JOINT TECHNOLOGY COMMITTEE
COSCA | NCSC | NACM

Managing Digital Evidence in Courts:

Policy, Process, and Technology for In-Person, Virtual, and Hybrid Proceedings

JTC RESOURCE BULLETIN UPDATED | [VERSION 1.0] 2026

Abstract

Courts increasingly rely on digital evidence across all case types, requiring consistent, secure, and efficient practices for its submission, management, presentation, and preservation. Courts are also supporting in-person, virtual, and hybrid proceedings, each introducing unique operational and technological demands.

This paper provides an integrated framework for managing digital evidence by consolidating and updating guidance from three prior Joint Technology Committee (JTC) publications: Managing Digital Evidence in Courts (2016), Managing Evidence for Virtual Hearings (2020), and Considerations for Procuring and Implementing Digital Evidence Management Software (2023).

The paper organizes guidance into three interconnected domains, policy and governance, process and workflow, and technology and platforms, to help courts align legal requirements, operational practices, and technology investments. It outlines governance structures, roles, and responsibilities; describes the digital evidence lifecycle and associated workflows; and identifies key considerations for procuring, implementing, and integrating Digital Evidence Management Systems (DEMS) with case management, eFiling, virtual hearing platforms, and other court technologies. It also addresses accessibility, cross-agency sharing, audit logging, security and privacy requirements, and the need for consistent practices across in-person, virtual, and hybrid proceedings.

The paper highlights common challenges, opportunities for innovation, and a maturity-based roadmap to support courts at varying stages of digital evidence modernization. By adopting a unified, lifecycle-based approach, courts can strengthen chain of custody, improve access and efficiency, enhance support for virtual and hybrid hearings, and ensure that digital evidence practices promote fairness, security, accessibility, and public trust across the justice system.

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	2/17/2016	JTC	Title: "Managing Digital Evidence in Courts"
1.0	6/25/2020	JTC	Title: "Managing Evidence for Virtual Hearings"
1.0	8/28/2023	JTC	Title: Considerations for Procuring and Implementing Digital Evidence Management Software"
1.0	06/15/2026	JTC	Managing Digital Evidence in Courts: Policy, Process, and Technology for In-Person, Virtual, and Hybrid Proceedings

Suggested Citation: *Managing Digital Evidence in Courts: Policy, Process, and Technology for In Person, Virtual, and Hybrid Proceedings* (Williamsburg, VA: National Center for State Courts, 2026).

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).

JTC MISSION

> **The Joint Technology Committee is a nexus that provides trusted and actionable thought leadership, guidance, education, and training for court use of technology to enhance administration and access to justice.**

JOINT TECHNOLOGY COMMITTEE

COSCA Appointments

Stacey Marz (Co-Chair)
Alaska Court System

Megan LaVoie
Texas Office of Court Administration

Amy Quinlan
Maine Administrative Office of the Courts

Herb Rouson, Jr.
District of Columbia Courts

Greg Sattizahn
South Dakota Unified Judicial System

NCSC Appointments

The Honorable Scott Schlegel
Louisiana Fifth Circuit Court of Appeal

The Honorable Andrea Vandeloecht
Chariton County Circuit Court

Ex-officio Appointments

Jim Cabral
IJIS Courts Advisory Committee

NACM Appointments

Paul DeLosh (Co-Chair)
Supreme Court of Virginia

T.J. BeMent
Georgia 10th Judicial Administrative District

Roger Rand
Oregon Multnomah Circuit Court

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Texas Office of Court Administration

CITOC Appointments

Pat Brooks
Missouri Office of State Courts

Winnie Webber
Illinois 19th Judicial Circuit

NCSC Staff

Shay Cleary

Table of Contents

Executive Summary

Courts operate in an environment where digital evidence is the norm rather than the exception. Documents, images, audio, video, and data generated by law enforcement, public agencies, and private parties now flow into nearly every case type, and courts must manage this evidence across in-person, virtual, and hybrid proceedings. These hearing formats introduce distinct operational and technological requirements, making consistent, secure, and efficient digital evidence practices essential.

