August 5, 2026

Bryan Bedford
Administrator
Federal Aviation Administration
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, D.C. 20590

Re: Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility (Docket No. FAA-2026-4558; Notice No. 26-03)

Dear Administrator Bedford,

The Edison Electric Institute ("EEI"), American Public Power Association ("APPA"), Large Public Power Council ("LPPC"), and National Rural Electric Cooperative Association ("NRECA") (hereafter the "Electric Utility Trade Associations" or "Associations") provide the following comments in response to the Federal Aviation Administration's ("FAA") Notice of Proposed Rulemaking on "Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility" (hereinafter "Proposed Rule").[1]

The Associations support the FAA's effort to address the threats posed by the unauthorized and malicious use of unmanned aircraft systems ("UAS" or drones) around sensitive fixed site facilities, including electric facilities. That said, the Associations have identified significant practical and operational concerns with the way the Proposed Rule is currently drafted. The Associations lay out these concerns, along with recommended solutions, below.

EXECUTIVE SUMMARY

The implementation of section 2209 of the FAA Extension, Safety, and Security Act of 2016 represents an important opportunity to protect critical infrastructure, including the nation's electric sector, from the growing threat posed by the unauthorized and malicious use of UAS. Such protections are vital to the electric sector, which undergirds the entire U.S. economy and is core to the operation of all other critical infrastructure sectors.

[1] Federal Aviation Administration, Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility, 91 Fed. Reg. 24650 (proposed May 6, 2026) (to be codified at 14 C.F.R. pts. 1, 74, 91, 107), https://www.govinfo.gov/content/pkg/FR-2026-05-06/pdf/2026-08943.pdf.

As described in the White House's recently released AI Action Plan, the electric grid "is the lifeblood of the modern economy and a cornerstone of national security."[2] Disruptions to electric infrastructure can have widespread effects across healthcare, water, emergency and financial services, for public safety and national security, and can cause massive economic disruption and potential loss of life. Accordingly, this Administration has made strengthening the supply of energy a day one priority and declared the "integrity and expansion of the Nation's energy infrastructure . . . an immediate and pressing priority for the protection of the Nation's national and economic security."[3]

The grid itself is interconnected and networked, to include a combination of large generating facilities and substations, as well as smaller transmission and distribution stations and substations that play critical roles in ensuring the operation of the grid. The disruption of any critical element, whether large or small, could have substantial, significant consequences for national security, health and public safety, and the nation's economic well-being. Due to their importance, critical elements of the electric grid are heavily regulated to include required compliance with multiple security mandates, including those required by the Federal Energy Regulatory Commission ("FERC") and the North American Electric Reliability Corporation ("NERC"), the two primary entities that regulate, secure, and oversee the United States' electrical grid.

The Associations are concerned that the Proposed Rule, as currently drafted, fails to account for the interconnected nature of the electric grid and excludes key and critical elements of the electric sector from the Rule's protections. The Associations are further concerned that the Proposed Rule establishes an unduly burdensome process for obtaining an unmanned aircraft flight restriction ("UAFR") and inadvertently creates new security vulnerabilities that would put our members' facilities at risk. Of additional concern, the proposed standard UAFR fails to give electric facilities meaningful control over their own airspace, even after a UAFR is in effect. Given the significant security concerns, commercial and recreational drones should not be permitted to fly over electric facilities absent affirmative facility approval. Meanwhile, facility-approved drones should not be subject to new restrictions as they carry out their critical safety, security, and inspection purposes over and around their facilities.

As described in detail in what follows, the Associations urge that the final rule:

---

[2] White House, Office of Science & Technology Policy, *Winning the Race: America's AI Action Plan* 15 (July 2025) https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[3] *See* Exec. Order No. 14156, *Declaring a National Energy Emergency*, 90 Fed. Reg. 8433 (Jan. 20, 2025) (declaring a national energy emergency and emphasizing the importance of a "reliable, diversified, and affordable supply of energy to drive our Nation's manufacturing, transportation, agriculture, and defense industries, and to sustain the basics of modern life and military preparedness"); *see also* Exec. Order No. 14213, *Establishing the National Energy Dominance Council*, 90 Fed. Reg. 9945 (Feb. 14, 2025) (emphasizing the importance of "reliable and affordable energy production to drive down inflation, grow our economy, create good-paying jobs, reestablish American leadership in manufacturing, lead the world in artificial intelligence, and restore peace through strength by wielding our commercial and diplomatic levers to end wars across the world").

- Revise the definition of "electricity facility" to cover additional electric facilities and networks critical to national security, public safety, and essential economic functions, and account for the integrated, networked nature of the electric grid, to include the protection of vulnerable *systems* composed of multiple facilities, not simply individual facilities meeting specified criteria.

- Adopt a more risk-based framework for determining eligibility and security requirements to better account for a facility's role in grid reliability, national security, support for critical loads, and vulnerability to cascading impacts. While facility voltage and generation capacity (which are the exclusive focus of the Proposed Rule) are relevant considerations, they are incomplete proxies for risk.

- Revise the application process to address the significant security concerns that would follow from creating a centralized database of electric grid vulnerabilities and security plans, and instead implement a self-attestation process, subject to FAA review in coordination with the Department of Energy ("DOE"), which is the Sector Risk Management Agency ("SRMA") for the electric grid.

- Revise the application process to eliminate costly and likely unworkable requirements that applicants obtain and submit information about third parties.

- Eliminate the advance notice and comment requirement, which would, as structured, effectively give adversaries a roadmap of vulnerable facilities—and thus an attack roadmap.

- Give electric facilities control over their airspace by requiring advance approval for commercial and recreational flights over restricted airspace, thus ensuring that the UAFRs provide meaningful protections for the grid.

- Ensure that facilities can continue to effectively deploy their own drones over their own facilities for the array of safety, security, maintenance, restoration, vegetation management, emergency response, and other operational functions that they serve.

With these changes, the Electric Utility Trade Associations support the promulgation of this Rule—which will help our members better protect their facilities and minimize the risk of catastrophic damage posed by negligent and malicious drone use.

