

# Cybersecurity update

Utah Public Service Commission

December 14, 2023



**Dominion  
Energy<sup>®</sup>**

# Introductions

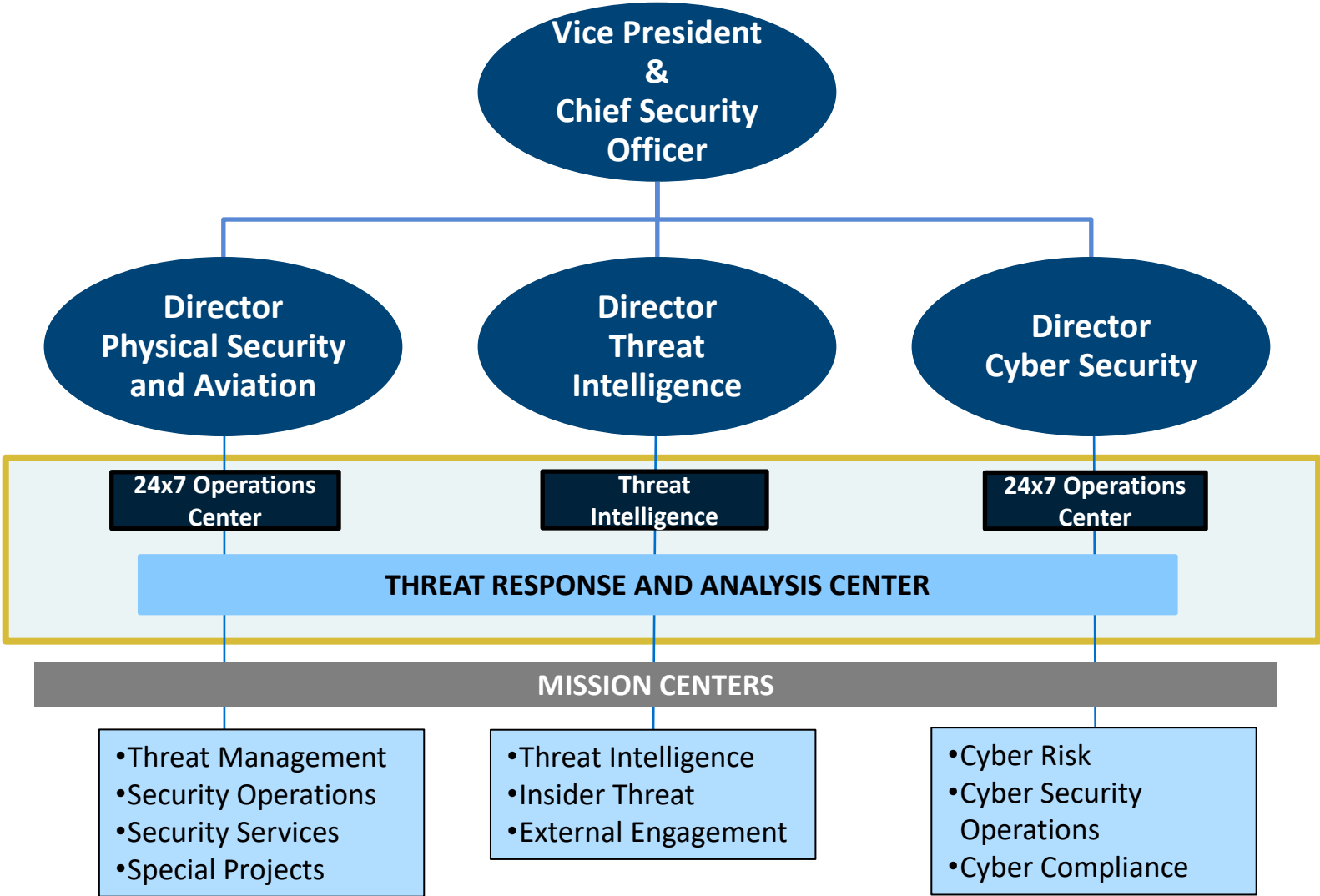
## Jonathan Bransky: Director Threat Intelligence

