CACI

EVER VIGILANT

INFORMATION DEPLOYED.
SOLUTIONS ADVANCED.
MISSIONS ACCOMPLISHED.

Worldwide Headquarters:
1100 N. Glebe Road, Arlington, VA 22201
703-841-7800

Law Enforcement Agencies, Body-Worn Cameras, and the Freedom Of Information Act

Managing the Need For Increased Redaction Capabilities

CACI's Digital Forensics Laboratory (CDFL) is a premier internationally accredited full service computer, mobile device, and audio/video forensics laboratory in Alexandria, VA providing a full range of onsite and offsite digital forensics services for government investigation, litigation, eDiscovery, FOIA, cyber security, and intelligence projects. CDFL received its ISO/IEC 17025 accreditation in computer forensics in April 2014 from the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) International, whose accreditation program provides a means for continuous quality improvement of lab services as well as criteria for assessing and improving the performance of digital forensics operations. This accreditation assures clients that CDFL's management, personnel, equipment, physical facilities, quality system, and operational and technical procedures meet recognized standards of excellence. Personnel certifications include: Certified Electronic Evidence Collection Specialist (CEECS), Certified Forensic Computer Examiner (CFCE), Digital Forensics Certified Practitioner (DFCP), Certified Information Systems Security Professional (CISSP®), et al.

CACI's Digital Forensics Lab in Alexandria, VA, is one of only six private digital forensics laboratories in the world to earn ISO/IEC accreditation from ASCLD/LAB – International.

CACI

EVER VIGILANT

INFORMATION DEPLOYED.
SOLUTIONS ADVANCED.
MISSIONS ACCOMPLISHED.

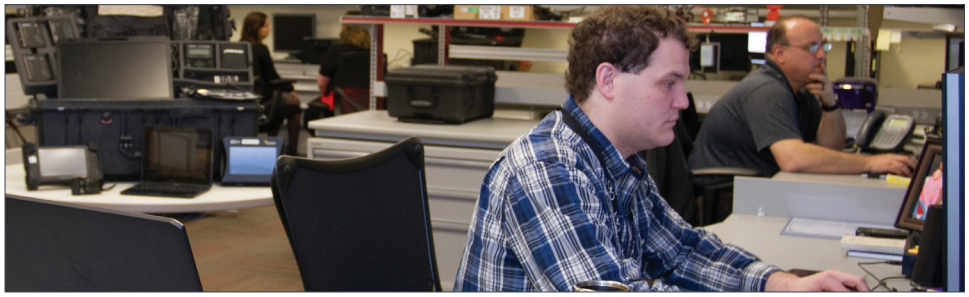
Worldwide Headquarters:
1100 N. Glebe Road, Arlington, VA 22201
703-841-7800

Rapid Growth Of Video In Law Enforcement Demands New Approaches to Managing and Redacting Digital Evidence

Driven by increasing media and public scrutiny of law enforcement activities, today there are an estimated 200,000+ body-worn cameras on the street or in pilot programs. That number is set to potentially double over the next five to seven years and as the number of body-worn cameras grows, so does the content. One agency is considering a deployment that would generate over 30 million hours of video each year.

Much of this content is subject to disclosure under local, state, and federal Freedom of Information Act (FOIA) requests. However, content requested under FOIA must be reviewed and redacted prior to release in order to remove personal identification information (PII), minors, and other subjects who are legally entitled to privacy. Redaction has commonly been handled internally by agencies and their related forensics labs. However, the anticipated volumes and unique requirements in audio/video redaction will necessitate that agencies either hire new employees or outsource this work to third parties.

CACI's Digital Forensics Laboratory (CDFL) is one of only six private digital forensics laboratories in the world to earn ISO/IEC 17025 accreditation from ASCLD/LAB - International. Their experience provides a unique opportunity to discuss the implications of increasing digital evidence management and redaction demands on law enforcement, as well as the qualifications needed in a third-party provider.



