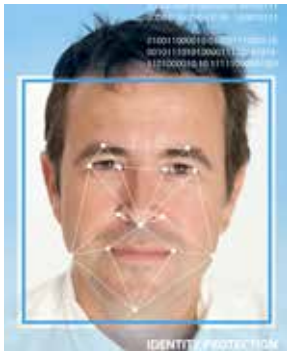
Bureau of Justice Assistance
U.S. Department of Justice

Global Justice Information Sharing Initiative

Video Evidence

A Law Enforcement Guide to Resources and Best Practices

With the rapid growth and improvements in video technology used in government, business, and personal applications, law enforcement leaders are recognizing the importance of improving their agencies' capabilities of utilizing that video evidence to solve crimes. Despite the growing availability of video evidence, many state and local law enforcement agencies have indicated that gathering and analyzing video information can be very difficult. Video evidence can come from a multitude of different devices, with differing systems, formats, players, and technology, yet an agency's ability to properly secure, catalog, store, and maintain its evidentiary value and integrity is critical to a professional police organization. Clearly, guidance and best practices are needed to improve public safety agencies' ability to appropriately utilize and manage video data.

The purpose of this resource is to provide answers to straightforward common questions that law enforcement officers, or the agencies they represent, may have regarding properly securing, collecting, storing, and analyzing video by directing them to valuable tools and resources from experts in the field.

Background

Many state, local, and tribal law enforcement agencies across the United States are not in a position to be able to fund, create, and maintain a specialized video forensics unit. Yet there are a number of larger law enforcement agencies, as well as federal and nonfederal agencies, that have such capabilities and are trained to respond to major threats and incidents (bombings, mass-casualty events, school shootings, etc.). They have the expertise that allows them to secure and analyze videos from multiple sources, which greatly improves the ability to investigate a crime and identify the suspect/suspects.

One such agency is the Federal Bureau of Investigation, which has many subcomponents devoted to this mission, including the Forensic Audio and Video Image Analyst Unit, the Scientific Working Group for Image Technology (SWGIT), the Digital Imaging and Video Recovery Team (DIVRT) initiative, and the Regional Computer Forensics Laboratory (RCFL). Others include the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), the National Forensic Science Technology Center, the Law Enforcement and Emergency Services Video Association (LEVA), Target Corporation, Inc.'s Forensic Analysis Unit, Internet Crimes Against Children (ICAC), and the International Association for Identification. These agencies are not only some of the nation's "go-to" sources for the quick retrieval and analysis of time-sensitive video, they are also the developers and providers of valuable best practices, guides, DVDs, training, and certification for educating the law enforcement field.

All law enforcement agencies, regardless of size, can utilize these best practices and resources to improve their ability and capability when it comes to video evidence, not just in a major incident, but also in their daily efforts to solve crime and protect the citizens they serve.

This document was a collaborative effort of representation from these entities through the Global Justice Information Sharing Initiative (Global), which is supported by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Global acknowledges that this document does not address all subject areas of this complex topic. Global is committed to helping justice agencies more readily and appropriately utilize video data and plans to develop additional video resources for justice and public safety communities.

Frequently Asked Questions

What tools would help me with video retrieval in the field?

a. Crime scene investigations

- ***Crime Scene Investigation: A Guide for Law Enforcement***, National Forensic Science Technology Center, with support from the Bureau of Justice Assistance (BJA), the National Institute of Standards and Technology (NIST), and the National Institute of Justice (NIJ), September 2013. This is a procedural guide for the complete range of crime scene investigation tasks, from securing the scene to submitting evidence. The publication provides law enforcement professionals and first responders with step-by-step guidance in this crucial first phase of the justice process. Contents include Arriving at the Scene—Initial Response/Prioritization of Efforts; Preliminary Documentation and Evaluation of the Scene; Processing the Scene; Completing and Recording the Crime Scene Investigation; Crime Scene Equipment, etc. This guide is available at www.nfstc.org/?dl_id=287.