- Director Threat Intelligence
- Over 25 years in energy sector security
- Oversees threat intelligence and insider risk functions
- Dominion Energy industry and government security liaison
- Chair of American Gas Association's Cybersecurity Strategy and Regulatory Action Committee
- Held leadership roles for Oil and Natural Gas Subsector Coordinating Council (2020-2023)

## Sean Stalzer: Director Cyber Security

- Director Cyber Security
- Over 25 years at Dominion Energy
- Oversees the Cyber Security program. Includes:
  - Monitoring, Cybersecurity Testing and Assessments, Third Party Risk Assessments, Security Awareness and Phishing Training, Policy Creation, Cyber Regulatory Compliance Program Governance, etc.
- FBI Domestic Security Alliance Council Executive Working Group and Committee Chair of Threat & Resilience Information Sharing Committee

# Dominion Energy: Security Organization



# Threats discussed in 2021 still relevant, but continue to increase

## 2021 threats

- Ransomware
- Supply Chain
- Advanced Persistent Threats
- Data Breaches

## Key changes to threat landscape

- Geopolitical landscape
  - Russia/Ukraine
  - Hamas/Israel
  - China/Taiwan
  - Etc.
- Ransomware challenges to all sectors continue
- Supply chain risks continue expanding
- Data breaches driven by criminal exploits of Vulnerabilities (see ransomware)

# Geopolitics significantly increase risk to critical infrastructure

## Russia

- Continue to attack Ukrainian critical infrastructure and government entities
- Targets energy infrastructure with disruptive/destructive attacks
- Supply chain attacks (e.g., Solarwinds)
- Use wiper malware and sophisticated malware toolkits
- Key recent activity: Attempts against Ukraine electric entities

## China

- Cyber espionage and theft of intellectual property
- Able to impact critical energy infrastructure using cyber
- Cyber activity aligns with its five-year plan
- Key recent activity: Volt Typhoon, email account access of key US government officials

## Iran and North Korea

- North Korea:
  - Funds military and nuclear ambitions via cyber thefts (cryptocurrency, SWIFT); Espionage to gather nuclear info.
  - Recent activity: Cryptocurrency thefts, social engineering
- Iran
  - Leverages cyber to retaliate and disrupt; opportunistic
  - Recent activity: attacks against Israeli targets

## Criminals/Hacktivists

- Low sophistication, disruptive attacks (DDoS) against nations (government and companies) supporting Ukraine from Russia aligned groups
- Ransomware attacks continue to increase with tactics continuing to change
- Key recent activity: MGM and Caesars Casino attacks, Killnet and Anonymous Sudan DDoS attacks

# Ransomware – here to stay

---

- Ever evolving with new tactics to try to coerce ransom payment
  - Double extortion (encrypt data – need key to decrypt, threat to release data)
  - Contact customers, regulators, etc. to increase pressure to pay ransom
  - Partial encryption of files (makes them unusable) speeds up attack
- Successful criminal business model
  - Ransomware as a Service
  - Full business and support structure to assist with attacks
- Take advantage of widely used solutions by exploiting recent security vulnerabilities (e.g., Progress Software MoveIT, Citrix products)
- Also, leverage social engineering techniques to gain initial access

# Dominion Energy continues to evolve its capabilities

---

- Identify:
  - Expanded internal penetration testing capabilities
  - Continue to incorporate additional intelligence feeds
- Detect:
  - Continue to expand capabilities to identify possible exposed vulnerabilities
  - Create new and update existing threat identification use cases
- Prevent:
  - Moved to video-based training and awareness
- Respond / Recover:
  - Broadened live-fire cyber exercises using internal cyber range; extended participation to state & federal partners
  - Updated “play books” and “go books” for use should an event occur
  - Conducted cyber event tabletops exercises with company senior leaders, including ransomware focused event

# TSA regulations – security directives

---

- TSA issued mandatory cybersecurity requirements in May 2021 and July 2021, reissued annually since
- DE in compliance and has met all regulatory milestones through December 2023
- DE completed first TSA inspection under the security directives

