STATEMENT OF JEFFREY BAUMGARTNER

VICE PRESIDENT OF NATIONAL SECURITY AND RESILIENCE POLICY

BERKSHIRE HATHAWAY ENERGY

BEFORE THE U.S. HOUSE COMMITTEE ON HOMELAND SECURITY

JOINT HEARING BY THE SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE AND SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

ENTITLED "SAFEGUARDING THE HOMELAND FROM UNMANNED AERIAL SYSTEMS"

DECEMBER 10, 2024

Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and members of both Subcommittees, thank you for the opportunity to testify. My name is Jeffrey Baumgartner, and I am Vice President of National Security and Resilience Policy at Berkshire Hathaway Energy. Berkshire Hathaway Energy owns energy production facilities, utilities, natural gas pipelines and a liquid natural gas import, export and storage facility. Our locally managed businesses share a vision for a secure and sustainable energy future. Delivering low-cost, secure, and reliable energy service each day to more than 13 million customers and end-users throughout the U.S., Great Britain, and Alberta, Canada, is at the core of everything we do. That is why we are committed to securing our energy services from all hazards, including unmanned aerial systems (UAS). I appreciate your invitation to discuss this important topic on behalf of Berkshire Hathaway Energy's businesses.

Critical infrastructure forms the backbone of our nation's economy, security, and public health. These assets—including energy facilities, transportation hubs, communications networks, and water systems—are increasingly vulnerable to a wide range of threats from UAS. Berkshire Hathaway Energy's businesses have customers or energy infrastructure in 35 states, and our energy services enable our customers' way of life. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives. Natural gas has grown to represent over 40 percent of electric generation as of 2023[1], making protection of pipelines, compressor stations and related infrastructure particularly important. Providing secure, resilient, and low-cost energy services is a responsibility we take seriously so that our customers can thrive.

The Evolving Threat Landscape

In recent years, the accessibility, affordability, and sophistication of UAS have surged. This technological proliferation has benefited a variety of industries with legitimate use-cases. We are hopeful that the Federal Aviation Administration (FAA) Part 108 rulemaking will advance our businesses' ability to fly UAS beyond visual line of sight (BVLOS) to enable faster damage assessments of energy infrastructure and restoration times for our customers and your

[1] U.S. Energy Information Administration, What is U.S. electricity generation by energy source? (February 2024), https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.

constituents. Simultaneously, however, the ease of procuring cheap, sophisticated UAS has empowered malicious actors.

Adversaries can use UAS to:

1. **Conduct Surveillance**: Equipped with cameras or sensors, UAS can collect sensitive information about critical infrastructure layouts and operations.

2. **Deliver Payloads**: UAS can carry explosives, incendiary devices, or hazardous materials, posing a direct physical threat.

3. **Disrupt Operations**: By interfering with airspace near airports or power lines, UAS can cause significant disruptions.

4. **Enable Cyber Intrusions**: UAS equipped with hacking tools can breach wireless networks and disrupt communications.

Incidents in the U.S. and around the world highlight the urgency of this issue. The U.S. Department of Homeland Security released its 2025 Homeland Threat Assessment in October. The annual assessment highlighted that the intelligence community "continue[s] to observe concerning UAS activity over sensitive critical infrastructure sites, which could interfere with regular facility operations, disrupt emergency response or authorized flight operations, and provide intelligence to malign actors."[2] The assessment raises instances where malicious actors have "considered using UAS to conduct intelligence collection, to drop explosives and other items on U.S. critical infrastructure for disruption purposes, and to endanger takeoffs and landings at airports via the mere presence of UAS."[3]

Critical infrastructure sectors—including energy, transportation, and communication—are particularly vulnerable. As the 2025 Homeland Threat Assessment highlighted, unauthorized UAS activities can disrupt operations, cause physical damage, and facilitate espionage. We have observed UAS flights over substations, pipeline compressors, and our liquid natural gas plant that may be providing intelligence for future attacks. The potential for UAS to carry hazardous payloads, such as explosives or conductive materials, further amplifies the risk to public safety and national security. For example, last month, federal agents arrested an individual in Tennessee

[2] U.S. Department of Homeland Security, Homeland Threat Assessment 2025 (October 2024), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.
[3] Id.

who planned to use a UAS to fly explosives into an electric substation. He was charged with attempting to use a weapon of mass destruction and attempting to destroy an energy facility.[4] When arrested, the individual was in the process of executing his planned attack, having armed the explosive device and powered up the UAS he intended to use.