- ***Digital Evidence Field Guide—What Every Peace Officer Must Know***, FBI RCFL Continuing Education Series. This field guide was designed to help law enforcement in properly handling and transporting digital evidence. Topics include five key facts about digital evidence, criminal uses of digital evidence, identifying digital evidence, legal considerations, executing the digital search warrant, packaging and transporting digital evidence, definitions, and more. This product is available only to law enforcement and government personnel and may be ordered at: http://www.rcfl.gov/DSP_N_orderDocs.cfm.

b. Retrieving video from CCTV systems

- ***Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems***, Version 1.0, joint project among the FBI's Operational Technology Division, Digital Evidence Section, Forensic Audio, Video, and Image Analysis Unit in conjunction with the Technical Support Working Group (TSWG) and the National Terrorism Preparedness Institute at St. Petersburg College, 2006. The purpose of this guide is to provide the best methods for the retrieval of video data evidence from digital closed circuit television (DCCTV) recording systems and to aid in the development of standard operating procedures (SOP). This guide provides responding law enforcement officers with guidance in securing and collecting video data from DCCTV systems, ensuring that best methods are utilized to retrieve the recorded data and maintain integrity. Topics covered: DCCTV, scene arrival, assessing the system, output options, non-native data retrieval, evidence handling, leaving the scene, legal issues, equipment needed, and more. http://www.cttso.gov/sites/default/files/DCCTV-PocketGuide-v1-final.pdf.

- ***Best Practices for the Retrieval of Digital Video***, Section 24, Version 1.0, FBI's SWGIT, September 27, 2013. The purpose of this document is to provide the best methods for the retrieval of video/audio data evidence and any associated metadata (referred to in this document as data) from digital closed circuit television (DCCTV) recording systems. These best practices, guidelines, and recommendations are intended to provide responding law enforcement personnel with guidance in securing and collecting data from DCCTV systems. This will ensure that best methods are utilized to retrieve the recorded data and maintain its integrity. These guidelines are meant to inform agencies of the best practices for DCCTV retrieval and to aid in the development of SOPs. These practices should be used in conjunction with current agency policies. This document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***Best Practices for the Analysis of Digital Video Recorders***, Section 23, Version 1.0, FBI's SWGIT, June 11, 2012. The objective of this document is to provide guidance regarding appropriate practices in the retrieval of video/audio evidence and any associated metadata (referred to in this document as data) from digital closed circuit television (DCCTV) systems that record to a digital video recorder (DVR). This document specifically addresses DVRs that have been powered down or removed from the scene. This document is not intended to address forensic video analysis techniques that may be performed after the retrieval of data. This document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System***, Section 1, Version 3.3, FBI's SWGIT, June 11, 2010. This document will familiarize the reader with important considerations in the capture, preservation, processing, and handling of images, whether the images are in digital, analog, or film format. This document will also refer the reader to other SWGIT documents for more complete details and guidelines. This document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***Best Practices for the Acquisition of Digital Multimedia Evidence (DME)***, Version 3.0, Law Enforcement and Emergency Services Video Association (LEVA), April 14, 2010. The goal of this document is to guide the investigator through best practices to ensure that best evidence is the target of DME acquisition and that the integrity of the original data is maintained. This document is available at: www.leva.org/wp-content/uploads/2013/01/Best_Practices-DME_Acquisiton_V_3_0-01-2013.pdf.

- ***Live Capture Field Guide V1.0—What Every Peace Officer Must Know***, FBI RCFL Continuing Education Series. This field guide was designed to help law enforcement personnel better understand the pros and cons of capturing volatile data—any data that is not recoverable once an electronic device loses power from a running computer system. Contents include key facts about digital evidence, if and when live capture is necessary, preparing for a live capture, on-scene best practices, commercial breaches, encryption, legal considerations, and more. This product is available only to law enforcement and government personnel and may be ordered at: http://www.rcfl.gov/DSP_N_orderDocs.cfm.

c. Ensuring integrity of the video

- ***Best Practices for Maintaining the Integrity of Digital Images and Digital Video***, Section 13, Version 1.1, FBI's SWGIT, January 13, 2012. This document is designed to cover the issues that can affect the integrity of digital media files. Integrity of a digital image or video file is best demonstrated through a combination of methods. This document will discuss specific methods and provide examples of how those methods can be applied. Maintaining integrity requires both documentation and security of the files throughout the workflow. A standard operating procedure (SOP) should describe the workflow. This document is available at: https://www.swgit.org/documents/Current%20Documents.

d. Securing video from handheld devices

- ***Mobile Forensics Field Guide—What Every Peace Officer Must Know***, FBI RCFL Continuing Education Series. This field guide was designed to help law enforcement personnel understand the potential role of handheld devices in criminal investigations and how to identify, properly handle, and preserve digital evidence on these media. Contents includes five key facts you should know about mobile forensics, mobile phones, flash media, iPods, MP3 players, gaming systems, global positioning system (GPS) devices, digital cameras, and legal issues. The digital camera section includes information on geotagging as well as a list of do's and don'ts. This product is available only to law enforcement and government personnel and may be ordered at: http://www.rcfl.gov/DSP_N_orderDocs.cfm.

