WHITE PAPER

Current Approaches and Regulations in the United States to:

Protect Energy Production and Grid Infrastructure from today's Drone Threats

Current Mitigation Options and Approaches, Operational Model, and a Call to Action

PREPARED FOR: North American Transmission Forum (NATF)
AUTHOR: Southern States, LLC DATE: April 2026

Southern States

Powers the Future™

CONTENTS

EXECUTIVE SUMMARY

Unmanned aerial systems (UAS), commonly referred to as drones, have rapidly evolved from hobbyist devices into tools capable of surveillance, sabotage, and kinetic attack with easily obtained energetics from local retail stores throughout the United States. Energy producing sites and the supporting pipeline and transmission infrastructure – including substations, generation facilities, pipelines, and control systems – represent one of the most strategically attractive targets for near peer adversaries and terrorist organizations seeking to attack the United States.

Recent geopolitical developments, including ongoing tensions with China and military actions involving Iran and its proxy networks, have heightened concerns regarding asymmetric threats to U.S. infrastructure. At the same time, domestic incidents and news reporting in the United States have documented increasing drone activity near critical infrastructure facilities, including power generation and grid assets.

In Iran, Ukraine, and other places, the first places targeted are energy sites. Terrorists know this also.

Many commercially available RF-based detection systems rely on signal libraries and are limited to identifying drones that emit command-and-control or telemetry signals. However, a significant portion of modern threat drones operate autonomously using pre-programmed waypoint navigation. No terrorist is using a joystick or is anywhere near the site being attacked. These terrorist drones often emit no detectable RF signal, relying instead on passive GPS reception or, in more advanced cases, visual odometry that eliminates dependence on GPS entirely. As a result, these “RF-silent” or “dark” drones are not detectable using RF listening technologies and cannot be disrupted using electronic jamming or protocol exploitation.

Accordingly, radar remains the only reliable method for early detection and tracking of non-cooperative or autonomous drones. Radar systems operate within regulated spectrum environments governed by the Federal Communications Commission (FCC) and are widely deployed across aviation and defense applications. When properly authorized and configured, these systems present no risk to the National Airspace System.

Given the limitations of electronic countermeasures, effective mitigation of non-cooperative drones must ultimately rely on physical (kinetic) means, such as interception or capture. These drone interceptors are being deployed across the United States and have been widely used at major events such as the Olympics and the World Cup.

Unlike military installations, most energy infrastructure was not originally designed with aerial surveillance or drone intrusion in mind. Fortunately, regulatory and technological conditions allow deployment today, with additional regulations rapidly evolving in favor of increased simplification of the operations for infrastructure protection:

- The SAFER Skies Act, in December 2025, now allows trained state and local law enforcement (SLTT) agencies to conduct drone mitigation in partnership with utilities and owners of private infrastructure.
- The FAA is advancing Part 108, which will enable expanded Beyond Visual Line of Sight (BVLOS) drone operations with performance-based safety requirements.
- Modern sensor architecture now allows utilities to monitor airspace around substations and generation sites with high confidence at reasonable price points.
- Kinetic mitigation techniques such as interceptor drones have been developed in partnership with Federal agencies and are now approved for the United States airspace. For example, these are being used in this year’s World Cup sites because they are proven safe and effective to use in commercial settings to defeat terrorist drones.
- Regulatory movement is under consideration via a pending Executive Order, which would allow certain infrastructure providers to mitigate drones over their property unilaterally without the coordination required today with local and state law enforcement.

While detection, tracking, and Identification (DTI) capabilities are legal for NATF members to deploy within the current regulatory framework, the mitigation authorities are still controlled, now by state and local law enforcement in addition to federal components.

There are options for NATF members to deploy the mitigation assets now in 2026 to be ready by 2027.

While mitigation authorities continue to be extended in this heightened threat environment, interceptor drones – highly recommended over missiles and electronic warfare/jamming approaches – can be used today most easily from remote security operations centers with law enforcement cooperation. The owner of the infrastructure is encouraged to deploy the mitigation assets immediately, develop procedures, processes, ownership, and operational methods allowing their use today in various modes with current regulations, while in parallel establishing coordination with law enforcement.