CACI's Digital Forensics Lab in Alexandria, VA, offers audio and video redaction as a service capabilities to ensure digital evidence is handled in a secure, reliable, and documented manner.

For more information, contact:

Digital Forensics Laboratory
at **cdfl@caci.com** to discuss their portfolio of digital forensics services currently in use by the DOJ, SEC, FTC, FDIC, and other federal agencies.

CACI

EVER VIGILANT

INFORMATION DEPLOYED.
SOLUTIONS ADVANCED.
MISSIONS ACCOMPLISHED.

Worldwide Headquarters:
1100 N. Glebe Road, Arlington, VA 22201
703-841-7800

Key Items to Consider

How Is Audio and Video Redaction More Complex Than Document Redaction?

In document redaction, text has to be blurred, removed or blacked out on each page in order to safeguard personal identification information or other sensitive content. As video records moving subjects at 30 frames per second, each frame has to be considered separately to ensure that all required content is redacted. At 30 frames per second, a five-minute video represents 9,000 frames.

What Methods Are In Place Today For Audio and Video Redaction?

Today, redacting limited video sources (interrogation rooms, dashboard cams) within agencies can be handled internally by a few full-time employees using commercial video editing software like Sony® Vegas or Adobe Premiere. Now, agencies are deploying dozens (if not hundreds or thousands) of body-worn cameras, and the volume and complexity of redaction is increasing proportionally. This does not include additional video sources, such as unmanned drones, that can be expected in the near future. Increasing volume requires increasing head count which is often a challenge in budget-constrained departments. There are also perception issues over allowing agencies to use sophisticated video editing tools like Adobe Premiere in-house to handle redaction of content relating to the conduct of their own officers. Concerns can be raised over what exactly was altered in a video before it was shared with the public.

What About the Automated Redaction Capabilities Now Offered In Several BWC Systems?

While an improvement over strictly manual redaction processes, these tools still require significant additional time-on-task for the officer or department employee. The video content still requires initial review, redaction, frame-by-frame review of content for quality control, manual corrections where the automated tool will have fallen short, and completion of related paperwork.

What Are Legal Or Regulatory Considerations Influencing Approaches to Redaction?

Two key ones are deadlines related to Freedom of Information Act requests and compliance with the Criminal Justice Information Systems (CJIS) Security Policy. To the first, different jurisdictions establish different deadlines by which FOIA-related requests have to be satisfied. As an example, the Washington DC Council passed regulations in 2015 that state a FOIA request for body-worn camera footage must be satisfied or rejected within 25 business days (along with a 10 business-day extension available if needed). These deadlines mean that requests cannot be indefinitely backlogged to meet employee availability.

The second is compliance with the Criminal Justice Information Systems (CJIS) Security Policy. CJIS is explicit in how evidence must be secured, controlled, handled, disseminated and destroyed, as well as the requirements around personal privacy protection. Law enforcement agencies will be expected to maintain clear chain-of-custody and evidentiary processes as they manage video evidence and redaction. This may require additional training for officers as well as establishing detailed and documented workflow, review, and quality control processes beyond what is already in place.

For more information, contact:

Digital Forensics Laboratory
at **cdfl@caci.com** to discuss their portfolio of digital forensics services currently in use by the DOJ, SEC, FTC, FDIC, and other federal agencies.

CACI

EVER VIGILANT

INFORMATION DEPLOYED.
SOLUTIONS ADVANCED.
MISSIONS ACCOMPLISHED.

Worldwide Headquarters:
1100 N. Glebe Road, Arlington, VA 22201
703-841-7800

Do All States Have Freedom Of Information Act Requirements?

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, makes almost every record possessed by a federal agency disclosable to the public unless specifically exempted or excluded. All states have some form of laws allowing the public to obtain documents and other public records from state and local governments. While not always identical to the federal statutes, state courts have held that federal judicial interpretations of FOIA are helpful in interpreting similar state public record laws.