What guidance is available for storing video files?

a. Labeling and categorizing video files for retrieval

- ***Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System***, Section 15, Version 1.1, FBI's SWGIT, January 13, 2012. This document is intended to familiarize readers with issues surrounding archiving DME and suggests best practices for establishing and maintaining an archiving program. This document may prove useful in the archiving of nonevidentiary images, video, and related files. This document is available at: https://www.swgit.org/documents/Current%20Documents.

Are there tools to help me with the analysis of video?

a. Image analysis

- ***Best Practices for Forensic Image Analysis***, Section 12, Version 1.7, FBI's SWGIT, June 7, 2012. Although aimed at image analysis (and end use of video gathered from crime scenes), there is some contextual information that may be helpful. The objective of this document is to provide personnel with guidance regarding practices appropriate when performing a variety of analytic tasks involving images, regardless of the knowledge domain that is the subject of analysis. This document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***Best Practices for Forensic Video Analysis***, Section 7, Version 1.0, FBI's SWGIT, January 16, 2009. The objective of this document is to provide guidance regarding appropriate practices for performing a variety of processing and analytical tasks involving video submitted for examination. This document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***Guidelines for the Best Practice in the Forensic Analysis of Video Evidence***, LEVA. The goal of this document is to provide a framework for the relevant concepts and issues in the scientific examination, comparison, and/or evaluation of video in legal matters. This framework is designed within the acceptable practices of the forensic video analysis community. The scope of this document includes the recovery of video evidence, equipment for forensic analysis, the process of forensic video analysis, output of video evidence, review of findings, and training considerations for analysts. https://www.leva.org/images/Best_Practices_FVA.pdf.

- ***Guidelines for Facial Comparison Methods***, Version 1.0, FISWG, February 2, 2012. The purpose of this document is to describe current methods for facial comparison and to provide guidelines for their appropriate use. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

- ***Facial Recognition System: Methods and Techniques***, Version 1.0, FISWG, August 13, 2013. This document provides a general outline of methods and techniques that can be helpful or considered when planning or operating a facial recognition (FR) system. The goal of this document is to provide guidance on methods and techniques to increase the likelihood of obtaining a true match in the candidate list. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

- ***Facial Image Comparison Feature List for Morphological Analysis***, Version 1.0, FISWG, DRAFT August 12, 2013. The purpose of this document is to provide a standardized facial feature list to be considered when conducting a morphological analysis. The feature list presented in this document is intended

to serve as the FISWG standard. This list includes the features of the face that may be visible and comparable between images. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

What tools would help me assist community businesses to share video?

a. Installation of CCTV/video equipment

- ***Best Practices for the Installation of CCTV Systems*** (two-part YouTube video), Forensic Audio, Video, and Image Analyst Unit (FAVIAU) of the FBI's Operational Technology Division. Part One of the video is available at www.youtube.com/watch?v=TRPVG9inn5w, and Part Two is available at www.youtube.com/watch?v=gA7VSGmTYG4. This video series features a realistic case scenario featuring the do's and don'ts of CCTV setup. It contains guidance for businesses on how to set up digital video recorders (DVRs) in a closed-circuit television (CCTV) recording system and obtain the best possible recorded footage to ensure that the video is useful in law enforcement investigations. Topics include setup, resolution, cameras and camera placement, best collection methods of the recorded footage for law enforcement, native/proprietary file format, retrieval methods, and more. Requests for DVDs may be made by e-mail to: cctvdvd@leo.gov.

