and international markets. Industrial control systems (ICS) are a key component of energy operators' efforts to monitor and ensure safe and reliable operations. If these control systems are not secure, they can be misused to cause damage to critical infrastructure (e.g., oil wells, pipelines and refineries), resulting in harm to Albertans and the environment.

In 2015, we performed an audit to evaluate if the government should assess the risks to Alberta from unsecured industrial control systems used in provincially regulated oil and gas infrastructure. We made one recommendation to the Alberta Energy Regulator and the Department of Energy to work together to determine whether a further assessment of threats, risks and impacts to ICS used in provincially regulated oil and gas infrastructure would benefit Alberta.[1]

We conducted a follow-up audit in 2017 and report on the results of this audit below.

Audit Objective and Scope

Our objective was to determine whether the Alberta Energy Regulator and the department have implemented our recommendation to determine if a further assessment of security risks to ICS is needed.

What We Examined

We examined the approach of the Alberta Energy Regulator and the department for assessing IT security risks to ICS in Alberta's oil and gas industry. We did not verify the operational effectiveness of the security controls identified from the ICS risk assessment.

We conducted our field work in June 2017, and substantially completed our audit on June 28, 2017.

Conclusion

The AER and the department have implemented our recommendation by conducting an assessment to understand how the oil and gas industry was managing its ICS security risk and the controls that the operators have implemented to secure their ICS.

Why This Conclusion Matters to Albertans

Unsecured ICS could lead to disruption to Alberta's provincially regulated oil and gas infrastructure, causing harm to Albertans and the environment. The AER and the department should understand the risks and impact to Albertans from unsecured ICS.

1 *Report of the Auditor General of Alberta—February 2016*, pages 27–31.

Findings

The AER and the department worked together and determined that an IT security assessment of ICS used in the oil and gas industry would benefit Alberta. They commissioned an independent consultant to conduct an ICS security assessment across a sample of Alberta oil and gas operators. The purpose of the assessment was to gain an understanding of existing ICS-related risks and what controls the operators have implemented to mitigate those risks. The assessment identified residual risks based on the identified controls and made observations to improve ICS security for the operators. The results were shared with industry associations to improve their awareness of ICS security.

The AER and the department also conducted a workshop to analyze the results of the risk assessment. They are currently working together to determine whether they need to take further action in response to assessed ICS security risks for Alberta's oil and gas industry. Through our ongoing interactions with both the AER and department, we will keep apprised of further developments in this area. Based on the work completed by both organizations to date, we are concluding that the recommendation has been implemented.