OBJECTIVE

THIS WHITE PAPER OUTLINES:

1. The evolving regulatory framework governing drone detection, tracking, identification, and mitigation
2. A proven layered approach for protecting energy infrastructure
3. Options and operational pathways utilities can deploy today and be within the regulations today to detect, track, identify, and mitigate terrorist drones

The objective is to provide confidence to NATF members that regulatory conditions exist and are continuing to shift in favor of responsible infrastructure protection, allowing utilities to begin implementing layered drone defense strategies in coordination with law enforcement and federal partners today.

1.0 The Emerging Drone Threat to Energy Infrastructure

Electric utilities have historically focused security investments on physical and cyber threats. However, drones introduce a **third operational domain: low-altitude airspace security**.

Threat vectors include:

- Surveillance of substations and switching yards
- Delivery of explosives or payloads to energy producing sites, such as dams, nuclear plants, etc., and key substations serving millions of energy users
- Kinetic disruption of transformers or control centers

Small commercial drones now possess:

- Ranges exceeding 10 km
- Autonomous navigation
- High-resolution cameras
- Payload capacity for explosive devices

These systems are inexpensive, widely available globally, and are not detected by traditional drone RF antennas because they are flown without emitting any radio signals.

Several recent domestic incidents reported in U.S. media outlets have documented suspicious drone activity over critical infrastructure locations, including energy facilities in California and other states. While many incidents remain under investigation, the trend has drawn increasing attention from federal law enforcement and homeland security agencies.

The concern is not hypothetical.

Nation-state actors have already demonstrated drone-based attacks on energy infrastructure in Ukraine and the Middle East, including coordinated strikes on oil facilities.

The energy grid presents a similarly attractive asymmetric target.

2.0 Regulatory Framework Governing Counter-UAS Detection, Tracking, and Identification (DTI) in the United States

Effective counter-UAS operations require the ability to detect, track, identify, and mitigate (DTI-M) unauthorized or malicious drones. While mitigation authorities remain tightly controlled under federal law (as discussed in Section 3.0), detection, tracking, and identification capabilities are broadly permissible when implemented in compliance with applicable communications, privacy, and aviation regulations.

This section outlines the regulatory considerations applicable to DTI systems deployed by critical infrastructure owners.

A key regulatory distinction must be emphasized:

- Detection, tracking, and identification (DTI): Generally permissible under U.S. law when conducted using passive or non-interfering technologies
- Mitigation (e.g., jamming, spoofing, takeover, capture, or destruction): Restricted to authorized federal entities and trained state and local law enforcement under statutory authorities such as 6 U.S.C. §124n and 10 U.S.C. §130i

DTI systems must therefore be designed to observe and characterize airspace activity without interfering with aircraft operations or communications.

The Southern States' solution for countering drones is compliant with all these regulations as they exist today.

2.1 Radar Detection

Radar systems form the foundation of non-cooperative drone detection and are governed by U.S. spectrum regulations.

Radiofrequency emissions in the United States are regulated by the **Federal Communications Commission (FCC)** for non-federal users and the **National Telecommunications and Information Administration (NTIA)** for federal spectrum coordination.

Key regulatory considerations include:

- Operation within authorized frequency bands (licensed or compliant with applicable FCC rules, such as Part 15 or Part 90 where applicable)
- Coordination near sensitive environments, including airports and federal installations
- Compliance with RF exposure safety standards for personnel and the public

Modern counter-UAS radar systems are engineered to operate within established regulatory limits for spectrum use and electromagnetic exposure.

These systems typically utilize low-power emissions relative to traditional aviation radar and are designed to support safe deployment in proximity to populated or operationally sensitive environments, subject to proper coordination.

When required, deployment may involve a standard FCC licensing or coordination process, which is well-established and routinely used for commercial and infrastructure applications. For example, AM/FM radio is widely broadcast at airports in the United States and is seen as safe given FCC licensing. To deploy a radar for counter-UAS, Southern States can help customers obtain an FCC license at their site. The process has a usual lead time of about 30 days and requires a small application fee.