Proactive Authorities to Address the Threat

Despite the clear and present dangers with UAS, existing federal laws have not kept pace with the rapid advancement and proliferation of UAS technology. The FAA has established regulations for UAS operations, but these regulations primarily address safety and airspace management and lack robust provisions for countering malicious UAS activities.

In pursuing the imperative to enhance counter-UAS capabilities, it is essential to balance security measures with the protection of civil liberties. Legislation must include safeguards to prevent abuse of authority and ensure that counter-UAS operations do not infringe upon individuals' rights to privacy and lawful UAS use. Implementing oversight mechanisms, transparency in operations, and clear accountability standards will help maintain public trust and uphold democratic principles.

While agencies like the FAA and the Department of Homeland Security (DHS) have made strides in regulating the use of UAS, significant gaps remain to fully address the threats:

1. **Limited Detection Capabilities**: Critical infrastructure owners and operators lack legal access to the most effective tools to detect, identify, and track UAS.

2. **Legal Constraints**: Existing laws restrict private sector and local authorities from deploying counter-UAS technologies, even for self-defense.

3. **Coordination Challenges**: There is no standardized protocol for coordination among federal, state, and local entities in response to UAS incidents.

4. **Expiring Authority**: Existing counter-UAS authorities for DHS and the Department of Justice are set to expire later this month, threatening to leave a critical gap in the legal

[4] U.S. Department of Justice, Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville (November 2024), https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility.

framework necessary to effectively detect and counter UAS threats in the public and private sectors.

Request from Critical Infrastructure

To mitigate these threats, I propose the following actions:

1. **Enhance Detection and Countermeasures**: Expand authorities for advanced detection technologies such as radar, radio frequency sensors, and AI-based tracking systems. Enable appropriate critical infrastructure owners and operators to work with law enforcement to deploy counter-UAS tools at high-risk sites with a limited authority that balances the need to address this pressing threat with respect for privacy and safety.

2. **Strengthen Public-Private Partnerships**: Establish formal mechanisms for information sharing between the government and private sector, ensuring timely dissemination of intelligence to prevent significant threats. Create incentives for infrastructure owners to adopt robust UAS security measures, and empower federal, state, and local law enforcement agencies with the necessary tools and legal authority to address UAS threats within their jurisdictions.

3. **Advance Research and Development**: Fund research and development programs focused on innovative UAS countermeasures and threat analysis. Promote joint exercises and simulations to test the resilience of critical infrastructure against both physical and cyber threats and the ability to neutralize threats without collateral damage.

4. **Develop a Framework for Countering UAS Threats**: Direct DHS, in collaboration with the FAA and the Department of Defense, to lead the development of a comprehensive strategy that aligns regulatory, technological, and operational efforts to systematically address UAS risks. Establish a clear legal framework that defines the parameters for counter-UAS operations, including addressing privacy concerns, ensuring compliance with existing laws, and providing guidelines for the use of force in UAS mitigation efforts. Combine these efforts with appropriate state and federal penalties for malicious use of UAS near protected facilities, including critical infrastructure.

Closing

The proliferation of UAS presents both opportunities and challenges. Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting this infrastructure, especially when there is a growing need to defend against nation-state actors. The U.S. government has long recognized the private sector is on the front lines of critical infrastructure protection, as recently embodied in National Security Memorandum on Critical Infrastructure Security and Resilience.[5] To harness the benefits of this technology while mitigating its risks, Congress must prioritize the enactment of comprehensive counter-UAS legislation that enables an industry-government partnership to address the evolving threat. By doing so, the U.S. can safeguard its critical infrastructure, protect public safety, and maintain its position as a leader in technological innovation and security.

The window of opportunity for Congress to address the escalating UAS threat is narrowing. With existing counter-UAS authorities set to expire and the rapid advancement of UAS technology, the time for action is now. Failure to enact comprehensive legislation will leave critical infrastructure vulnerable to malicious UAS activities, resulting in potentially devastating consequences for national security and public safety.

The threat of UAS to critical infrastructure is no longer theoretical—it is a reality demanding urgent and coordinated action. By modernizing our defenses, updating our legal frameworks, and fostering collaboration, we can ensure our infrastructure remains secure against this evolving threat. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to work with both public and private partners across all sectors to address all threats to U.S. energy security. Thank you again for holding this hearing.

[5] White House, National Security Memorandum on Critical Infrastructure Security and Resilience (April 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.