OFFICE of PRIVATE SECTOR

ACADEMIA ENGAGEMENT REPORT (AER)

CONNECT to PROTECT

ACADEMIA

22 February 2022 **AER 220222007**

Previously "Hardened" Targets at Risk for Hidden Camera Intrusion

References in this Academia product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.

The FBI's Oklahoma City Field Office, in coordination with the FBI's Office of Private Sector (OPS), prepared this Academia Engagement Report to alert partners in education and community centers of emerging technologies which may be exploited to target childcare and youth learning for production of child sexual abuse material (CSAM) using hidden cameras. The FBI is issuing this report based on recent threat indicators in which individuals targeted bathrooms in daycare facilities.

Due to the ever-expanding availability of prefabricated hidden cameras, their minimal cost, and the ease with which non-technologically savvy actors can gain knowledge to install, hide, and fabricate their own cameras, schools, childcare, and youth learning facilities previously considered "hardened" targets, may become vulnerable to exploitation. "Hardened" targets refer to places that have security measures, such as identification requirements, alarms, double-locked doors, and video cameras. These facilities are largely seen as difficult to access, and have security measures in place beyond what is typical of locations accessible to the general public.

In July 2021, the FBI investigated a case in which hidden cameras were widely utilized to produce CSAM. Evidence suggested the offender was targeting a daycare facility. No cameras were found in the facility, but the offender, whose child went to the daycare, was known to consistently use a private bathroom on the daycare campus. Evidence suggested the offender was attempting to modify and/or build cameras to be placed in various items, such as vents, baseboards, and toys.

Potential Threat Indicators: The following indicators, taken singularly may not be indicative of criminal behavior, but should be considered in their totality.

- Requests for accessing private areas of a facility such as bathrooms, locker rooms, or classrooms outside of normal duties/need.
- Abnormally long time spent alone in private areas of facilities.
- Large bags or other concealment devices not consistent with an individual's role or duties in a facility.
- Access by individuals without a need to be at the facility, such as a parent accessing a school locker room for students, or a person with no membership to the facility.
- A smell of burnt plastic or raw wood in an area with previously no abnormal smells. This could indicate someone has altered products in the room or used electrical equipment like a soldering iron.
- Abnormal trash in restrooms such as button batteries, wires, and plastic wrapping.

- Nervous or agitated behavior exhibited by an individual after leaving a private area.
- Previous suspicious behavior, or suspected child abuse, by an individual accessing the facility.

Recommendations for Childcare Facilities, Schools and Youth Centers

Offenders who produce CSAM often obtain access to children through exploiting positions of trust and authority. This is typically referenced when speaking of careers such as teachers or coaches, but offenders can utilize that same brand of trust from other roles to manipulate other adults and environments. The following are some proactive methods to educate staff, parents and children:

- Implement age-appropriate sexual development and safety education for children.
- Train and support staff on identifying signs of sexual exploitation and abuse.
- Trust your intuition and report signs of possible child abuse/alarming behavior immediately.
- Teach age-appropriate body safety and boundaries.
- Avoid letting unauthorized peoples gain access to private facilities such as restrooms. If unavoidable, do not let bags, purses, boxes, etcetera to go with the individual into these areas.
- Be aware of your surroundings, especially in areas where undressing is common, such as locker rooms, bathrooms and changing areas. If there is something new, inspect the device.
- Clean air vents and filters regularly so you know what those areas should look like.
- Educate staff on what small cameras may look like, how to detect them and what to do if they think there is one.

The OPS Information Sharing and Analysis Unit disseminated this AER. Direct any requests and questions to the 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.