TLP CLEAR – DISSEMINATION UNLIMITED

In Obscura

Vincent M. Nasti, Founder, Chief Executive Officer, Consultant
In Obscura, LLC | Threat Intelligence | Security Countermeasures | Investigations
https://inobscura.org/

(TLP-C) (RECOVERED) THEFT OF CROP DRONES, NEW JERSEY, MARCH 2026, FBI INVESTIGATING 25 APR 2026

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED

IN OBSCURA THEAT LEVEL – IMMINENT

CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED UNCLASIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND ACTIONS DEEMED APPROPRIATE.

UPDATED 27 APR 2026 RECOVERED

Stolen Chemical-Spraying Drones Located in North Jersey Warehouse, Shore News Network, April 27, 2026
https://www.shorenewsnetwork.com/stolen-chemical-spraying-drones-located-in-north-jersey-warehouse/#google_vignette

Dover, NJ — Fifteen high-capacity agricultural drones stolen in a coordinated New Jersey heist earlier this month have been recovered at a warehouse in Dover, easing fears that the equipment could be misused to disperse dangerous materials. The drones were originally taken from Harrison, about 30 miles away, prompting a multi-agency investigation that included the FBI.

The drones, designed for precision crop spraying using GPS-guided routes, can disperse large volumes of liquid over targeted areas—capabilities that raised alarm among security experts after the theft.

EXECUTIVE SUMMARY

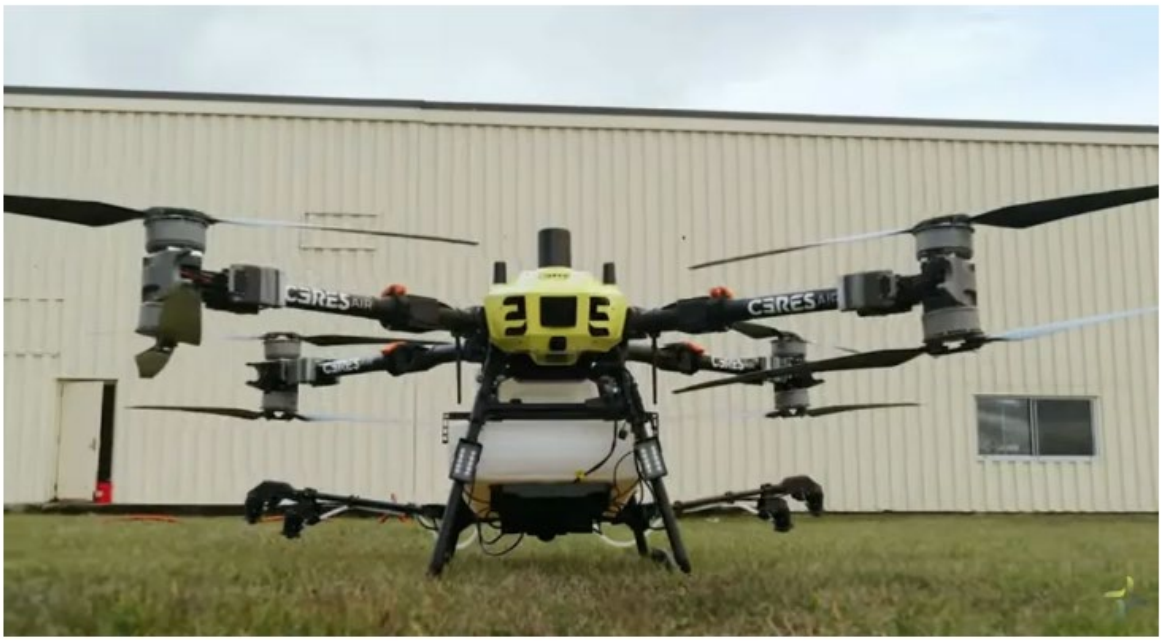
The following open-source reporting is forwarded for threat awareness, but more specifically the brief but revealing information concerning target identification, planning and tradecraft leading to the very successful the of these drones. I am not at all pleased with the author's release of description of the cameras present at the facility and the apparently brilliant counterfeiting of the tractor trailer. This was indeed a very sophisticated organization behind this theft, and probably a host of intelligence and targeting operations. I will not provide further details, out of operational security concerns of this investigation and my non-disclosure agreements. My motive here is educate and inform the Christian Community of very real danger to our church and country. My review of this reporting contains my tallow highlighting.