PART I: RELEVANT BACKGROUND

A. BACKGROUND ON THE ELECTRIC UTILITY TRADE ASSOCIATIONS

1. *Edison Electric Institute (EEI)*

EEI's member companies are the nation's investor-owned electric utilities. Together, they provide electricity to nearly 250 million Americans, operate in all 50 states and the District of Columbia, and support over seven million jobs in communities across the country. EEI member companies work every day to provide reliable energy to their customers at the lowest cost possible. EEI member companies also form the backbone of our nation's electric power industry, which is essential to advancing our economic and national security priorities. Over the next five years, investor-owned electric companies will invest more than $1.3 trillion to enhance the electric grid, building critically needed new generation, transmission, and distribution infrastructure required to power economic prosperity.

2. *American Public Power Association (APPA)*

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. Public power utilities are in every state except Hawaii; they collectively serve over 55 million people in 49 states and five U.S. territories, and account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers. APPA members seek to provide the communities they serve with safe, reliable electric service at the lowest reasonable cost, consistent with good environmental stewardship. This mission aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities.

3. *Large Public Power Council (LPPC)*

The LPPC represents 29 of the nation's largest state and locally owned, not-for-profit public power systems, serving 30.5 million Americans across 23 states and territories. LPPC's members include the larger, asset-owning members of the public power community and account for approximately 90 percent of the transmission assets owned by public power. LPPC members are also members of APPA.

4. *National Rural Electric Cooperative Association (NRECA)*

NRECA represents nearly 900 local electric cooperatives, including 63 generation and transmission cooperatives that generate and transmit power and 832 distribution cooperatives that provide electricity to the end of line co-op consumer members. Local electric cooperatives power 56% of the nation's landmass, serving 42 million Americans, and covering more public lands and forests than any other type of utility. America's electric cooperatives operate at cost and without profit incentive. They are owned by the people that they serve and comprise a unique sector of the electric industry. Due to their unique, not-for-profit business model, cooperatives often operate on thin financial margins, and any increases in regulatory compliance costs and liabilities are passed on to the end of the line consumer.

B. THE CRITICALITY OF THE ELECTRIC GRID

1. *The Electric Grid*

The nation's electric grid is a complex, integrated system with thousands of interdependent facilities, encompassing over 22,000 generators, 55,000 substations, 642,000 miles of high voltage transmission lines, and 6.3 million miles of distribution infrastructure.[4] These components work together to serve as the backbone for public services, economic activity, and other critical infrastructure sectors. The components of the grid are interdependent, such that overall grid reliability depends on continued operation and coordination across the system.

Compromise of critical elements of this system can create substantial radiating harm. Critical elements include both the large facilities covered by the definition of "electricity facility" in the Proposed Rule and smaller facilities that play a central role in the grid's network. Yet, smaller facilities are excluded under the Proposed Rule's unduly narrow definition of "electricity facility," despite their significance to public safety, national security, economic activity, and the communities that depend on the grid's continued functioning.

2. *Regulation of the Electric Grid*

Over two decades ago, in recognition of the critical role that electric grid reliability plays in support of the nation's economic and social welfare, Congress enacted section 215 of the Federal Power Act in 2005, which transformed U.S. electric grid oversight by shifting from voluntary industry standards to mandatory, enforceable federal reliability standards.[5] This statutory provision directs FERC to oversee a certified Electric Reliability Organization (which is now NERC), and to approve mandatory, legally binding grid reliability standards for "bulk-power systems." Violators can be fined up to $1 million a day in civil fines.

The definition of "bulk-power system" recognizes the interconnected, networked way in which the electric grid operates, and encompasses: (i) "facilities and control systems necessary for operating *an interconnected electric energy transmission network* (or any portion thereof);" and (ii) "electric energy from generation facilities needed to maintain *transmission system reliability*."[6] The related definition of "bulk electric system," which is a subset of the "bulk-power system," includes transmission elements operated at 100 kilovolts (kV) or higher—most of which fall outside of the narrow definition of "electricity facility" under the Proposed Rule.[7]

---

[4] Concentric Energy Advisors, Inc., *The U.S. Electric Grid: A Critical Backbone for the Economy and National Security* 1 (2026), https://ceadvisors.com/wp-content/uploads/2026/05/CEA-Grid-Benefits-ES.pdf.

[5] Energy Policy Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 594 (2005) (codified at 16 U.S.C. § 824o).

[6] 16 U.S.C. § 824o(a)(1) (emphasis added).

[7] *See* NERC, *Glossary of Terms*, Bulk Electric System, https://www.nerc.com/glossary-of-terms?alpha=B.

In 2013, following a rifle attack on grid facilities, FERC adopted NERC Standard CIP-014, which mandated key physical security standards for infrastructure deemed critical to grid operations.[8] Standard CIP-014 applies to "Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack *could result in instability, uncontrolled separation, or Cascading within an Interconnection*."[9] Covered utilities include a range of transmission stations and substations that fall below 500 kV, either because they meet specified criteria, are essential to meeting nuclear plant interface requirements, or are defined as critical to the derivation of Interconnection Reliability Operating Limits, the specific limits within a bulk electric system that, if exceeded, could result in instability, uncontrolled separation, or cascading outages.[10]

Covered utilities are required to conduct an "evaluation of the potential threats and vulnerabilities of physical attack to each of their" critical facilities that considers "unique characteristics" of the critical facility, "prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events," and "intelligence or threat warnings received from" government agencies.[11] The utility must develop and implement a utility-specific physical security plan that addresses the specific vulnerabilities identified.[12]

The Proposed Rule's definition of "electricity facility" excludes the many facilities operating below 500 kV that have been deemed critical by FERC and NERC.

3. *The Associations' Use of Drones to Meet Security Needs*

In order to ensure the safe and reliable operation of the electric grid, the Associations' members must regularly inspect power lines. Electric utilities continue to expand the frequency and scope of these inspections in response to evolving regulatory requirements and increased risk factors, caused by fires, extreme weather, and external threats. As investments in new energy generation and grid integration infrastructure grow, inspection demands are expected to continue to increase.