2.2 RF Detection, Remote ID, and Applicable Federal Statutes

2.2.1 Regulatory Context

RF-based detection systems operate by passively monitoring radiofrequency activity associated with unmanned aircraft. These systems may identify:

- Signal characteristics (frequency, modulation, power)
- Drone and controller location (via signal triangulation)
- FAA-required Remote ID broadcast information

Importantly, compliant systems do not access or decode the content of communications (e.g., video payloads or command data) but instead analyze signal metadata and publicly broadcast identification information.

The FAA Remote ID rule (14 CFR Part 89) requires drones to broadcast identification and location data over publicly accessible frequencies, explicitly intended to be receivable by third parties for safety and accountability purposes.

As affirmed in *Brennan v. Dickson*, 45 F.4th 48 (D.C. Cir. 2022), such broadcasts are not considered private communications.

2.2.2 Applicable Federal Statutes

Several federal statutes govern electronic surveillance and communications monitoring. Properly designed DTI systems operate within these legal boundaries:

- Wiretap Act (18 U.S.C. § 2511): Prohibits interception of the *contents* of communications. Passive monitoring of signal characteristics or publicly broadcast Remote ID data does not constitute interception of content.
- Pen Register and Trap and Trace Statutes (18 U.S.C. §§ 3121–3127): Apply primarily to routing and addressing information in telecommunications networks (e.g., phone numbers), and do not restrict analysis of RF signal characteristics or publicly broadcast drone identification data.
- Communications Act (47 U.S.C. § 605): Prohibits unauthorized interception and disclosure of non-public communications. It does not apply to publicly broadcast signals or signal-level analysis.

Consistent with these statutes, compliant RF detection systems:

- Do not intercept or store communication content
- Operate on signals that are either publicly broadcast or inherently observable in the RF environment
- Support aviation safety objectives by enhancing situational awareness

This approach aligns with federal guidance and existing case law, including distinctions drawn in *Joffe v. Google*, where liability was tied to the collection of payload data rather than signal characterization.

2.3 Relationship to Federal Counter-UAS Authorities (6 U.S.C. §124n)

Section 124n provides authority for the Department of Homeland Security and the Department of Justice to conduct counter-UAS activities that would otherwise violate certain federal laws.

However, this authority is only required when an activity involves:

- Interference with communications
- Capture, destruction, disruption, or control of aircraft
- Access to protected communication content

DTI systems that are passive, non-interfering, and limited to signal detection and publicly available information do not trigger these statutory restrictions. Accordingly, such systems can be lawfully deployed by infrastructure owners without requiring federal counter-UAS authorization.

2.4 Compliance Position of Layered DTI Architectures

A properly designed layered DTI architecture – combining radar, RF detection, and EO/IR sensors – can be deployed in full compliance with U.S. law when it adheres to the following principles:

- Non-interference: No jamming, spoofing, or protocol manipulation
- No content collection: No interception of payload data or communications content
- Use of public or observable signals only: Including Remote ID and RF emissions
- Spectrum compliance: Operation within FCC and, where applicable, NTIA guidelines
- Privacy-by-design: Minimization of data collection and alignment with civil liberties expectations

Such architecture provides critical airspace awareness capabilities while remaining clearly distinct from regulated mitigation activities.

3.0 Regulatory Framework Governing Counter-UAS in the United States

Drone detection and mitigation in the United States are governed by a layered framework of federal statutes, aviation regulations, and communications laws.

The key regulatory reality today is that **detection is broadly permissible. Mitigation authority is tightly controlled.**

3.1 Federal Counter-UAS Authorities

The core legal authority enabling counter-drone operations is the Preventing Emerging Threats Act of 2018, codified at 6 U.S.C. 124n. Federal law enforcement domestic counter-UAS operations are governed by 6 U.S. Code § 124n - *Protection of certain facilities and assets from unmanned aircraft.* 6 U.S. Code § 124n, part of the 2018 FAA Re-authorization, has been extended each year without update or change since its first expiration in 2022.

Department of Defense domestic authorities come from for 10 U.S. Code § 130i which is similar in terms of the coordination process required to mitigate a drone in the United States.