FBI 'spooked' by sophisticated theft of agricultural drones in New Jersey

The crop sprayers could be extremely dangerous in terrorist hands

JACK MURPHY AND SEAN D. NAYLOR
APR 22, 2026 · PAID

41 1 12 Share



Source: "Ceres Air C31 Payload Test" on YouTube

FBI 'spooked' by sophisticated theft of agricultural drones in New Jersey

15 chemical spraying drones stolen in NJ | The crop sprayers could be extremely dangerous in terrorist hands, Jack Murphy and Sean D. Naylor, Apr 22, 2026

The High Side, Substack https://thehighside.substack.com/p/fbi-spooked-by-sophisticated-theft

The sophisticated theft of 15 crop-spraying drones last month in New Jersey has the FBI worried as experts warn of "ridiculously bad" consequences and "a potential nightmare scenario" if terrorists get their hands on the machines.

The unsolved theft has revived fears rampant in the post-9/11 years that terrorists might use crop dusters to disperse biological or chemical weapons with the aim of inflicting mass casualties inside the United States. The difference now is that the potential threat consists not of one pilot flying a small propellor-driven plane, but more than a dozen remotely piloted vehicles. Heightening the concern even further is the fact that the crime occurred against the backdrop of the United States' war against Iran.

"The bureau is freaked out for a good reason," Steve Lazarus, a retired FBI agent, told The High Side in an email. "These aren't hobby drones with cameras. They're industrial sprayers designed to carry and disperse significant amounts of liquid quickly and with precision. A typical agricultural drone can cover a large area in minutes, following GPS-guided paths — that's exactly what they're built for in farming, but it also means that, in the wrong hands, they're a ready-made delivery system."

March 24 appeared to be a day like any other at a Harrison, New Jersey, shipping and logistics company called CAC International. A truck showed up to pick up 15 Ceres Air C31 agricultural drones, presenting a bill of lading that CAC International believed it had confirmed via email. After the drones were loaded on his vehicle, the driver took off with them.

Later that day, Ceres Air called the shipping company and law enforcement in a panic. The drones had been picked up by an impostor pretending to be the delivery man for the rightful buyer, according to an unclassified law enforcement report provided to The High Side. The potential implications were immediately clear: The C31 drone sells for about $58,000 and can aerosolize and spray 31 gallons across more than 15 acres in 7 minutes and 40 seconds.

By flying the drones at low altitude over a crowded area while spraying "any number" of toxic substances, especially neurotoxins, "you could do a tremendous amount of damage,"

a former senior government scientist familiar with similar threats told The High Side. “The potential absolutely could be ridiculously bad.”

The FBI team put on the case has been very tight-lipped, working out of the Newark, New Jersey, field office with support from tech specialists at FBI headquarters in Washington D.C., according to a person familiar with the investigation who described the theft as “spooky.” The bill of lading turned out to be counterfeit, and as the FBI dug deeper it only got worse.

At the warehouse there was clear video footage of the truck that picked up the drones, but the Department of Transportation numbers on the side of the vehicle were copied from another, and the license plates were also a dead end, likely stolen, according to the person familiar with the investigation. Likewise, the driver’s commercial driver’s license, of which CAC International retained a copy, appears to have been stolen or illegally modified, as the picture on it does not appear to match video footage of the actual driver at the warehouse. License plate readers and traffic cameras in the area also came up empty, implying that the truck was dumped somewhere nearby and the drones transferred to a different vehicle. “This method of theft is a first,” said the person familiar with the investigation. “It almost always happens after the buyer takes delivery and custody.”

The FBI scrutinized Ceres Air but as of this writing does not suspect an inside job. However, bureau officials are taking a hard look at the legitimate purchaser of the drones, as they suspect that someone had to tip off the thieves that the drones were waiting for pickup, according to the person familiar with the investigation. The High Side has not been able to determine the identity of the buyer. A small element from the Bureau of Alcohol, Tobacco, Firearms and Explosives has also joined the investigation, mostly to monitor fertilizer sales, due to the FBI’s concern that an explosive payload could be loaded into the drones in addition to the potential for a toxic spray, according to a person familiar with the investigation.