UAS have been invaluable in helping the electric industry meet this increased demand for inspections; they bring significant benefits in terms of cost, safety, accuracy, and access to hard-to-reach areas. The Associations' members report cost reductions of up to 80 percent compared to other inspection methods. UAS can access challenging terrain more quickly, more safely, and more efficiently than traditional manned crews. UAS also can engage in repeatable inspections, which increases accuracy. And they are particularly invaluable in the event of

---

[8] *See* Paul W. Parfomak, Cong. Rsch. Serv., R45135, *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* (2018), https://www.congress.gov/crs-product/R45135.
[9] *See* NERC, *CIP-014-3 — Physical Security* (June 16, 2022), https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-014-3.pdf.
[10] *Id*. at A.4.1.1.
[11] *Id*. at B.R4.
[12] *Id*. at B.R5 (requiring the plan to include "[r]esiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities *identified during the evaluation conducted in Requirement R4*") (emphasis added).

outages or disasters, as they are able to assess damage even before crews arrive, speeding up restoration efforts and reducing service outages.

The Associations seek to ensure that the Rule continues to fully preserve and enable the expansion of the facilities' own UAS use for these critical safety and security reasons, that facilities can appropriately control their airspace to enable these operations to continue unhindered, and that facility-approved UAS are not subject to otherwise applicable requirements that they transit the restricted airspace in the least time practicable—which would make it impossible to use UAS for repeat and critical safety and security purposes.

C. THE SCOPE OF THE THREAT

The electric grid is central to the nation's economic welfare, public health, and national security. In fact, the electric grid serves an enabling function across all other critical infrastructure sectors. This interdependence creates a distinct risk profile: grid disruptions can cascade into water and wastewater systems, telecommunications, healthcare delivery, fuel supply chains, emergency response, financial services, and transportation systems. As described above, and in recognition of the importance of the electric grid, this administration declared the "integrity and expansion of the Nation's energy infrastructure . . . an immediate and pressing priority for the protection of the Nation's national and economic security."[13]

1. *Key Threats*

Negligent and malicious drone use poses significant risk to the electric grid and all the Electric Utility Trade Associations' members. As the Proposed Rule recognizes, unauthorized and malicious use of UAS can cause a combination of physical, surveillance, and cybersecurity threats to the grid.[14] As UAS technology becomes more sophisticated and more readily available, often at very low cost, the risks spread, to include the following:

- Physical Risks: Drones with payloads can drop explosives from above, causing significant damage. Drones can also crash into facilities (both intentionally and unintentionally), causing potential explosions, wildfires, release of hazardous materials, damage to the electric grid, and loss of life.

- Tech Failure Risks: Adding to the risk posed by malicious or negligent drone use, technology failures, such as firmware or software issues, could cause a drone to crash, resulting in damage to the facility, explosion, and wildfires.[15]

- Surveillance Risks: Drones can also be used to surveil facilities and their associated structures. Such surveillance can be used by malicious actors to identify structural,

[13] Exec. Order No. 14156, *Declaring a National Energy Emergency,* s*upra* note 3.
[14] Proposed Rule, 91 Fed. Reg. at 24655.
[15] *See, e.g., Grounding of All Astro Aircraft – In-Flight Software Failure Investigation*, Freefly Systems (Feb. 8, 2023), https://freeflysystems.com/knowledge-base/astro-sb005 (describing an in-flight software failure that affected the flight controls of a Freefly Astro drone and caused it to crash).

physical, and operational vulnerabilities, and to plan subsequent attacks or forced outages.

- Cyber Risks: Unmanned aircraft can be used to deliver malware, steal credentials, or otherwise initiate cyber-attacks against sensitive information technology and operational technology, including supervisory control and data acquisition communication systems. This can cripple sensitive electric infrastructure without resorting to kinetic action.

The risks are far from hypothetical. In November 2024, a young man was arrested moments before he allegedly attempted to attack an electric substation in Nashville, Tennessee with a drone laden with explosives, in an effort to cause a massive explosion that would "shock the system."[16] More recently, in March 2026, the Department of Homeland Security issued an advisory to energy companies warning of potential threats to U.S. energy and urging the sector to increase security and review incident response plans.[17]

Recent drone attacks on energy infrastructure outside the United States further demonstrate the vulnerability of electric infrastructure. In May, a drone strike hit an electric generator outside the inner perimeter of the Barakah Nuclear Power Plant in the United Arab Emirates.[18] In Ukraine, energy infrastructure has faced sustained drone and missile attacks, leaving hundreds of thousands of civilians with limited power.[19] These are two examples of many. GridEx VIII, the electricity industry's largest cyber and physical security exercise in North America, included multiple UAS attacks on a nuclear generating station and transformer station

[16] Press Release, U.S. Dep't of Just., U.S. Att'y's Off. for the Middle Dist. of Tenn., *Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville* (Nov. 4, 2024), https://www.justice.gov/usao-mdtn/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy. *See also* Sean Lyngass, *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,' according to federal law enforcement bulletin*, CNN (Nov. 4, 2021), https://www.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation (describing a July 2020 incident, in which a drone crashed near a Pennsylvania power station in what the FBI, Department of Homeland Security, and National Counterterrorism Center deemed a deliberate attempt to cause damage to transformers or distribution lines).

[17] *See* Transp. Sec. Admin., No. 2026-SAM-200-001, *Surface Transportation Security Awareness Message* (2026), https://buses.org/wp-content/uploads/2026/03/TSA-Security-Awareness-Message-Nation-State-Actors_2026-SAM-200-001_02.28.2026.pdf; Ben Lefebvre, Myah Ward & Mike Soraghan, *DHS Warns US Energy Companies to Beef Up Security for Possible Iranian Retaliation*, EnergyWire (Mar. 4, 2026), https://subscriber.politicopro.com/article/eenews/2026/03/04/homeland-security-warns-us-energy-companies-to-beef-up-security-for-possible-iranian-retaliation-ee-00810691.

[18] Ella Kipling, *UAE Reports Strike Near Abu Dhabi Nuclear Power Plant*, BBC News (May 17, 2026), https://www.bbc.com/news/articles/cwy27pkj1l1o.