- ***Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions***, Section 4, Version 3.0, FBI's Scientific Working Group for Image Technology (SWGIT), June 8, 2012. This document provides recommendations and guidelines for the use of closed-circuit television (CCTV) security systems in commercial institutions, such as banks, convenience stores, and other facilities. For the purposes of this document, fixed-site cameras and recording devices will be discussed. The basic principles and recommendations can, in most cases, be applied to any system using CCTV cameras and video recorders. This document addresses analog and digital video systems. The intent of these recommendations and guidelines is to optimize image quality to facilitate the identification of unknown people and objects depicted therein. The document is available at: https://www.swgit.org/documents/Current%20Documents.

- ***General Guidelines for Video Capture and Facial Recognition Systems***, Version 1.0, Facial Identification Scientific Working Group (FISWG), DRAFT August 12, 2013. The purpose of this document is to provide an overview of the considerations a practitioner should take when making decisions for the capture of facial images using video installed in fixed infrastructure (e.g., a CCTV system). This document is not intended to replace or supersede any existing standards documents. It summarizes the most important elements of existing standards, provides an introduction for new users, and provides direction to more detailed guidance available elsewhere. It outlines best practices for video collection to ensure that the images captured are suitable for facial recognition (FR) system use. This document is available in the Documents section of the FISWG Web site, www.FISWG.org.

- ***Digital Video Quality Handbook***, U.S. Department of Homeland Security's (DHS) *Science and Technology Directorate (S&T), May 2013* (http://www.dhs.gov/science-and-technology-directorate). This guidance document links a design process with real-life situations that use video in public safety applications, called "use cases," to the product classes, network infrastructure, and display devices in the solution. This handbook specifies public safety's minimum requirements for design, selection, and deployment of video surveillance systems (VSS) and associated infrastructure devices and components. It documents best practices of VSS design, system and component selection, deployment, and conformance. This handbook is primarily focused on network video systems, and its purpose is to specify a minimum level of performance for a VSS to satisfy common use cases: first responders; urban surveillance; in-car and transit video surveillance; public arenas;

loss prevention; and emergency operations, city security, and rail control centers. This document is available at: http://www.firstresponder.gov/TechnologyDocuments/Digital%20Video%20Quality%20Handbook.pdf.

b. Guidance for purchasing video systems

- ***Defining Video Quality Requirements: A Guide for Public Safety***, Volume 1.0, DHS S&T, July 2010. Often, emergency responders must consider a multitude of factors, such as installation, testing, support, redundancy, and training, before making video component procurement decisions. The guide provides an overview of video systems, defines functional concepts of video quality, explains how to generalize a use case with a use class, and provides a brief explanation of the qualitative aspects of video components. Emergency responders involved in the procurement process—of a video system either in part or in its entirety—will find this guide valuable because it considers an end-to-end system. For example, this guide identifies needs associated with a video stream as it travels from the scene (camera) through the system to the end user viewing the scene on a remote display. A wide range of information exists related to video quality and selection of video components such as installation, maintenance, training, and interoperability. While this guide does not provide detailed specifications and standards for video components, the Video Quality in Public Safety Working Group plans to release future guidance on technical performance specifications and standards that address various components of the video system. This document is available at: www.firstresponder.gov/TechnologyDocuments/Defining%20Video%20Quality%20Requirements.pdf.

- ***Facial Recognition Systems Guidelines for Specifications, Procurement, Deployment, and Operations***, Version 1.0, FISWG, November 18, 2010. This document provides a general outline of issues to consider when commissioning a facial recognition searching system (FR). It is structured as five high-level sections, each representing a phase in a logical process flow: business case definition; requirements gathering; proposal and procurement; deployment planning; and operations and maintenance. Each section provides an overview of relevant topics and main questions to be asked at that particular phase in the commissioning process. The goal of the requirements gathering phase is to turn the business case into requirements that can be understood by vendors and ensure that the purchased FR system is fit for purpose. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

What training programs or resources are available?

a. Terminology associated with video forensics

- ***Forensic Imaging and Multi-media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), and Forensic Video (FV)***, Version 7.0, a joint project of the International Association for Identification and LEVA, July 15, 2006. This document is available at: www.theiai.org/guidelines/iai-leva/forensic_imaging_multi-media_glossary_v7.pdf.

