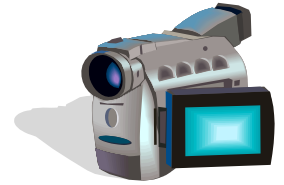


NNEVDV

Video Cameras



How the Technology Works

Video cameras transmit images using either analog or digital technology and can be monitored onsite or remotely. Some cameras are “always on,” while others are motion activated. Some security systems operate on closed circuit TV (CCTV) while others broadcast over the Internet. Some offer “real-time” monitoring without a recording -- such as a camera pointed towards an outside entrance, allowing a receptionist to see who is knocking on the door.

How Are Grantees (Agencies and Partnerships) Using It?

Grantees use video cameras in a variety of ways, including as part of a security system, to document interviews, to capture evidence and to monitor visitation at supervised visitation centers. Sometimes, they’re used as part of medical examinations in cases of rape and domestic violence. Video cameras can be great for web-conferencing between agencies that are geographically distant, communicating with survivors through a video interpreter or video relay, and for virtual protection order hearings before a judge. Agencies might also use cameras for office and parking lot security.

Benefits and Risks

- Cameras can help increase remote access to services, and, document perpetrators violating restraining orders.
- Cameras are vulnerable to interception and perpetrators will go to great lengths to gain access to the victim.
- Wireless analog cameras are easily intercepted from ¼ mile away, and skilled hackers can add antennas that intercept camera feeds from even further. Using antennas to direct the signal, agencies can try to limit how far a wireless camera transmits. Unfortunately, interception is often difficult to detect. Wireless digital cameras that encrypt transmissions and use spread-spectrum technology are designed to be less easily intercepted.
- In general, password protected wired cameras not viewable over the Internet are the most secure. Any camera viewable over the Internet has a higher risk of interception than those viewed solely through a CCTV system or DVR.

Things To Consider

- Have you taken sufficient steps to prevent interception risks? Agencies should maintain the security of any system or computer used to view camera or video feeds. Security steps can include having strong computer and system firewalls, keeping anti-virus and anti-spyware definitions current, encrypting the camera feed/transmission, and, requiring each person to have a unique user name and password for the computer/system and for the camera/video account.
- All passwords should be changed from the factory-set defaults to make cameras more secure. Passwords should be changed often, and at the very minimum, every time there is staff turnover.
- Video camera footage is like any other personally identifiable data collected by agencies. To protect victim privacy and confidentiality, agencies and partnerships should keep video footage only for the shortest time necessary to address victim safety or other security issues. Your agency or partnership policies should address the retention, use and purging of camera images. Policies should address how you will limit access to the images, the camera and any media (memory card, videotape, hard drive) and ensure that they are not lost or stolen. A log should be kept of all instances of access to, and use of, recorded material.
- To ensure upfront notification, signs and information should tell people accessing services that they are being taped or viewed by cameras. Consider where and how many signs must be posted, and what languages should be used.
- Security and privacy are both impacted by whether cameras are actively monitored or the system is passive, simply recording images in case they are later needed. Wording on posted signs should not create a false sense of security or privacy and lead someone to believe that the cameras are being monitored live if they are not.
- Make sure your agency reviews relevant local, state/territorial/tribal and national laws relating to privacy, consent and video/audio recording before purchasing, installing and using cameras to record or view people. The legality of video monitoring and recording may vary by context (workplace, bedroom) and recording type (audio capture).

Video Cameras

Supported by US DOJ-OVW Grant #2007-TA-AX-K012. Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.
© 2009 National Network to End Domestic Violence, Safety Net Project • www.nnedv.org/safetynet • Email: safetynet [at] nnedv.org • Phone: 202-543-5566