[19] Tim Lister & Kosta Gak, *We Must Get Through the Next Few Days*, CNN (Feb. 8, 2026), https://www.cnn.com/2026/02/08/europe/ukrainians-attacks-cold-intl.

and similarly underscored the ways drones pose a credible and growing threat to the electric sector.[20]

2. *The Broader Costs*

The misuse and malicious use of drones threatens not only the safety and reliability of the grid itself but has potential for cascading impacts to many other critical industries and systems such as hospitals, water distribution, and emergency services that rely on the electric grid. Even temporary outages can cause massive disruptions to communities, businesses, and schools, and possibly even lead to the loss of life.

Drone incidents will almost inevitably result in increased energy costs and decreased reliability, as the Associations' members work to address outages, manage system damage, rebuild destroyed or exploited systems, face potential liability for drone-caused wildfires, and absorb increased insurance rates as a result. This makes it hard to achieve the long-standing objective of keeping costs down and reliability high, consistent with the administration's priorities.[21]

[20] NERC, *GridEx VIII: Lessons Learned Report* (Mar. 2026), https://www.nerc.com/globalassets/programs/electricity-isac/gridex/gridex-viii-lessons-learned-report-tlp_clear_final.pdf.

[21] Exec. Order No. 14154*, Unleashing American Energy*, 90 Fed. Reg. 8353 (Jan. 20, 2025) (highlighting the national importance of ensuring affordable and reliable energy resources); Exec. Order No. 14213, *Establishing the National Energy Dominance Council*, *supra* note 3.

PART II. ELECTRICITY INDUSTRY CONCERNS AND RECOMMENDATIONS

UAFRs are important tools that, if implemented effectively, could meaningfully minimize overall risk to our nation's electrical system. By establishing appropriate restrictions over sensitive facilities, entities can protect their facilities from increasingly significant airborne threats, while continuing to enable the productive use of drones for inspections, perimeter surveillance, and other safety and security needs. Flight restrictions also enable entities to better distinguish between compliant and non-compliant UAS operators and thus focus limited security and law enforcement resources on addressing concrete threats.

The Associations are concerned, however, that the Proposed Rule, as currently drafted:

- Fails to account for key and critical portions of the electric sector;
- Establishes an unduly burdensome process that inadvertently creates new security vulnerabilities; and
- Includes so many exceptions that it does not give critical infrastructure owners and operators meaningful control over their airspace—thus undercutting the core purpose of the Proposed Rule.

A. THE SCOPE OF COVERED ELECTRICITY FACILITIES FAILS TO PROTECT CRITICAL FACILITIES

The Proposed Rule's definition of "electricity facility" excludes key facilities and distribution systems that serve significant national security and homeland security interests, and are thus highly vulnerable to the threat posed by the negligent and malicious use of drones. The definition of "electricity facility" also fails to account for the reality of the way the electric grid operates, as networked facilities that operate as an interconnected whole, and thus fails to provide protections for key elements of this network.

1. *Limited Definition of "Electricity Facility"*

The Proposed Rule's definition of "electricity facility" excludes key, critical facilities and systems. The core definition of "electricity facility" includes just three types of fixed site facilities eligible for a UAFR: (1) a power-generation facility with a combined nameplate capacity of 500 megawatts or greater of power; (2) an electrical substation with a capacity of 500 kilovolts or greater of power; or (3) an electrical substation with a capacity of 345 kilovolts or greater of power in the Electric Reliability Council of Texas.[22]

Other sections cover additional but narrow categories of electricity facilities. The Dams Sector covers the narrow category of a "hydroelectric dam with a combined nameplate capacity of 350 megawatts or more of power and have produced 1,850,000 megawatt hours or greater during the previous calendar year;" the Nuclear Reactors, Materials, and Waste Sector covers a "nuclear power plant that is currently operating and generating electricity;" and the

[22] Proposed Rule, 91 Fed. Reg. at 24688 (to be codified at 14 C.F.R. § 74.88(a)(1)-(3)).

Transportation Systems Sector covers electric substations that provide power to pipeline pumping and compressor stations and to railroad catenary systems.[23]

These definitions fail to capture the full range of critical facilities that underpin critical water, health, and communications systems and those which are recognized by the entities with primary responsibility for oversight of the energy systems in the United States (namely NERC and FERC). These definitions also fail to account for the integrated, interdependent nature of the facilities that comprise the electric grid. As described above, a facility's importance in the electric sector depends not only on voltage or nameplate capacity, but also on its role in maintaining grid stability, serving critical load, supporting national security assets, enabling restoration, or preventing cascading outages. The proposed definition's bright-line capacity and voltage thresholds do not capture key facilities that are vital to the continued operation of the grid.

At minimum, the Final Rule should cover "critical electric infrastructure" as defined in the regulations implementing the Federal Power Act—namely "a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters."[24]

Among other concerns, the definitions exclude the following:

- *Defense Critical Electric Infrastructure*, which includes key electric facilities and infrastructure that supports military installations critical to national defense yet does not meet the specified thresholds in the Proposed Rule. In Alaska, for example, which operates on a decentralized grid, *no asset* meets the capacity thresholds in the draft Rule. Yet, there are nine military installations in Alaska, including essential airfields that hold nuclear missile interceptors, and are supported by cooperatives that supply electricity to these installations.[25] None of these cooperatives would be covered by the Proposed Rule.

[23] *Id*. at 24688–89 (to be codified at 14 C.F.R. §§ 74.85, 74.94, 74.95).
[24] *See* 18 C.F.R. § 388.113(c)(3); 10 C.F.R. § 1004.13(c)(3).
[25] For example, the Golden Valley Electric Association provides power to Eielson Air Force Base, the Murphy Dome Long Range Radar Site, the Clear Space Force Station—which holds a sophisticated long-range ballistic missile warning and defense radar system—and Joint Base Elmendorf-Richardson. *See* Golden Valley Elec. Ass'n, *GVEA Awarded Multiple Grants from the Department of War's Defense Community Infrastructure Program* (Oct. 2, 2025), https://www.gvea.com/news-releases/gvea-awarded-multiple-grants-from-the-department-of-wars-defense-community-infrastructure-program/; J. Brian Garmon, *Overcoming Alaskan-Sized Challenges to Provide Energy Assurance*, Air Force Civil Engineer Center (Nov. 27, 2017), https://www.afcec.af.mil/News/Article-Display/Article/1380767/overcoming-alaskan-sized-challenges-to-provide-energy-assurance; U.S. Space Force Combat Forces Command, *Combat Forces Command Long Range Discrimination Radar (LRDR) Operational Acceptance* (Dec. 8, 2025), https://www.ussf-cfc.spaceforce.mil/News/Article-Display/Article/4351261/combat-forces-command-long-range-discrimination-radar-lrdr-operational-acceptan.