- ***Glossary***, Version 1.1, FISWG, February 2, 2012. This document contains a list of facial recognition and video forensic-related terms, acronyms, and definitions. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

- ***Glossary, Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems***, Version 1.0, Joint project among the FBI's Operational Technology Division, Digital Evidence Section, and Forensic Audio, Video, and Image Analysis Unit, in conjunction with the TSWG and the National Terrorism Preparedness Institute at St. Petersburg College, 2006. The purpose of this guide is to provide the best methods for the retrieval of video data evidence from DCCTV recording systems and to aid in the development of SOP. The guide contains a glossary of video-related terms, acronyms, and definitions. This document is available at: www.cttso.gov/sites/default/files/DCCTV-PocketGuide-v1-final.pdf.

b. Training guides

- FBI's Regional Computer Forensics Laboratory developed field guides and other resources in a continuing education series. These guides are available only to law enforcement and government personnel and may be ordered at: http://www.rcfl.gov/DSP_N_orderDocs.cfm.

  - ***Mobile Forensics Field Guide—What Every Peace Officer Must Know***. This field guide was designed to help law enforcement personnel understand the potential role of handheld devices in criminal investigations and how to identify, properly handle, and preserve digital evidence on these media. Contents includes five key facts you should know about mobile forensics, mobile phones, flash media, iPods, MP3 players, gaming systems, global positioning system (GPS) devices, digital cameras, and legal issues. The digital camera section includes information on geotagging as well as a list of do's and don'ts.

  - ***Digital Evidence Field Guide—What Every Peace Officer Must Know***. This field guide was designed to help law enforcement in properly handling and transporting digital evidence. Topics include five key facts about digital evidence, criminal uses of digital evidence, identifying digital evidence, legal considerations, executing a digital search warrant, packaging and transporting digital evidence, definitions, and more.

  - ***Live Capture Field Guide V1.0—What Every Peace Officer Must Know***. This field guide was designed to help law enforcement personnel better understand the pros and cons of capturing volatile data—any data that is not recoverable once an electronic device loses power from a running computer system. Contents include key facts about digital evidence, if and when live capture is necessary, preparing for a live capture, on-scene best practices, commercial breaches, encryption, legal considerations, and more.

  - Other RCFL Program Continuing Education Series DVDs:

    - ***Decoding Digital Evidence—What Every Law Enforcement Officer Must Know***, November 9, 2011.

    - ***Capturing a Running Computer System—What Every Digital Forensics and Cyber Professional Must Know***, October 14, 2010.

» ***Managing Mobile Forensics—What Every Peace Officer Must Know***, October 14, 2009.

» ***Managing Digital Evidence in the 21st Century—What Every Peace Officer Must Know***, June 6, 2007.

- Facial Identification Scientific Working Group (FISWG) develops consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features, primarily facial, as well as provides recommendations for research and development activities necessary to advance the state of the science in this field. The following training document is available in the Documents section of the FISWG Web site, www.fiswg.org.

  - ***Guidelines and Recommendations for Facial Comparison Training to Competency***, Version 1.1, November 18, 2010. The purpose of this document is to provide an overview of what practitioners should consider when making decisions for the capture of facial images using video installed in fixed infrastructure (e.g., a CCTV system). This document summarizes the most important elements of existing standards, provides an introduction for new users, and provides direction to more detailed guidance available elsewhere. It outlines best practices for video collection to ensure that the images captured are suitable for FR system use.

c. Entities that offer training and certification

- Law Enforcement and Emergency Services Video Association (LEVA), www.leva.org. LEVA is widely recognized as the global leader in forensic video and digital multimedia evidence processing training. It is the only entity that offers training and certification in this science. LEVA has conducted training since 2000 and operates the LEVA Lab, the first-of-its-kind training facility at the University of Indianapolis, which accredits LEVA's core courses. LEVA was presented with the August Vollmer Excellence in Forensic Science Award by the International Association of Chiefs of Police (IACP) for supporting a major investigation using the lab manned by the LEVA-trained Forensic Video Response Team.

- International Association for Identification (IAI), www.theiai.org. According to its Web site, the IAI, founded in October 1915, is "the oldest and largest forensic association in the world. This professional forensic association represents a diverse, knowledgeable, and experienced membership that is assembled to educate, share, critique, and publish methods, techniques and research in the physical forensic science disciplines." Though most publications are only available online for payment, they do offer training seminars regarding video evidence, as well as a forensic video certification, http://www.theiai.org/certifications/video/index.php.