In summary, DHS, DOJ, DoW, and in limited cases DOE, have authority to disrupt, mitigate, and stop a drone in the United States. Only a few components in DHS have the authority to stop drones (USSS/ CBP / USGG / FPS, not TSA). Within DOJ, the FBI, USMS, DEA, and BOP can be authorized by the Attorney General. The USSS and FBI deploy most frequently within the DOJ construct in support of SEAR events and NSSE's with significant caveats and following an in-depth coordination process.

Process for authorized Federal components to act on a 124n or 130i mission:

- Component appeals to the Department-level Program Office to include a new covered facility or asset with a requisite risk-based assessment.
  - Some covered facilities or assets are considered inherently high-risk, negating the risk-based assessment requirement.
- Submit the Concept of Operation document detailing all aspects for the proposed deployment to the FAA for coordination.
- Concept of Operations covers:
  - NOTAMS
  - TFRs
  - Public outreach
  - Privacy notifications
  - Authorized enforcement area
  - Anticipated enforcement area
  - Inter and intra-agency notification process
  - Identification of authorized agent
  - Component and FAA leadership (SES) sign a joint coordination official memorandum (OM) on behalf of their respective Director/Administrator stating all coordination is complete and both sides concur.
  - Final approval to deploy is made by the Department Cabinet Head (Sec DHS, AG, or Sec Def) for the respective requesting component.

This process is well known by the authorized components. Approval happens quickly, provided all criteria are met.

This process is completed multiple 100's of times a year, with the USSS the most frequent user.

Authorized components must go through the coordination process to deploy counter UAS equipment for each location and mission with final approval to deploy assigned to the Cabinet level executive (Secretary Homeland for DHS / Attorney General for DOJ / Secretary of Defense for DoW – or designee). Authorities only cover counter-UAS missions as they relate to components' authorized duties. For example:

- For U.S. Secret Service protection operations:
  - Security or protection functions of the U.S. Customs and Border Protection
  - Protection of facilities pursuant to Title 40 (Government Buildings) Federal Protective Service
  - Missions authorized to be performed by the United States Coast Guard
- For DOJ protection operations, it must relate to missions pertaining to personal protection operations conducted by:
  - Federal Bureau of Investigation
  - United States Marshals Service (courts and witnesses)
  - Federal Bureau of Prisons
  - Or support of missions performed by DHS or DOJ for NSSEs, SEAR events, and in support of SLTT - upon request through the governor of the state to DHS.

3.2 Expanding SLTT Authorities: Safer Skies Act of December 2025

The Safer Skies Act, in December 2025, is a tidal shift in the counter-drone industry. The act expands the role of state and local law enforcement (SLTT) by granting authority to allow state and local law enforcement to mitigate drones. SLTT must be certified via federal training before protecting critical infrastructure and large events, such as the World Cup in 2026.

The act also reauthorizes and expands federal counter-drone authorities through 2029 and establishes FAA counter-UAS performance standards, expands covered sites, and strengthens privacy protections.

Federal training programs – including those conducted at the FBI facility in Huntsville, Alabama – are preparing operators for:

- Detection, tracking, and identification with advanced systems supporting classification
- Legal compliance
- Mitigation execution, including interceptor drones

3.3 FAA Regulatory Environment

The FAA governs the National Airspace System.

Key elements of the FAA regulatory framework for drones include:

3.3.1 Part 107

Part 107 currently governs commercial drone operations, where today drones must be flown by an operator with line of sight (LOS), and not over people, and not at night. Beyond Visual Line of Sight (BVLOS) operations today require waivers under 14 CFR Part 107.

3.3.2 Remote ID (Part 89)

Requires drones to broadcast identity and location. Remote ID provides a mechanism to distinguish compliant drones from unidentified or potentially hostile aircraft. Under FAA Remote ID Rule, the aircraft must broadcast:

- serial number / session ID
- aircraft position
- altitude
- velocity
- control station location

This information has a similar cooperative effect as does ADS-B information broadcast by commercial airlines and general aviation aircraft. The FAA does not want drones broadcasting ADS-B Out because it can overload the surveillance system. Relevant rule:14 CFR §91.225. Instead, the FAA encourages ADS-B IN for traffic awareness. Interceptor systems use ADS-B data and Remote ID data to improve safety.