This integrated Resource Bulletin consolidates and updates guidance from three prior Joint Technology Committee (JTC) publications, *Managing Digital Evidence in Courts* (2016), *Managing Evidence for Virtual Hearings* (2020), and *Considerations for Procuring and Implementing Digital Evidence Management Software* (2023), to provide a unified, end-to-end framework for modern digital evidence management. This Bulletin also incorporates field practices distilled from NCSC's Criminal Backlog Reduction Learning Collaborative resource on digital evidence (2023–24)[1].

The paper organizes guidance into three interconnected domains: **policy and governance, process and workflow,** and **technology and platforms**. This structure helps courts align legal rules, operational practices, and technology investments so that digital evidence is handled securely, consistently, and efficiently across different hearing types and procedural stages.

The **policy and governance** section outlines foundational decisions that shape digital evidence practices, including governance structures, roles and responsibilities, legal frameworks, and court-level policies. The section emphasizes cross-agency coordination, access and confidentiality rules, retention and destruction requirements, and the need for policies that address accessibility, protective orders, and sensitive data.

The **process and workflow** section describes the full digital evidence lifecycle, from creation and collection through intake, submission, review, pre-hearing preparation, in-hearing presentation, post-hearing access, and final disposition. It provides detailed guidance on operational processes, including standardized submission channels, required metadata, naming conventions, chain-of-custody practices, and quality assurance. It also integrates virtual and hybrid hearing workflows, recognizing that remote participation is now a permanent feature of court operations and that courtroom

[1] National Center for State Courts. (2024). *Pandemic Rapid Response Team: Criminal Caseload Backlog Reduction Learning Collaborative Series*. https://www.ncsc.org/sites/default/files/media/document/RRT-Criminal-Backlog-Reduction-Learning-Collaborative-Resources-Final.pdf

and virtual-hearing technology must support clear presentation and accurate capture of what is shown.

The **technology and platforms** section addresses the systems and tools that support digital evidence, including Digital Evidence Management Systems (DEMS), case management systems, eFiling portals, virtual hearing platforms, online evidence portals, identity and access management, judicial viewers, and audit logging and monitoring tools. It outlines key procurement and implementation considerations such as security, usability, accessibility, scalability, integration, vendor risk, and data portability. It also highlights mechanisms for sharing evidence and the security and reliability requirements necessary to protect sensitive information, including encryption, role-based access, and incident-response procedures.

Finally, the paper identifies common obstacles, opportunities for innovation, and a maturity-based roadmap to help courts advance from foundational practices to fully integrated, enterprise-level digital evidence environments. By aligning governance, workflow, and technology decisions, courts can improve fairness, efficiency, and access to justice while reducing risk and operational burden. Courts that adopt an integrated, lifecycle-based approach will be best equipped to meet the demands of the modern justice system.

Introduction and Statement of the Problem and Scope

Courts now receive digital evidence with increasing regularity in nearly every case type. Digital evidence includes documents, images, audio, video, structured data, and derived files such as transcripts or redacted copies. These materials originate from law enforcement, public agencies, private entities, and self-represented litigants.[2] As digital evidence becomes ubiquitous, courts must ensure that policies, workflows, and technology platforms support secure, consistent, and efficient handling across all phases of a case.[3] By adopting dedicated digital evidence management systems, courts may achieve increased efficiency, a reduction in continuances stemming from evidence exchange issues, and better access to digital evidence.[4]

At the same time, courts must support in-person, virtual, and hybrid proceedings. Each hearing format introduces unique operational and technological requirements for how evidence is submitted, reviewed, presented, and preserved. The rapid expansion of virtual hearings during the COVID-19 pandemic accelerated the need for standardized digital evidence practices that function reliably regardless of how participants appear.

