The CYBERFORCE INFORMATION SHARING & ANALYSIS CENTER

INTELLIGENCE BULLETIN

SOUTHERN NORTH REGION

help@cyberforceisac.com | Phone: 202-555-2525 | Fax: 202-555-2626

CFC-2024-02

Cascading Consequences Seen after Energy Company Cyber Attack

Executive Summary

Between February 2024 and June 2024, a wind energy company within our area of responsibility (AOR) has identified a significant cyber breach to both its internal business network and operational network. This was previously reported in our CFC-2024-01 Intelligence Bulletin. This bulletin is to highlight the new information received from stakeholders.

While vulnerability mitigation efforts are underway, the wind energy company continues to see degraded energy output to those within their service area. Outages have been reported.

The threat is still imminent until the wind energy cyber team has been able to remedy all their systems which is not planned until mid-October.

The CyberForce Information Sharing and Analysis Center (ISAC) assesses with **HIGH** confidence the following points:

- The AOR has many key government facilities which are likely to be impacted.
- The AOR has the largest government-run AI-driven data center operating on clean energy, which is likely to be impacted.

Recommendations

The CyberForce ISAC recommends the following:

- Identify key dependencies within your AOR that may become critical if energy is lost or degraded.
- Identify potential resources and data sets that may be impacted and identify potential alternative options.
- Identify and remediate all known vulnerabilities within the system to ensure stable infrastructure.
- Ensure inventories include not only your dependencies but those that are dependent upon you.