## Security Directive 01: Enhancing Pipeline Cybersecurity

- Now on its third iteration
- Requires critical pipeline systems to:
  - Designate Cybersecurity Coordinator(s)
  - Report to US DHS CISA cybersecurity incidents within 24 hours
  - Complete and submit to TSA a gap assessment against the 2018 Pipeline Security Guidelines

## Security Directive 02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning and Testing

- Now on its fourth iteration
- Requires critical pipeline systems to:
  - Submit a Cybersecurity Implementation Plan detailing controls to meet the directives requirements
  - Develop and maintain a Cybersecurity Incident Response Plan
  - Submit annually a Cybersecurity Assessment Plan detailing how it assesses effectiveness of cybersecurity measures
  - (New) Submit annually results from prior year Cybersecurity Assessment



# Key government partnerships

## Department of Defense



- Host an active US Marine as part of military fellowship
- Will soon be hosting an NSA analyst
- Both (will) work with our cyber security operations center team
- Partner with National Guard

## Department of Energy



- Participate in the Cyber Risk Information Sharing Program (CRISP)
- Public-private partnership for cybersecurity
- Real time information sharing to identify potential cybersecurity threats
- Provides situational awareness of threats via bi-directional information sharing

## Department of Homeland Security (DHS)






- Participate in CyberSentry program
- Partnership between Dominion Energy and DHS
- Monitors in real time for both known and unknown threats
- Data monitored does not leave Dominion Energy

## Intelligence Community and State/Local Police

- Interact with members of the US Intelligence Community
- Work with state fusion centers

# Cyber Fortress Exercise

Event Overview	Expanded Participation	VIP Day
<ul style="list-style-type: none"><li>■ The only event of its kind in the nation.<ul style="list-style-type: none"><li>— Conducted in 2022 and 2023</li></ul></li><li>■ Utilizes Dominion Energy’s cyber range.<ul style="list-style-type: none"><li>— Simulates nation state attack.</li><li>— Uses current, sophisticated attack methods.</li></ul></li><li>■ Live-fire exercise, not a tabletop<ul style="list-style-type: none"><li>— Red team has broad discretion.</li><li>— Write custom malware, use insider threats, and simulated vendor compromises.</li></ul></li></ul>	<ul style="list-style-type: none"><li>■ One feature of 2023 exercise is participants are better prepared for an event than last year.</li><li>■ A number of business units actively participated or observed.<ul style="list-style-type: none"><li>— Utilized an actual substation as the target of real attacks.</li></ul></li><li>■ External participants include:<ul style="list-style-type: none"><li>— FBI, DHS CISA, Secret Service, US Marine Corps, National Guard, Commonwealth of Virginia agencies</li></ul></li></ul>	<ul style="list-style-type: none"><li>■ Visitors received:<ul style="list-style-type: none"><li>— Remarks from key state and federal partners</li><li>— Tour and overview of the DE Threat Response and Analysis Center (TRAC).</li><li>— Interaction with the Blue team on how the defense is proceeding.</li><li>— Observation of the Red team with explanation on what we have learned.</li></ul></li></ul>
		

# Dominion Energy Continues Its Cybersecurity Engagement Efforts

## Industry and Government

- Active in energy industry security communities, both natural gas and electric subsectors
  - American Gas Association Security Committee and Cybersecurity Strategy and Regulatory Action Committee
  - Edison Electric Institute Security and Security & Technology Policy Executive Advisory Committees
- Active engagement on both energy Sector Coordinating Councils and their security efforts with Federal and State Partners
  - Oil and Natural Gas Subsector Coordinating Council
  - Electric Subsector Coordinating Council
- Participate in industry Information Sharing and Analysis Centers (ISACs):  
Downstream Natural Gas ISAC and Electricity ISAC
- Engage with state fusion and emergency response/preparedness organizations:  
Includes Utah Public-Private Partnership (UP3), Utah Division of Emergency Management,  
Utah Department of Public Safety