This paper consolidates and updates guidance from three prior JTC publications:

- *Managing Digital Evidence in Courts* (2016), which introduced the concept of a digital evidence lifecycle and emphasized the need for coordinated policy, process, and technology decisions.
- *Managing Evidence for Virtual Hearings* (2020), which provided rapid-response guidance for handling evidence in remote proceedings.
- *Considerations for Procuring and Implementing Digital Evidence Management Software* (2023), which offered detailed procurement and implementation considerations for DEMS platforms.

---

[2] Joint Technology Committee. (2016). *Managing digital evidence in courts* (Version 1.0). https://cdm16501.contentdm.oclc.org/digital/collection/tech/id/866/rec/39

[3] Joint Technology Committee (2020). *Managing evidence for virtual hearings* (JTC quick response bulletin). https://cdm16501.contentdm.oclc.org/digital/collection/tech/id/1242/rec/60

[4] National Center for State Courts. (2024, November). *Pandemic rapid response team: Criminal caseload backlog reduction learning collaborative series resources*. State Justice Institute. https://www.ncsc.org/sites/default/files/media/document/RRT-Criminal-Backlog-Reduction-Learning-Collaborative-Resources-Final.pdf

Historically, court practices for managing digital evidence evolved in a fragmented manner. Email, CDs, DVDs, USB drives, and shared drives often supplemented or replaced traditional paper and physical exhibits. These improvised approaches frequently lacked consistent chain of custody, provided a cybersecurity risk, did not optimize the presentation view for every participant or juror, and were not integrated with case management and eFiling systems. As digital evidence volumes grow and virtual participation becomes routine, courts require standardized, scalable, and secure practices supported by modern technology platforms.[5]

This paper is intended for court leaders, technologists, judges, clerks, justice partners, and policymakers who are responsible for designing, approving, and operating digital evidence processes. It guides courts at all maturity levels, from those just beginning to receive digital evidence to those implementing statewide or enterprise digital evidence management solutions.

While deepfakes and other forms of AI-generated or AI-enhanced evidence are the subject of increasing discussion and concern within the court and legal community at the time of this publication, a detailed examination of those topics is beyond the scope of this paper. This bulletin focuses on broadly applicable policy, process, and technology considerations for managing digital evidence, regardless of its source. Courts seeking more targeted guidance on AI-generated evidence, including deepfakes, may find useful resources developed by the National Center for State Courts, such as the *AI-Generated Evidence Guide for Judges*[6].

[5] Vidizmo.AI (December 3, 2025). *Digital Evidence Management*. https://vidizmo.ai/blog/digital-evidence-management-iacp

[6] National Center for State Courts. (n.d.). *AI-Generated Evidence Guide for Judges. National Center for State Courts*. https://www.ncsc.org/resources-courts/ai-generated-evidence-guide-judges

Common Definitions and Context

To promote clarity and consistency across policy, process, and technology discussions, this paper uses the following definitions:

- **Digital evidence**: Any evidence in electronic form, including documents, images, audio, video, structured data, and derived files such as transcripts or redacted copies.
- **Digital Evidence Management System (DEMS)**: A system designed to receive, store, organize, and provide secure access to digital evidence across its lifecycle, typically with audit logging and role-based access controls. It may also include evidence presentation features.
- **Case Management System (CMS)**: The court's core system of record for case data, events, and documents.
- **eFiling system or portal**: The platform used by attorneys and parties to file documents and, in some configurations, submit digital evidence to the court.
- **Virtual hearing platform**: The video and audio-conferencing solution used to conduct remote or hybrid proceedings.
- **Online evidence portal**: A web-based interface where parties and justice partners can upload, view, or download digital evidence associated with specific cases under court-defined permissions. The portal may be part of the DEMS.
- **Chain of custody**: The documented history of who collected, handled, accessed, or changed a piece of digital evidence, including timestamps and actions taken.
- **Metadata**: Descriptive and technical information associated with digital evidence, such as file type, size, creation date, creation physical location, source system, and case number.