3.3.3 Part 108 (Pending)

Enables Beyond Visual Line of Sight (BVLOS) operations under performance-based standards. This rule is expected to become law in 2026, significantly expanding the number of drones in the United States airspace and subsequent innovations of technology.

The Part 108 requires utilities and infrastructure owners using drones, BVLOS, or security drones such as the Fortem DroneHunter to have an airspace awareness system in place, most often powered by radar for security purposes. This system is key for safe operations.

The rule also requires:

- Redundant power and control
- Redundant command and control (C2) links to BVLOS drones and lost link procedures, such as linger in place, land, etc.
- Ground risk mitigation, such as parachutes
- Deconfliction capabilities such as geo cages, altitude limits, and other safety features.
- Demonstration of wind tolerance, precipitation tolerance, and icing limitations
- Cybersecurity standards such as:
  - AES-256 encryption
  - Certified to the US Government that we are NIST SP 800-171 compliant, meeting U.S. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting.”
  - End-to-end encryption through SSL.
  - TLS certificates.
  - Passwords are encrypted, and access controls are used to differentiate authority on the system.
  - JSON Web Tokens (JWTs) are used for all API and direct access to the system, and these tokens expire frequently every hour.
  - Upgrade processes are protected using PGP encryption.
  - Software builds are run against NESSUS Scans to validate OS and Application-level protection against viruses and third-party vulnerabilities.
  - Detect and avoid (DAA) radar data feeds are hardwired into customer network(s)
  - Emitted radar signals have an extremely specific center frequency, pulse rate (PRF), and bandwidth. It would be nearly impossible to “inject” false tracks.
  - Jamming the radar on its specific frequency and over the entire bandwidth exceedingly difficult.

4.0 What can Energy Producers and Utilities do Today to Stop Dangerous Drones

Federal laws restrict private mitigation actions. As a result, utilities cannot independently Jam, Spoof, Capture, or Destroy drones. Mitigation must be conducted by authorized federal or trained State and local law enforcement (SLTT) entities. It is currently illegal (March 2026) for any private security team that is not a trained SLTT or any Federal agency not named above to mitigate a drone. This is because of the freedom for Americans to fly. Vast areas of the country are unrestricted airspace. This means that despite the observable potential national security threat from drones, the offenders flying the drones may not technically be breaking any U.S. law. There is just not any common air picture for drones that exists today, like there is for commercial or general aviation aircraft.

Therefore, the most viable regulatory pathway would be a combination of three options.

4.1 Option A

1. Utility deploys Detection, Tracking, and Identification system (DTI) and the Fortem DroneHunter on site with all Part 107 and Part 108 safety measures.
2. Detection, Tracking, and Identification alerts Federal or SLTT partner in real-time
3. Authorized Federal or SLTT use of Fortem DroneHunter
4. The solution used at the World Cup is the same proposed by Southern States LLC, but includes integrations and operational capabilities suited to long-term fixed-site security deployments and security system integrations.

AND / OR

4.2 Option B

Deploy DroneHunter under a federal pilot program with SLTT, DHS, or DOJ oversight.

AND / OR

4.3 Option C

Interceptor drone systems, such as the Fortem DroneHunter, enable a graduated response model that aligns with current regulatory constraints. In a “pursuit and observation” mode, an interceptor may:

- Track a non-cooperative drone at a safe stand-off distance
- Provide real-time video and telemetry to a Security Operations Center
- Enable threat assessment and escalation decisions
- Operate within current FAA Part 107 rules or applicable waivers (and future Part 108 frameworks)

In this configuration, the interceptor is not performing mitigation but rather enhancing situational awareness and supporting lawful response decisions, including coordination with authorized law enforcement partners. This approach provides immediate operational value while remaining compliant with existing federal law.

