My name is Clare Nelson, I am a Burnet County land owner affected by the Bell County East to Big Hill 765-kilovolt transmission project, specifically Segment i1.

I am a retired business executive and cybersecurity professional with certifications in information security, data privacy, and cloud technology. I previously served on the board of the Austin chapter of the Information Systems Security Association.

Many of the assumptions underlying the ERCOT Permian Basin Reliability Plan deserve renewed scrutiny. For example, **Public Utility Regulatory Act (PURA) §37.056** was enacted in 1997 and updated in later years—well before today's rapid changes in technology and grid security.

In fact, it looks like there is a gap between plans for the 765 projects and two recent, imperative Texas security bills: SB 2116, better known as the Texas Infrastructure Protection Act and SB 75 for Grid Security.

There is growing recognition that grid security is a national security issue. The U.S. Department of Energy has stated that *"the electric grid is the backbone of the nation's critical infrastructure." Add quote about Texas.*

Texas has begun addressing security risks through laws such as the **Lone Star Infrastructure Protection Act**, which restricts ownership and participation in critical infrastructure projects by entities associated with foreign adversaries—including China, Russia, Iran, and North Korea. It requires careful scrutiny of supply chains used in infrastructure development.

- For example, a component manufactured in China could potentially contain a hidden access point—sometimes referred to as a "backdoor"—allowing remote access or control.

Very large transmission corridors rely on complex digital monitoring and control systems, meaning the scale of the infrastructure can expand the potential cyber attack surface if supply-chain security is not carefully evaluated.

In addition, **Texas Senate Bill 75** created the **Texas Grid Security Commission** to evaluate threats to the electric grid, including cyberattacks, **physical attacks on substations**, electromagnetic pulse events, and other vulnerabilities in grid infrastructure.

As Texas evaluates major transmission investments, it is important to consider how security, resilience, and evolving system needs affect long-term planning.

I respectfully ask you to help ensure that the statutory standards for supply-chain security under the **Lone Star Infrastructure Protection Act**, and the grid-security concerns identified under **Senate Bill 75**, are fully evaluated for the proposed transmission projects of such unprecedented scale.

While the 765 planning documents address reliability and economics in detail, the publicly available materials contain relatively little discussion of supply-chain security, cyber resilience, or other emerging threats relevant to the proposed 765-kilovolt projects.

Thank you for your consideration.

My name is Clare Nelson, I am a Burnet County land owner affected by the Bell County East to Big Hill 765-kilovolt transmission project, specifically Segment i1.

I am a retired business executive and cybersecurity professional with certifications in information security, data privacy, and cloud technology. I previously served on the board of the Austin chapter of the Information Systems Security Association.

Many of the assumptions underlying the ERCOT Permian Basin Reliability Plan deserve renewed scrutiny. For example, **Public Utility Regulatory Act (PURA) §37.056** was enacted in 1997 and updated in later years—well before today's rapid changes in technology and grid security.

In fact, it looks like there is a gap between plans for the 765 projects and two recent, imperative Texas security bills: SB 2116, better known as the Texas Infrastructure Protection Act and SB 75 for Grid Security.

There is growing recognition that grid security is a national security issue. The U.S. Department of Energy has stated that *"the electric grid is the backbone of the nation's critical infrastructure." Add quote about Texas.*

Texas has begun addressing security risks through laws such as the **Lone Star Infrastructure Protection Act**, which restricts ownership and participation in critical infrastructure projects by entities associated with foreign adversaries—including China, Russia, Iran, and North Korea. It requires careful scrutiny of supply chains used in infrastructure development.

- For example, a component manufactured in China could potentially contain a hidden access point—sometimes referred to as a "backdoor"—allowing remote access or control.

Very large transmission corridors rely on complex digital monitoring and control systems, meaning the scale of the infrastructure can expand the potential cyber attack surface if supply-chain security is not carefully evaluated.

In addition, **Texas Senate Bill 75** created the **Texas Grid Security Commission** to evaluate threats to the electric grid, including cyberattacks, **physical attacks on substations**, electromagnetic pulse events, and other vulnerabilities in grid infrastructure.

As Texas evaluates major transmission investments, it is important to consider how security, resilience, and evolving system needs affect long-term planning.

I respectfully ask you to help ensure that the statutory standards for supply-chain security under the **Lone Star Infrastructure Protection Act**, and the grid-security concerns identified under **Senate Bill 75**, are fully evaluated for the proposed transmission projects of such unprecedented scale.

While the 765 planning documents address reliability and economics in detail, the publicly available materials contain relatively little discussion of supply-chain security, cyber resilience, or other emerging threats relevant to the proposed 765-kilovolt projects.

Thank you for your consideration.