Key stakeholders include judges, court administration, clerks, IT staff, law enforcement, prosecutors, defense counsel, other agencies, and self-represented litigants. Another stakeholder may be a judicial reviewer, who examines digital evidence prior to or during a proceeding to determine admissibility, ensure compliance with court rules, and assess whether the evidence is complete, accessible, and properly labeled. The judicial reviewer may identify deficiencies, such as missing metadata, improper formatting, or late submissions, and issue instructions to parties to resolve issues before a hearing. This role supports early

case management, promotes fairness, and reduces delays during in-hearing presentation. Each stakeholder's role in submitting, reviewing, presenting, and accessing digital evidence must be reflected in court policy, workflow design, and system configuration.

Policy and Governance

Effective digital evidence management begins with strong governance, clear legal authority, and well-defined court-level policies. Courts must ensure that decisions about digital evidence are coordinated, transparent, and aligned with broader modernization efforts. Governance structures, rules, and policies form the foundation upon which workflows and technology platforms are built.

Governance, Roles, and Accountability

Digital evidence management requires coordinated decision-making across judicial leadership, court administration, IT, security, and justice partners. Without clear governance, courts risk inconsistent practices, security vulnerabilities, and technology investments that fail to meet operational needs.

Establishing Governance Structures

Courts should designate a governance body or steering committee responsible for:

- **Strategic direction**: Setting long-term goals for digital evidence management and aligning them with broader court modernization initiatives.
- **Policy approval**: Reviewing and approving policies related to security, privacy, access, retention, and sharing of digital evidence.
- **Technology oversight**: Prioritizing investments, approving technology selections, and overseeing major implementations and upgrades.
- **Cross-agency coordination**: Ensuring that clerks and justice partners, such as law enforcement, prosecutors, public defenders, and attorneys adhere to shared standards and practices.

A well-structured governance model ensures that decisions are made consistently, transparently, and with input from all relevant stakeholders.

Defining Roles and Responsibilities

Clear operational roles are essential for maintaining accountability and ensuring that digital evidence is handled consistently across cases and locations.

- **Judicial Officers**
  Judges set expectations for how evidence is submitted and presented, rule on admissibility, and ensure that proceedings are conducted fairly when evidence is digital.

- **Clerks and Court Staff**
  Clerks manage intake, indexing, quality control, chain-of-custody records, and retention and destruction activities. Staff must understand how to verify file integrity, apply naming conventions, and maintain accurate metadata.

- **IT Staff**
  IT teams design, configure, integrate, and support the technical environment, including security controls, identity management, and business continuity measures.

- **Judicial Reviewer**
  Reviews digital evidence prior to hearings to assess admissibility, identify deficiencies, and issue pre-hearing instructions that reduce delays and ensure compliance with court rules.

- **Justice Partners**
  Law enforcement, prosecutors, defense counsel, and other agencies must submit evidence in formats and through mechanisms defined by the court. They are responsible for protecting evidence in their custody and complying with court-defined standards.

- **Vendors**
  Vendor responsibilities must be clearly defined through contracts and service level agreements. These agreements should address data security, uptime, incident response, maintenance, and compliance with court policies.

Shared or Multi-Agency DEMS Governance

Where DEMS platforms are accessible among multiple agencies with shared responsibility, governance structures must define:

- How configuration changes are proposed and approved.
- How cross-agency standards are established and enforced.
- How data ownership, access, and retention responsibilities are allocated, including consideration of case-type-specific retention schedules that align with appeal timeframes.
- How disputes or inconsistencies are resolved.

Shared governance ensures that the DEMS functions as a unified, reliable platform rather than a collection of siloed practices. This often requires formal mechanisms, such as memoranda of understanding (MOUs), interagency agreements, or governance charters, to define responsibilities, decision-making authority, data-sharing expectations, and compliance obligations across participating agencies.

Legal Framework: Rules, Laws, and Administrative Orders

Digital evidence practices must operate within a clear legal framework that addresses admissibility, authentication, submission requirements, and preservation. Courts should review and, where necessary, amend rules of evidence, rules of procedure, and local administrative orders to explicitly address digital formats and remote participation.