In limited circumstances, questions arise regarding whether a property owner or security provider may act to protect persons or property from an imminent drone-related threat. While federal law generally preempts unauthorized interference with aircraft, courts and legal scholarship have begun to explore the intersection of drone activity with:

- Reasonable expectation of privacy
- Trespass and nuisance doctrines
- Self-defense and protection of property principles

Several notable cases and legal developments illustrate this evolving landscape, for example: in *Boggs v. Merideth* (Kentucky, 2017), a property owner shot down a drone he claimed was surveilling individuals on his property. While criminal charges were dismissed, the civil case highlighted unresolved tensions between airspace rights and privacy expectations. Legal commentary and state-level statutes increasingly recognize that low-altitude drone operations over private property, particularly when invasive, may implicate privacy and nuisance concerns, though clear federal precedent remains limited.

It is important to emphasize that there is no broad legal authorization today for private entities to unilaterally disable or destroy drones. However, the legal environment continues to evolve, particularly where credible threats to safety, privacy, or critical infrastructure exist. In all cases, actions taken outside established federal authorities carry legal risk and should be carefully evaluated in coordination with legal counsel and law enforcement partners.

5.0 Approach – Layered Detection, Tracking, and Identification (DTI) Architecture

Effective protection requires a layered, multi-sensor approach.

5.1 Radar Sensors

Radar provides the foundational counter-drone sensor:

- Radar remains the most reliable technology for detecting small drones at long range. Examples include FMCW counter-UAS radar systems capable of:
  - detecting drones several kilometers away
  - tracking multiple objects simultaneously
  - operating in all weather conditions
- Radar provides the earliest possible detection of airborne threats.
- Tracking of RF-silent drones
- High accuracy for camera and mitigation cueing.
- Radar systems are inherently resistant to spoofing due to waveform characteristics, while layered architecture provides resilience against disruption.
- Creation of 3D volumetric airspace zones, when entered by a classified drone, trigger escalations, with some zones forbidding even whitelisted drones.
- Remote Id antenna to feed C2 and align with radar tracks.

5.2 EO/IR Camera Sensors

Cameras vary in price due to range, zoom, slew-and-cue speed, etc. They provide:

- Visual confirmation of drone, threat level
  - Classification, distinguishing birds from drones, etc.
  - Payload assessment
  - Key is the integration between the EO/IR and Radar in a distributed and modular command and control systems, easily integrated with existing other security systems.
  - Slew and cue speed and zoom capability. Radar sees a broad airspace simultaneously with a field of view of 360 degrees, where cameras see a very narrow 1–2-degree field of view. Radar systems can slew and cue a camera and control the zoom to keep a fast-moving drone on frame for inspection, classification, and escalation decision-making.

5.3 RF Detection, Remote ID, and Whitelisting

RF systems – such as those provided by partners like SkySafe – enable:

- Identification of compliant drones via Remote ID
- Detection of known signal signatures to give the make and model of drones that are cooperative.
- Approximate operator location

Remote ID enhances identification and reduces false positives. Authorized drones can be identified and whitelisted through Remote ID and Integration with utility drone lists.

6.0 Approach – Interceptor Drone Mitigation Systems and Regulatory Considerations

6.1 Legal Reality

Mitigation technologies, including interceptor drones, are restricted to authorized operators.

Counter-UAS Equipment and Technology Controls

Under federal law, mitigation systems must be on the DHS and DOJ approved list of counter-UAS systems that can be deployed. Approval takes multiple years and requires coordination with:

- Federal Aviation Administration (airspace safety)
- Federal Communications Commission (spectrum)
- National Telecommunications and Information Administration (federal spectrum)
- Federal Bureau of Investigation (training)

Systems are evaluated for:

- spectrum interference
- aviation safety
- cybersecurity risks
- counterintelligence risks

Any mitigation system must meet these requirements in the United States.

6.2 Interceptor Drone Operations

A typical model includes:

- Deployment at critical infrastructure sites
- Remote operation from centralized control by authorized operators
- Physical capture of hostile drones
- Recovery for forensic analysis

The time is now to ready mitigation systems with FAA Part 108 in 2026. While detection is critical, the ability to safely remove hostile drones from protected airspace is also essential. Net-capture interceptor drones, which physically capture hostile drones and safely remove them from the airspace, are now being deployed at military bases and the World Cup in the United States.