Neither the FBI nor Ceres Air, CAC International Worldwide Express and Teleport Logistics responded to The High Side’s requests for comment. (Worldwide Express held the contract to transport the drones, which it subcontracted to Teleport Logistics.)

"This was one of the most highly sophisticated thefts [the FBI] have seen in a long time, which is the main thing that has them so spooked," said a person who has been briefed on the case. But beyond the sophistication of the heist, the feds are also worried by the fact that there is neither a legal resale market nor a black market for such drones, begging the question of why someone would go to such trouble to steal them, according to the person who has been briefed on the case.

A terrorist group wouldn't need to spray "anything exotic" to create real problems with the drones, said Lazarus. "Even common chemicals, used improperly, can be a public safety danger. Throw in the internet recipes for biological and chemical weapons that anyone with a Tor browser has access to, and this is a potential nightmare scenario.

"What makes the thefts concerning isn't just the equipment itself, it's how easy they are to use once someone has them," Lazarus continued. "Keep in mind these are deployed by farmers, not rocket scientists or even aviation professionals. They're battery-powered, portable, and don't require much setup—basically plug-and-play. They can be launched from just about anywhere, complete their job quickly, and be gone before anyone realizes what happened."

While the investigation continues, the FBI hopes that its technical experts will be able to detect when and if the drones are powered up and activated, and if so, they hope to be able to shut them down remotely before they could be used for any nefarious purposes, according to two individuals familiar with the case.

The possibility that 15 crop-spraying drones might be in the hands of Iranian proxies or other terrorists echoes the fears that gripped the national security community in the wake of the 9/11 attacks: that such actors would use crop-spraying aircraft as weapons to spread biological or chemical weapons. "Post-9/11, this was a really, really major area of focus for a lot of people," said the former senior U.S. government scientist familiar with similar threats, adding that back then the concern was more over manned aircraft. "There wasn't that much conversation" about the drone threat, the scientist said.

U.S. government experts modeled the crop-duster threat until it became something that they were "really, really well versed in," the scientist said. "We got really good at this."

However, much of that expertise has now left the government, according to the scientist. "While there are people who still do that, a lot of them have left," resulting in "an erosion of understanding" of the threat since about 2010, the scientist said. "Of the 20 best people [then] ... in government, I can only think of a couple who are left," the former senior government scientist said. **"Who is melding the past with the present on this?"**

However, the former senior government scientist noted that the New Jersey drone heist occurred in the context of a massive increase nationwide in transshipment thefts. According to Republican Sen. Deb Fischer of Nebraska, between 2021 and 2025 cargo theft increased 1,500 percent. "A lot of what's happening is people show up looking completely legit" and then take off with a vehicle loaded with goods, the former senior government scientist said. "They are very sophisticated." The drone theft appears to fit within that pattern.

"There are rational explanations" for the drone theft that do not involve terrorists, the scientist said. For instance, it might have been conducted by a group looking to use or sell the drones abroad. "It is possible to get stuff like that out of the country," the scientist said. However, the former senior government scientist said, the FBI was right to be worried. "Should they be spooked? Yeah," the scientist said, adding that in the hands of terrorists, the drones could "absolutely" pose a very serious threat. "If [current government] people are worth their salt ... they're modeling this thing to death, quietly."

///END///

TLP CLEAR – DISSEMINATION UNLIMITED

==========

IN OBSCURA HAS ADOPTED THE OSINT CLASSIFICATION SYSTEM OF DEPARTMENT OF HOMELAND SECURITY CLASSIFICATIONS 'TRAFFIC LIGHT PROTOCOL' RELEASE CAVEATS. THESE REGULATE IN OBSCURA REQUIREMENTS FOR PUBLIC RELEASE TO PROTECT CLIENTS AND IN OBSCURA SOURCES, METHODS, AND TECHNQIUES. IN OBSCURA RELEASE PROHIBITION MARKINGS ALSO APPLY. NONE ARE RELEASABLE TO NEWS MEDIA OR JOURNALISTS WITHOUT WRITTEN REQUEST AND PERMISSION.

==========

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN-OBSCURA PRODUCTS OR INFORMATION. TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION FOLLOW...

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
TLP: GREEN Limited disclosure, recipients can spread this within their community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP: CLEAR Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

TLP CLEAR – IN OBSCURA CAVEATS APPLY