- *Assets, including control centers, designated under the NERC CIP-014 standard as critical to the electric grid*, based on a determination that their inoperability or damage "could result in instability, uncontrolled separation, or Cascading within an Interconnection," yet do not meet the criteria established in the Proposed Rule.[26] None of these facilities would be covered by the Proposed Rule.

- *Almost all electric substations in the United States*. Approximately 98 percent of electrical substations in the United States have a maximum voltage rating of less than 500 kV.[27] As a result, the capacity threshold for substations would eliminate most electric substations in the United States.

2. *Failure to Account for the Networked Reality of the Electric Grid*

The Proposed Rule approaches protecting electric infrastructure by assuming a generation facility-by-generation facility, substation-by-substation, and transmission facility-by-transmission facility approach. For reasons discussed above, this does not reflect the reality of how the electrical grid operates. The electric infrastructure is an integrated system of generation facilities, substations, transmission facilities, and distribution facilities supporting specific communities and regions. Owners and operators focus on security of the broader network, not just single, discrete facilities. Risks and vulnerabilities are also spread across networks, comprised of interconnected fixed sites.

There is, as a result, a dangerous mismatch between the Proposed Rule's facility-by-facility approach to securing airspace, the reality of how the electric grid operates, and the networks that our members work to protect. The Associations urge that the definition of electric facilities also account for networked facilities, thus better mapping the Final Rule's protections to the layout of facilities and security needs.

RECOMMENDATIONS:

(i) Lower the thresholds in the definition of "electricity facility" in 74.88(a) to **200 megawatts** for power-generation facilities and **200 kV** for substations.

(ii) Add in the following additional criteria to 74.88(a):

[26] *See* NERC, *CIP-014-3*, *supra* note 9. A description of the vulnerabilities leading FERC and NERC to require these protections is found in *Physical Security Reliability Standard,* Order No. 802, 149 FERC ¶ 61,140 (2014).

[27] Hitachi Energy, *The Velocity Suite*; *see* U.S. Dep't of Energy, *How It Works: Electric Transmission & Distribution and Protective Measures* (Nov. 2023), https://www.energy.gov/sites/default/files/2023-11/FINAL_CESER%20Electricity%20Grid%20Backgrounder_508.pdf.

> **"**(4) Facilities designated under the NERC CIP-014 standard as critical to the electric grid[28]; or
>
> (5) A system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters."[29]

B. THE APPLICATION PROCESS IS UNDULY BURDENSOME, COSTLY, AND CREATES INADVERTENT SECURITY RISKS

The process and criteria for establishing a UAFR under the Proposed Rule ask for extremely sensitive data that, if made publicly available, would create significant security risks. Other parts of the process seek information that is simply not available. The Associations urge that the final rule protect against the creation of a centralized database with sensitive vulnerability and security information, include other essential protections for sensitive information, and avoid unduly burdensome and costly data gathering exercises that could ultimately result in increased costs to consumers.

The Proposed Rule would require UAFR applicants to submit information demonstrating a safety or security need to justify the requested airspace restrictions. This includes: (i) requirements to describe details, where available, about unmanned aircraft operations over the fixed site facility in question *during the last 24 months*; (ii) detailed information about the facility's vulnerabilities; and (iii) detailed information about the consequences of those vulnerabilities, if exploited.[30] Each of these requirements poses a concern.

1. *§ 74.66(A) – Existing unmanned aircraft traffic patterns*

The FAA proposes to require applicants to provide extensive information about UAS traffic patterns over a given site in the past 24 months, where available, including the "type of unmanned aircraft operation, if known; identify whether the operator is known to the operators or proprietors; and quantify the total number of operations not associated with the facility itself."[31]

FAA states that it is seeking this information in order to establish "a baseline for existing traffic" in order to "help FAA understand current operations over the facility [and to] create a reference point for evaluating the effectiveness of the UAFR once it is active."[32] The agency

[28] NERC, *CIP-014-3, supra* note 9.
[29] *See* 18 C.F.R. § 388.113(c)(3); 10 C.F.R. § 1004.13(c)(3).
[30] *See* Proposed Rule, 91 Fed. Reg. at 24687 (to be codified at 14 C.F.R. § 74.66).
[31] *Id*. (to be codified at § 74.66(a)).
[32] Proposed Rule, 91 Fed. Reg. at 24664.

further states that it will "use this information to understand existing threats and hazards and to evaluate the likelihood that a safety or security incident could occur."[33]

This provision raises several concerns:

- *First*, it asks for information that most owners and operators of electrical facilities simply do not have. Even if available in part, compiling this information would be labor intensive, extraordinarily costly, and almost certainly incomplete. While the FAA includes a caveat that this information is required "where available," the Associations are concerned that there will be an expectation that this information be provided, and an implicit bias against those that fail to do so. This is an expectation that most electric facilities cannot meet.

- *Second,* even if historical UAS activity data were to be available for a facility, the Associations question the utility of such data, particularly given how quickly UAS technology and associated threats are evolving. Put simply, two-year-old historical data is likely to have limited relevance to current and future drone activity and risks; requiring the FAA to review such data creates an unnecessary administrative burden, with limited value. Moreover, the absence of prior drone activity is a poor measure of future risk.

- *Third,* this kind of requirement raises broader concerns about the kind of costs utilities are expected to bear in order to obtain a UAFR. The Associations recognize that once a UAFR has been issued, applicants will be required to implement Remote ID detection or equivalent technology to be able to receive data about unmanned aircraft operating within or in proximity of the UAFR.