6.2.1 Local or Remote Control

Interceptor systems can be positioned at critical infrastructure sites and deployed when a drone threat is confirmed. Operations may be conducted either locally at the site or remotely through a security operations center.

In either approach, both can be coordinated with trained law enforcement operators. The interceptor systems are valuable because they also return captured drones for forensic investigation.

6.2.2 Technical Readiness for FAA Part 108

The FAA is expected to introduce Part 108, enabling expanded BVLOS operations. Interceptor platforms developed for counter-UAS missions are being engineered to comply with anticipated Part 108 requirements, including:

- Remote ID broadcasting
- Anti-collision lights
- Geofencing and flight envelope protections
- Encrypted command-and-control links
- Detect-and-avoid operation

Additional capabilities – such as redundant communications links, strategic airspace deconfliction, and integration with Unmanned Traffic Management (UTM) networks – are expected to further strengthen compliance with future FAA performance standards.

7.0 Summary – Overall Operational Model

The security professionals for each utility will need to create roles, responsibilities, processes, and procedures to mitigate this new threat. These resources will also be key points of contact with federal, state, and local law enforcement to operate a practical security model, which includes:

1. **Deployment of Detection, Tracking, and Identification Systems**
   Radar, EO/IR, and RF sensors deployed at critical sites
2. **Centralized Monitoring**
   Integration of multiple sites into a unified airspace picture
3. **Threat Identification**
   Sensor fusion combining radar, EO/IR, and RF (including SkySafe inputs when a rogue drone is emitting)
4. **Escalation and Coordination**
   Automated alerts to authorized law enforcement partners
5. **Mitigation Execution**
   Get the mitigation assets in place now. Operate legally with Pursue-only functions or in coordination with authorized local, state, or federal partners at centralized locations

This architecture enables utilities to establish a persistent airspace security posture while remaining fully compliant with current regulations.

8.0 Call to Action

It is hard to remember a world without metal detectors at airports. The truth is, it was exceedingly difficult for a metal detector company to sell their product before the events of 9/11 in 2001.

Similar events with drones have already happened in the world.

In 2026, the United States needs this counter-drone assets put in place throughout the country, as our Golden Dome does not cover lower altitude airspace and threats from within the country. The world has changed, and security is now required above the fence line for key sites. It is imperative that energy companies work in partnership with government regulatory teams (like utilities with NERC and FERC) to work in a virtuous cycle of deployment, learning, and adapting to these threats in a future proof evolution of technology and safe kinetic defeat capability.

The trends and threats are such that NATF needs to expand their relationship and coordination activities with federal, state, and local law enforcement as it relates to the protection of the energy producing sites and the national electric grid. Utilities can act today by deploying detection, tracking, and identification systems, with mitigation systems also in place for use under current regulations. The key is to put these mitigation assets in place now as the threat profile increases. It is important to continue to expand coordination pathways with SLTT and Federal authorities as your situation demands.

There are many trends that support this call to action, including:

- Increasing drone threats to infrastructure
- Expansion of federal and SLTT authorities for mitigation with technologies available today that are future proof and usable under current regulations.
- Expanding mitigation authorities
- Advancements in detection, tracking, and identification technologies
- Emerging BVLOS regulatory frameworks require investment that can serve a dual use for safety and security above the fence line.

CONCLUSION

Energy infrastructure and the electric grid are foundational to national security.

Drone threats represent a rapidly evolving risk that requires a coordinated, technology-enabled response. Regulatory frameworks – while complex – are increasingly supportive of infrastructure protection.

Utilities can take meaningful action today by deploying detection systems, integrating layered sensor architectures, and establishing coordination with authorized mitigation partners.

NATF and its members are well positioned to lead the adoption of airspace security as a core component of infrastructure protection to get these assets in place around our country.

The time to act is now.

Powers the Future™

24/7 emergency support line: (770) 946-4565

SouthernStatesLLC.com

30 Georgia Avenue | Hampton, GA 30228

phone (770) 946-4562

fax (770) 946-8106

Sales@SouthernStatesLLC.com