



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



FOOD & AGRICULTURAL SECTOR

23 October 2020

LIR 201023-007

Threat Actors Very Likely Surreptitiously Surveil and Release Information on Farms and Livestock Processing Plants, Increasing the Risk of Violence against Agricultural Facilities in the Near Term

The FBI Weapons of Mass Destruction Directorate, in coordination with the Counterterrorism Division and Office of Private Sector (OPS), prepared this LIR to alert security personnel at farms, livestock processing facilities, and animal agriculture industry groups of the potential for threat actors to surreptitiously install wireless cameras at agricultural facilities. This emerging tactic is intended to illicitly document the internal activities of the victim facility. Key indicators of such threat activity and actionable recommendations for mitigation are provided for the benefit of our private sector partners.

Threat Actors Seek to Surreptitiously Surveil Agricultural Facilities

In 2020, threat actors employed the new tactic of installing wireless cameras at farms and other livestock processing plants to surreptitiously surveil and document the internal actions of targeted locations. The use of wireless cameras is more reliable and less attributable than body camera or cellular phone footage, which can diminish law enforcement response to threat actors' surveillance actions.

- On 28 September 2020, animal rights activists staged a protest outside of a meat processing plant and trespassed on the facility's property. Upon accessing the facility, the activists retrieved a hidden camera previously installed near a slaughter line and captured nearly 81 hours of footage.
- On 29 May 2020, individuals affiliated with an animal rights group illicitly recorded and released footage of a farm euthanizing animals through a depopulation management method called ventilation shutdown.^a The footage depicted the euthanizing of a large group of pigs and was captured with a hidden wireless camera installed by an employee at the farm.

Release of Information Increases the Risk of Criminal and Violent Activities against Agricultural Facilities^b

Threat actors surreptitiously surveil and release information about agricultural facilities to potentially mobilize others for criminal or violent activity against agricultural facilities. Initiatives to publicly release

^a According to the American Association of Swine Practitioners, ventilation shutdown is an approved, although least desirable, depopulation method that includes "closing up facility openings, shutting inlets, and turning off ventilation fans."

^b The FBI does not initiate investigations based on activities like viewing or publishing publicly available content to online platforms, as these activities are protected by the first amendment. Evidence of an individual or group partaking in criminal or violent activities must be present for the FBI to initiate any investigative procedures.



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



information regarding farm locations have resulted in increased criminal and violent acts against some of the identified facilities.

- In late May 2020, animal rights activists published an online interactive map “revealing the locations of more than 27,500 farms and animal agriculture facilities, including 5,812 identified using satellite imagery, many of which do not appear in public records.” The facility profiles included the facility’s address and the type of animals.
- In January 2019, after a comprehensive map of 5,832 Australian farms was published, a confrontation took place when an Australian dairy farmer demanded two animal rights activists stop filming his animals.

Potential security risks arise when the locations and non-public information regarding agricultural facilities are compromised online. Historically, criminal activities, such as animal thefts and arsons, have increased following the publication of lists of the locations of prominent agricultural facilities. Threat actors likely will continue to employ tools, such as interactive maps and wireless cameras, which streamline their capabilities to gather information and aid in the targeting and planning of violence against agricultural facilities.

The following observable indicators alone do not determine the mobilization of threat actor activity. Organizations should evaluate the totality of suspicious activity before notifying security and law enforcement personnel.





- Increases in surveillance activities at agricultural facilities
- Increases in attempted or successful trespassing efforts
- Increases in online postings that include agricultural facility photos or videos that appear to be illicitly obtained
- Increases in attempts by suspected threat actors to recruit agriculture employees for video documentation of internal facility activities

The FBI suggests law enforcement and private sector entities remain vigilant of this threat and report persistent attempts by unauthorized individuals to access property, in order to aid the prevention and mitigation of potential extremist activity. The FBI also recommends animal agriculture facilities increase security measures, to include the use of security cameras, and to monitor and report any illicitly obtained videos or images of their facility that may be present online.

This LIR was disseminated from OPS’s Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your [local FBI Field Office](#):
<https://www.fbi.gov/contact-us/field-offices>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.