  But they should not be required to invest in costly detection systems as a condition of even applying for a UAFR *prior* to obtaining one. Of particular concern, utilities are regulated entities that recover prudently incurred compliance costs through increased rates. This is particularly important given the ongoing and significant concerns about affordability and increasing electricity costs. A facility receiving a UAFR should not be contingent upon the ability to afford air traffic detection technologies and personnel; nor should it come at the expense of the ratepayer.

  As discussed further below, the Associations are also concerned about a rule that entrenches Remote ID as the sole detection standard and recommends additional language that will enable broadcast requirements and detection systems to adapt to evolving technology over time.

[33] *Id.*

RECOMMENDATIONS:

- For initial applications, the FAA should ask for any *known* information about flight patterns over a facility, should ask for historical data going back up to 12 months at the most, and should make it clear in the text of the Rule that UAFR applicants should not attempt to retroactively produce data that is not readily available.

- For renewal requests, the FAA should ask for data consistent with the Remote ID requirement or similar detection technology.

- The FAA should require that applicants commit to implementing Remote ID or similar detection technology if granted a UAFR; applicants should not be required to invest in potentially costly detection systems unless they are granted a UAFR.

2. *§ 74.66 (B), (C), (D) – Vulnerability, Consequence, and Effect*

The Proposed Rule would require applicants to "describe the weaknesses or gaps that may be intentionally or unintentionally exploited" by a UAS and the consequences of those identified vulnerabilities, if exploited by a UAS.[34] Applicants are also required to describe current security plans and how the flight restrictions would be integrated into those plans to reduce risk.[35]

These provisions would require the sharing of highly sensitive data that, if made public, would give adversaries a roadmap of electrical facilities that may be vulnerable and how to attack them. Moreover, even if the FAA never intends to make such data public, it would essentially be creating a honeypot of valuable information that adversaries would seek to exploit and access.

In fact, much of this information is separately recognized by FERC as Critical Energy/Electric Infrastructure Information ("CEII"), pursuant to section 215A of the Federal Power Act, and thus is subject to multiple protections in terms of how it is handled and shared.[36]

[34] *See* Proposed Rule, 91 Fed. Reg. at 24687 (to be codified at 14 C.F.R. § 74.66(b), (c), (d)). Vulnerability is defined broadly, as "something in a fixed site facility's infrastructure, software systems, operations, or procedures that an unmanned aircraft could exploit or inadvertently interfere with in a way that could harm the facility, impede the facility's mission, or present a hazard to people or property." Proposed Rule, 91 Fed. Reg. at 24664.

[35] Proposed Rule, 91 Fed. Reg. at 24687 (to be codified at 14 C.F.R. § 74.66(d)).

[36] *See* 18 C.F.R. § 388.113.

RECOMMENDATIONS:

- The FAA should not require entities to share detailed information about vulnerabilities and security plans. The FAA should instead establish a self-attestation framework to establish need, vulnerability, and effective security plans, incorporating the risk-based approach adopted in NERC and FERC security frameworks.

- A self-certification process would guard against the disclosure of vulnerabilities and reduce administrative burdens. It also matches processes that have been successfully used by agencies for many years.[37]

- The FAA should adopt a presumption of accuracy of self-attestation, should deny an application only with clear evidence that the attestation is inaccurate or incomplete, and should defer to the Sector Risk Management Agencies to the extent there is any question as to need and vulnerability.

- Entities should be required to maintain documentation to support the self-certification, which can be audited by the FAA, in coordination with the SRMA, as necessary.

- The FAA should rely on existing NERC and FERC compliance structures wherever feasible, rather than creating duplicative federal processes for validating security need, vulnerability, or protective measures. This aligns with the administration's stated objective of alleviating burden by eliminating unnecessary regulation.[38]

[37] In a recently issued Interim Final Rule, DHS and DOJ allow private correctional facilities and law enforcement agencies to self-attest to compliance with Counter-UAS regulations. *See* Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correction Agencies, 91 Fed. Reg. 41466, 41488 (to be codified at 6 C.F.R. § 124.6(d)). Other agencies have similar self-attestation rules. *See* 47 C.F.R. § 2.906 (requiring a manufacturer, importer, or integrator to certify that the equipment complies with applicable FCC technical standards and other requirements); 18 C.F.R. § 292.207(a) (allowing an owner or operator of a qualifying facility to self-certify that the facility meets the requisite criteria without going through a formal FERC review process); Financial Industry Regulatory Authority (FINRA) Rule 3130(b) (requiring the CEO or equivalent officer to certify annually that the entity has policies and written supervisory procedures in place that are reasonably designed to achieve compliance with applicable FINRA rules, MSRB rules, and federal securities laws and regulations); Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7241 (requiring regular certification or attestations to the SEC as to the accuracy of financial disclosures); 17 C.F.R. § 40.2 (allowing a designated contract market or securities exchange firm to list a new contract for trading without prior Commodity Futures Trading Commission (CFTC) approval by filing a written self-certification that the product complies with the Commodity Exchange Act and CFTC regulations); 32 C.F.R. §§ 170.15–.16 (laying out the requirements for self-assessment and affirmation for the Cybersecurity Maturity Model Certification Program of the Department of War).

[38] Exec. Order No. 14192, *Unleashing Prosperity Through Deregulation*, 90 Fed. Reg. 9065 (Jan. 31, 2025).

3. *§ 74.68 – Externalities*

Under the Proposed Rule, the FAA would also require applicants to describe externalities resulting from the proposed UAFR, including details about costs and disruption to *other* users of the airspace.[39] This is an unworkable requirement—one that would require electric facilities to gather information about third parties' activities and plans that they simply do not have access to.

RECOMMENDATION: Delete the Proposed Rule's requirement to describe externalities in the application.

4. *§ 74.70 – Environmental Impact*

Under the Proposed Rule, applicants would be required to identify and describe ten distinct categories of sensitive land uses and other resources that are within, adjacent, or proximate to the boundary of the proposed UAFR, and potentially generate an environmental assessment about these adjacent facilities.[40]

Electric utilities simply do not have access to this kind of detailed information about third parties. It is impracticable and unworkable to expect electric utilities to have this kind of nuanced, detailed information about adjacent landowners and potential environmental impacts on third parties outside their control. It is difficult to see how restricting drone operations in electric airspace due to security concerns would result in a significant environmental impact.