Could State Legislation Exempting Body-Worn Camera Video From FOIA Requests Eliminate the Concerns Around Needing Redaction Resources?

Legislation exempting this content may not always succeed should the courts find that it limits public access rights without significant cause. Additionally, redaction will still be needed for some audio/video content shared with lawyers, investigators, and the courts. Should unredacted content showing individuals with a constitutional right to privacy somehow make its way into the public eye, departments could face significant legal action. Agencies should plan to have some form of scalable redaction capabilities in place so they can meet all eventualities.

What Is the Value Of Considering a Third-Party Provider For Redaction Services?

A vendor providing "redaction as a service" is going to offer law enforcement agencies several advantages:

- **Scalability:** FOIA demand is not likely to be consistent, but agencies would be required to staff for peak anticipated demand. Using on-demand resources would reduce overall agency costs significantly.
- **Consistency:** Vendors will have trained personnel just focusing on redaction while officers may have multiple priorities. An officer that is not frequently engaged in redaction may be more prone to errors or require re-training.
- **Transparency:** In the handling of sensitive content such as incidents that are highlighted in the media, a third-party vendor may be perceived as more independent than an agency employee.
- **Efficiency:** Vendors will not be subject to changing agency priorities or re-tasking, ensuring that established deadlines are met consistently.
- **Cost Control:** Utilization of a predictable "pay only for what you redact" model provides agencies the ability to redeploy staff to more direct tasks or avoid/eliminate unnecessary FTEs and the costs associated with infrastructure and facilities.

CACI's Digital Forensics Lab offers "redaction as a service" capabilities to help customers meet the need for increased redaction services stemming from body-worn cameras and Freedom of Information Act requests.

For more information, contact:

Digital Forensics Laboratory at **cdfl@caci.com** to discuss their portfolio of digital forensics services currently in use by the DOJ, SEC, FTC, FDIC, and other federal agencies.

CACI

EVER VIGILANT

INFORMATION DEPLOYED.
SOLUTIONS ADVANCED.
MISSIONS ACCOMPLISHED.

Worldwide Headquarters:
1100 N. Glebe Road, Arlington, VA 22201
703-841-7800

What Should Agencies Look For In a Vendor Offering Redaction Services?

Agencies should strongly consider a number of items when selecting a vendor for redaction services:

- **CJIS-Compliance:** CJIS is explicit in stating "Private contractors who perform criminal justice and non-criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function…" Vendors should be able to demonstrate appropriate facility and software security, documented evidence management and chain-of-custody procedures, and provide fully screened and cleared personnel.

- **Secure Online Transfer:** Secure portals allow agencies to efficiently provide and receive content. If physical media is required, clear handling procedures should be documented.

- **Customizable Workflows:** Vendors should be able to demonstrate a clear understanding of local or state FOIA requirements and design workflows that fully conform to those requirements. These could include how FOIA requests are submitted and evaluated, the handoff between agency and vendor, final acceptance and release criteria, etc.

- **Clear Documentation:** Along with the redacted content, vendors should provide a chain-of-custody report, detailed notes regarding what was redacted and where, and destruction dates for when the content will be removed from the vendor's system in compliance with local/state/federal regulations.

- **Fixed and/or Tiered Fee Structures:** the Freedom of Information Act, along with many state and local regulations, allow agencies to charge reasonable fees to recapture the costs of meeting FOIA requests. Vendors should have established pricing based on video length and redaction complexity that allow agencies to clearly understand what the cost will be per request and whether they can recoup most or all of that through a fee structure.

Whether considering a vendor to manage all redaction requirements, or to simply handle requests in an on-demand model, law enforcement agencies should be confident that their digital evidence is being handled in a secure, reliable, and documented manner that will withstand scrutiny by media, public, and regulatory review.

For more information, contact:

Digital Forensics Laboratory
at **cdfl@caci.com** to discuss their portfolio of digital forensics services currently in use by the DOJ, SEC, FTC, FDIC, and other federal agencies.