Harry Krejsa Responses to Kathy Castor QFRs

1. *To limit future vulnerabilities in the electric grid, the United States is currently undergoing efforts to onshore manufacturing for key grid components such as inverters. My Republican colleagues recently sent a letter noting the security concerns regarding Chinese inverters and other connected devices that could pose security concerns. Democrats share many of these concerns. However, for companies that seek to re-shore inverter manufacturing, they need to know that a U.S. market exists for their products. The Department of Interior's efforts since July to block permitting for the deployment of all inverter-based resources has created a new level of uncertainty, as non-Chinese inverter companies were planning expanded U.S. manufacturing. How can companies plan for expansion when their end-customers can't get permits to put their products on the grid?*

Inverters are among the energy components I am most focused on from both a cybersecurity and a resilience perspective. They are digitally active, software-defined, and networked, constituting an increasingly "smart" pillar of our critical infrastructure. That digital sophistication is of course a double-edged sword: on one hand, modern smart inverters can serve as grid stability assets while acting as automated "firebreaks" that isolate disruptions before they cascade, and enabling the kind of distributed, self-healing grid architecture that is fundamentally more resilient than what we have today. On the other hand, those same digital capabilities can be exploited if they are compromised – particularly when they are manufactured by or dependent on adversary-controlled supply chains.

The imperative, then, is not to slow the deployment of inverter-based resources – which would forfeit their considerable security and resilience benefits – but to ensure we are deploying *trusted* inverters built to high cybersecurity standards. Reshoring their manufacture at home and among our allies is how we capture upside potential while managing downside risk.

But that strategy requires investment certainty; current policy policy is too often forfeiting both sides of that equation. We lose the resilience benefits that secure inverter-based resources offer to our grid, *and* we lose the domestic manufacturing momentum needed to reduce our dependence on Chinese vendors. If the only manufacturers still standing when permitting eventually resumes are Chinese ones, we will have worsened rather than ameliorated that dependency. Our experience in telecommunications – where delay in building trusted and affordable alternatives left us with inadequate technical and policy

solutions – should inform our approach here. We should be clearing the path for trusted inverter demand and deployment, not blocking it.

2. *We need to make sure that all secure energy sources have a path to deployment to meet our energy needs, and we need to reshore the manufacturing of these energy products at the same time. What policies could help domestic manufacturing of inverters that are not threats to national security and could create certainty that inverter-based energy has a path to deployment?*

Modern and digitally-enabled energy technologies, when deployed securely, represent a significant upgrade to grid resilience by being digitally native, updatable, and capable of supporting a more distributed and defensible grid architecture. The policy challenge is ensuring we capture those benefits by building a trusted domestic and allied manufacturing base, rather than ceding that industrial capacity to adversaries. Several complementary approaches can achieve this:

- **Risk-informed procurement frameworks.** Not all energy components pose the same security risk, and not all "smart" components are liabilities. Digitally active technologies like inverters and battery management systems are precisely the components where secure design yields the greatest resilience dividends, but also where compromised supply chains could pose the greatest threat. Congress should direct the relevant agencies – including DOE, CISA, and ONCD – to develop a joint risk prioritization framework that distinguishes these high-consequence components from "dumber" analog and commodity parts. This lets us concentrate reshoring resources and cybersecurity standards on the components where they yield the greatest security return.
- **Sustained manufacturing incentives.** The 45X Advanced Manufacturing Production Credit established in the Inflation Reduction Act catalyzed significant private investment in domestic advanced energy technology manufacturing. Maintaining these incentives or comparable successors provides the demand signal manufacturers need to commit capital to U.S. factories.
- **Cybersecurity standards as a market-shaping tool.** Congress should support the adoption and enforcement of cybersecurity standards for advanced energy technologies, with testing and certification performed by U.S.-authorized entities.

This creates a regulatory floor that advantages manufacturers willing to meet rigorous security requirements – which, in practice, will disproportionately advantage U.S. and allied manufacturers over FEOC vendors that have demonstrated poor vulnerability disclosure practices and resist independent inspection.

- **Easier and more certain energy permitting.** Building must become easier and permitting processes more certain. Too often the current approach expedites some energy sources while blocking others, sending contradictory signals to developers and the manufacturing base.
- **Allied-nation coordination.** The United States cannot build the entire trusted electrotech supply chain alone. Congress should support bilateral and multilateral industrial partnerships – particularly with Japan, South Korea, Australia, and European allies – to co-develop secure advanced energy manufacturing capacity. This is analogous to what the CHIPS & Science Act is doing for semiconductors, and it is equally necessary for the electrotech components that will define our energy infrastructure for decades.

Taken together, these policies would create a virtuous cycle: security standards that reward trusted manufacturers, sustained incentives that anchor their investment, and deployment certainty that ensures demand for their products.