RECOMMENDATION: Delete the Proposed Rule's requirement to assess environmental impact in the application.

5. *§ 74.56 – "Protective Security"*

The Proposed Rule would require that an applicant has in place protective security, including security monitoring.[41] However, it does not specify what kind of monitoring is required. For this to be workable, applicants should be able to demonstrate a risk-based approach to security monitoring, including by demonstrating compliance with existing security frameworks, such as the NERC CIP standards requirements discussed above or other federal government security programs.

Given ongoing cost concerns, the Associations are also concerned about the potential for this requirement to be interpreted to require investment in high-cost detection systems that most

[39] Proposed Rule, 91 Fed. Reg. at 24687 (to be codified at 14 C.F.R. § 74.68).
[40] *Id*. (to be codified at 14 C.F.R. § 74.70).
[41] *Id*. at 24686–87 (to be codified at 14 C.F.R. § 74.56).

of our members simply cannot afford. A multi-layered radio frequency, camera, and acoustic detection system could cost upwards of half a million dollars per facility.[42] These are costs that will ultimately be borne by consumers. As a result, a detection system requirement should be focused on the technologies needed to identify drones that are broadcasting Remote ID signals or equivalent technology, to establish a baseline of lawful drone use at a given site.

RECOMMENDATIONS:

- Adopt a risk-based approach to protective security, commensurate with the nature, sensitivity, and risk profile of a given facility.
- Applicants should be able to rely on compliance with existing NERC, FERC, or other applicable security compliance frameworks as evidence of an effective security plan.

6. *The FAA Should Allow Batched Applications*

Given the interconnected nature of the grid and large number of facilities, the requirement that individual applications be submitted for each individual facility is incredibly burdensome. The FAA should instead allow a single applicant representing multiple locations to submit batch applications for facilities with similar profiles. This would significantly decrease administrative burden for FAA reviewers while streamlining the protection for similar facilities that each plan to apply. The FAA could retain discretion to evaluate UAFR locations individually while saving time by analyzing facilities with similar security plans, chemicals of interest, physical layouts, and hazards. Ideally, the single applicant in the energy and chemical sectors would be the parent company of the batch facilities. To address the potential administrative burden for both the private and public sectors that would stem from a facility-by-facility approach to applying for UAFRs, the FAA should create a system to allow applicants to submit consolidated or programmatic applications where facilities or operations share similar characteristics, with standardized criteria applied across qualifying assets.

RECOMMENDATIONS:

- Applicants should be permitted to submit a single application covering multiple facilities or assets (e.g., substations, transmission corridors, or distribution systems) that have common ownership, operate under a single operational plan, and meet the requisite criteria within a defined service territory.
- This batched approach will streamline the number of applications a given entity will need to submit, reduce the administrative burden on FAA, and enable consolidated review of facilities with similar vulnerabilities and security plans.

[42] WaveDone, *Counter-UAS Cost-Benefit Analysis: Economics of Drone Defense* (Mar. 12, 2026), https://wavedone.com/counter-uas-cost-benefit-analysis-economics-of-drone-defense/.

- A batched application and designation process also would better align the UAFR process with the manner in which utilities assess risk, develop security plans, coordinate restoration activities, and manage interconnected infrastructure systems.

7. *The Renewal Process Should Be Streamlined*

While § 74.210 of the Proposed Rule establishes a renewal process requiring an applicant to renew their request for a UAFR every five years, the text of that section lacks any additional specificity as to the structure or content of that reapplication process.[43] To prevent potential lapses in protection, the FAA should adopt a streamlined process for renewal. This would ensure an efficient UAFR renewal process that limits the burden on both applicants and the FAA.

RECOMMENDATIONS:

- Establish presumptive renewals for applicants whose operations remain unchanged from their original UAFR application.

- Create a short form certification for renewals using streamlined templates. These templates should focus on addressing any material changes made since the last application and avoid requiring the resubmission of previously approved information as much as possible.

C. THE NOTICE AND COMMENT PROCESS RAISES SIGNIFICANT SECURITY RISKS AND RELATED CONCERNS

The Proposed Rule envisions a public notice and comment period for *each* UAFR request that is conditionally approved, unless the agency has "good cause" to forgo that period.[44] This process creates significant security concerns and appears to be based on a misguided application of rules governing manned aircraft to flight restrictions governing low-altitude airspace.

1. *The Notice and Comment Process Raises Significant Security Concerns*

The notice and comment period would effectively put a target on a facility's back—alerting the world that it deems itself vulnerable, has requested the protection of a UAFR, but does not have one. This creates significant security risk, which would be exacerbated if the notice includes any of the sensitive information that the FAA seeks to collect from applicants.

[43] Proposed Rule, 91 Fed. Reg. at 24690 (to be codified at 14 C.F.R. § 74.210).
[44] *Id*. (to be codified at § 74.100(c)).

2. *The Notice and Comment Process Creates Significant Administrative Burdens*

Creating individual notice and comment periods for even a subset of all potential UAFR requests will pose a significant administrative burden. It will require the FAA to publish the proposed restrictions in the Federal Register (which itself requires several administrative steps), provide for a 30-day review period, and then review and assess comments. This will inevitably add time to the process and cause delays in decision-making, making it hard for the FAA to finalize its review within the presumptive 90-day statutory deadline for making a final UAFR determination.[45]

3. *The Notice and Comment Process Should Be Replaced With a Mechanism for Affected Third Parties to Seek Modification or Rescission Post UAFR Issuance*

It appears that this provision is modeled after the requirements for designating controlled airspace for civil aviation operations.[46] Those provisions are intended to provide public input on much more weighty and consequential government actions affecting manned aircraft and commercial airspace. As applied to UAS operations at or below 400 feet, the potential disruptions to third party operations are nowhere near as significant, and there is no equivalent basis to require a notice and comment period for such UAFRs.

The FAA can—and should—create a mechanism for third parties to raise concerns and identify specific externalities. But this process should be triggered only after a flight restriction has been announced, so as to protect against the significant security concerns highlighted above.