- Digital Imaging and Video Recovery Team (DIVRT), three-day training module. This training combines hands-on instruction for safely recovering videos from various DVRs and exploiting video evidence through social media. This initiative sponsored by the FBI is geared toward assisting local and state law enforcement in reducing violent crime and is modeled after the Philadelphia Police Department's successful video exploitation program. For more information on this training, contact robert.bornstein@ic.fbi.gov.

d. Developing your own video training program

- ***Guidelines and Recommendations for Training in Digital and Multimedia Evidence***, Version 2.0, coauthored by SWGIT and the Scientific Working Group on Digital Evidence (SWGDE), www.swgde.org, January 15, 2010. The purpose of this document is to provide guidelines and recommendations to assist with designing a proper training program in forensic digital and multimedia. This document is available on the Documents Released with SWGDE Web page on the SWGIT Web site at: https://www.swgit.org/documents/Documents%20Released%20with%20SWGDE.

- ***Recommendations for a Training Program in Facial Comparison***, Version 1.0, February 2, 2012. The consistent and reliable use of facial comparison methods and facial recognition technologies requires the appropriate training of personnel to competence. The purpose of this document is to provide recommendations for training programs. Personnel who perform facial comparisons must be familiar with the capabilities and limitations of specific tools, technologies, and methods. Those engaged in facial comparisons should be familiar with the procedures commonly followed. They should also endeavor to be cognizant of, and adapt to, new developments. Additionally, trainers of those performing facial comparisons need advanced knowledge of these areas. In support of these goals, this document offers recommendations for training personnel engaged in this field. This document is available in the Documents section of the FISWG Web site, www.fiswg.org.

Acknowledgements

Guidance for Video Sharing for Investigations Task Team, Global Strategic Solutions Working Group

Sheriff Mike Milstead
Minnehaha County Sheriff's Office, South Dakota
Representing: National Sheriff's Association

Deputy Chief William Aubry
Forensic Investigative Unit
New York Police Department (NYPD)

Mr. Robert E. Bornstein
Cellular Analysis Survey Team
Violent Crimes Threat Section
Criminal Investigative Division
Federal Bureau of Investigation (FBI)

Agent Chad Carpenter
South Dakota Division of Criminal Investigation

Sergeant Edwin Coello
Facial Identification Section
NYPD Real Time Crime Center

Mr. Grant Fredericks
Forensic Video Solutions

Mr. Jan Garvin
FBI Academy/TV Studio
Representing: Law Enforcement and Emergency Services Video Association

Ms. Katrina Gossman
Forensic Audio and Video Image Analyst Unit, FBI

Captain Chris Jones
Southern Nevada Counter-Terrorism Center, Las Vegas

Mr. Richard Lautenbach
Target Corporation's Forensic Analysis Unit

Ms. Sandra Putnam
Child Exploitation and Computer Crimes Unit
Georgia Bureau of Investigation
Representing: Internet Crimes Against Children

Mr. Mike Roosa
Maryland State Police

This project was supported by Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice and the U.S. Department of Homeland Security.

For More Resources

The information contained within this document is also located online at https://it.ojp.gov/videoresources. Global is actively working to identify additional video resources and best practices that may be valuable to the field and has developed an online repository to house this information. Refer to https://it.ojp.gov/videoresources to view this growing compilation of FAQs and the tools recommended to address them.




About Global

The Global Justice Information Sharing Initiative's (Global) Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment.

GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global. BJA engages GAC-member organizations and the constituents they serve through collaborative efforts to help address critical justice information sharing issues for the benefit of practitioners in the field. These include the facilitation of Global Working Groups.

About Global Strategic Solutions Working Group

In support of the overall mission of Global, and with particular emphasis on providing the greatest value to fellow practitioners, DOJ, and the public, the Global Strategic Solutions Working Group (GSSWG) identifies high-priority information sharing business problems that can be significantly addressed through information sharing solutions. Through input from the field, GSSWG identifies priority business problems and uses a systematic process to fully consider evolving technology and the dynamic demands on the justice and public safety enterprise. Identification of priorities includes consideration of the complementary goals of supporting federal agencies, such as DOJ, the Office of Justice Programs (OJP), and the Bureau of Justice Assistance (BJA), and mission partners such as Global partners, industry, and other federal organizations. Determination of solutions includes a focus on evidence-based practices, as well as rigorous attention to privacy, civil rights, and civil liberties protections. For more information on GSSWG, refer to it.ojp.gov/gsswg.