RECOMMENDATIONS:

- Eliminate the notice and comment provision.
- Replace with a **post-designation process** for interested parties that are negatively affected by a UAFR to raise their concerns and petition to modify or lift the UAFR **subsequent to UAFR issuance**.

D. THE SCOPE OF RESTRICTIONS IS INSUFFICIENT AND RISKS UNDULY LIMITING THE PROACTIVE USE OF DRONES FOR SECURITY AND SAFETY

The standard UAFR includes several exceptions for commercial and recreational drones that provide advance notice to the FAA and fixed site facility, broadcast a Remote ID, and transit the UAFR in the shortest time practicable.[47] These provisions raise significant concerns:

[45] *See* FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 2209(b)(2)(A), 130 Stat. 615, 634 (codified at 49 U.S.C. § 40101 note).
[46] *See* 14 C.F.R. § 71.1 (establishing a notice and comment period for controlling commercial airspace).
[47] Proposed Rule, 91 Fed. Reg. at 24690 (to be codified at § 74.250(a)).

- *First,* they are overbroad and significantly less restrictive than existing temporary flight restrictions ("TFRs"), which generally require affirmative authorization or waiver to fly over a restricted area. Such authorization is typically available to entities with a demonstrated need to operate in the restricted airspace, such as public safety agencies, first responders, emergency-response personnel, or certain media operations.

  The proposed UAFR, by contrast, authorizes a wide array of commercial and recreational drone activity, with advance notice only. These kinds of broad, automatic exceptions undermine the security purpose of the Proposed Rule. It would allow operators with no relationship to the facility, no site-specific need, no facility authorization, and no separate emergency or public safety justification to enter protected airspace.

  A UAFR with such broad exceptions will fail to provide the practical security benefit Congress intended when it directed the FAA to establish this process.

- *Second*, the Associations are concerned that, as drafted, the Proposed Rule does not include sufficient protections for facility-approved drones used for safety, security, or inspections. As drafted, the Proposed Rule appears to require even facility-owned drones to be subject to the operational conditions laid out by § 74.250(a), including the requirement that they transit the airspace in the shortest time possible.

  This is inconsistent with the way facility-owned drones are used. In practice, facility-owned or authorized UAS may need to remain within a UAFR to perform legitimate operational functions that require a UAS to hover, circle, conduct repeated passes, follow electric infrastructure, or otherwise operate for a duration longer than the shortest amount of time practicable.

RECOMMENDATIONS:

- Ensure fixed site facility owner/operators have meaningful control over the airspace protected by UAFR.
- Commercial and recreational drone operations over defense critical electric infrastructure, nuclear sites, and other critical elements of the electric infrastructure pose an inherent risk and should be categorically prohibited.
- To the extent commercial and recreational UAS operations are permitted over restricted airspace, such flights should require *express approval* by the relevant facility prior to operating. Conversely, drones being used for emergency response and public safety reasons should be permitted with notice to the facility owner/operator, as the Proposed Rule envisions.

- The Rule should explicitly authorize facility managers to maintain a list of approved drones that are permitted to transit the protected airspace without restriction, which is essential to enabling routine inspection, maintenance, reliability, restoration, vegetation management, emergency response, and security-related operations.

E. ADDITIONAL RECOMMENDATIONS

1. *Provide Flexibility to Adapt to Evolving Technologies*

The Proposed Rule is premised, in part, on the continued use of Remote ID as the key technological means to distinguish authorized and unauthorized drones. In light of evolving technology, the Final Rule should create flexibility to enable the FAA to require *either* Remote ID and associated detection equipment, *or* other equivalent technology, as approved by the FAA. This is needed to allow for technological developments over time without requiring a new rulemaking.

RECOMMENDATIONS:

- The FAA should not lock itself into Remote ID technology as the sole approved detection technology.

- Instead, any requirement should reference Remote ID "or other technology designated by the FAA for these purposes," thereby preserving the agency's flexibility to update or supplement these requirements as technology evolves without the need to initiate a new rulemaking proceeding.

2. *Expand the Scope of Protected Areas Based on Security Needs*

The Proposed Rule specifies that flight restrictions may not exceed the fixed site facility property boundary.[48] The final rule should also account for the fact that the risks posed by UAS are not limited to direct overflight of a protected asset.

A drone operating just outside a facility boundary may still be capable of conducting surveillance, identifying security vulnerabilities, interfering with operations, or delivering a payload with precision. In many cases, the relevant security concern is not simply whether a UAS crosses the vertical plane above a facility, but whether it is operating close enough to create a credible threat to the facility, its personnel, or its supporting infrastructure.

[48] *Id.* at 24687 (to be codified at 14 C.F.R. §§ 74.58, 74.60) (defining the lateral boundary and altitude ceiling of the flight restrictions).

RECOMMENDATION: Enable applicants to apply for buffer zones, based on identified security needs. The appropriate buffer zone will vary based on the size, configuration, location, and risk profile of the facility.

3. *Support Strong Enforcement*

The Associations encourage the FAA to exercise active enforcement authority over drone flights that violate restricted airspace. The final rule should enable and encourage critical infrastructure and law enforcement to work together to enforce violations of UAFR restrictions.

F. CONCLUSION

The Electric Utility Trade Associations thank the FAA for the opportunity to comment on this important Proposed Rule. The Associations look forward to serving as a resource for the FAA on this subject and encourage the FAA to reach out to our counsel, Jennifer Daskal, at 202-344-4975 or JDaskal@Venable.com, with any questions or comments.

Respectfully submitted,

Jennifer Daskal

Jennifer C. Daskal
Venable LLP
Partner
Jdaskal@venable.com

Aryeh B. Fishman
Edison Electric Institute
Associate General Counsel
afishman@eei.org

Latif Nurani
American Public Power Association
Senior Regulatory Counsel
lnurani@publicpower.org

Jonathan D. Schneider
Stinson LLP
Counsel for the Large Public Power Council
jonathan.schneider@stinson.com

Megan Olmstead
National Rural Electric Cooperative Association
Regulatory Affairs Director
megan.olmstead@nreca.coop