Key legal topics include:[7]

- **Recognition of Digital Originals**
  Rules should clarify that digital exhibits can satisfy requirements for "originals" or best evidence when properly authenticated.
- **Authentication Standards**
  Courts should define acceptable methods for authenticating digital evidence, including metadata, hash values, system logs, or testimony about system reliability.

[7] Arizona Task Force on Court Management of Digital Evidence. (2019). *Arizona task force on court management of digital evidence. Washington Journal of Law, Technology & Arts, 13*(2), 229–270. https://digitalcommons.law.uw.edu/wjlta/vol13/iss2/4/.

- **Remote Testimony and Presentation**
  Rules should address how exhibits are presented in virtual and hybrid hearings, including requirements for visibility, access, and record capture.

- **Electronic Submission and Signatures**
  Courts may need to authorize electronic submission of exhibits and the use of electronic signatures or seals. In addition, courts need to address how notary public requirements will be met or whether they can be disbanded and instead individuals sign under penalty of perjury if permitted by statute or rule.

Administrative Orders and Local Practices

Administrative orders may be required to define:

- Deadlines for pre-hearing submission of digital exhibits
- Naming conventions and labeling requirements
- Acceptable file types (including prohibiting executables and zip archives)
- Procedures for handling oversized or sensitive files
- Requirements for testing file compatibility before hearings

Administrative orders should be:

- Technology-neutral, so they remain relevant as systems evolve
- Specific enough to guide system configuration and training
- Consistently applied across locations and case types

Court-Level Policies and Standards

Court-level policies translate governance decisions and legal requirements into operational expectations. Well-defined policies reduce variation, support security and consistency, and provide the basis for training and quality assurance.

Key policy topics include:

- **Access and Confidentiality**
  Policies must define which roles may view, download, or share digital evidence, including sealed or confidential materials. Access should follow the principle of least privilege.

- **Public and Media Access**
  Courts must also determine whether, and under what circumstances, members of the public or media may access digital evidence. Public access is governed by court rules, statutes, and case-specific restrictions, and may differ from access provided to parties. Policies should address how requests for digital exhibits are made, what formats may be provided, whether redaction is required, and how access is logged or monitored. Courts should ensure that any public access complies with confidentiality requirements, protects sensitive information, and does not compromise the integrity of the evidence.

- **Retention and Destruction**
  Courts must establish retention schedules and triggers for archiving or securely destroying digital exhibits. Policies should align with statutory requirements and records management standards. Automated purge and notice generation processes should be integrated with the case management system whenever possible.

- **Naming Conventions and Organization**
  Standardized file naming, exhibit numbering, and folder structures reduce errors and improve retrieval. Policies should specify required metadata fields and labeling practices.

- **Handling Sensitive Categories**
  Courts must define special requirements for evidence involving minors, sealed cases, medical or financial information, and other protected data. Policies should address redaction, restricted access, and secure storage.

Policy, Maintenance, and Review

Policies should be:

- Documented and approved by appropriate authorities
- Communicated clearly to staff, judges, and justice partners
- Periodically reviewed to ensure alignment with evolving law, technology, and practice

Process and Workflow

Digital evidence follows a predictable lifecycle, and courts must design workflows that support consistency, security, and fairness at every stage. Standardized processes reduce risk, improve efficiency, and ensure that judges, staff, and parties understand how evidence is handled across in-person, virtual, and hybrid proceedings. This section provides a comprehensive framework for operationalizing digital evidence management.

Evidence Lifecycle and High-Level Workflow

A lifecycle approach helps courts understand how digital evidence moves through the justice system and where policy, workflow, and technology must align. Although specific practices vary by jurisdiction and case type, most digital evidence follows these stages:

1. **Creation and Collection**
   Digital evidence is first created in the world, such as body-worn camera video, phone data, emails, text messages, social media content, surveillance footage, or digital files generated by agencies or private parties. Law enforcement, public agencies, or parties' experts collect, preserve, and document this evidence before it is ever submitted to the court. This stage includes initial chain-of-custody documentation, metadata capture, and any technical processes used to extract or export the evidence from source systems. Although courts do not control this stage, its quality directly affects the reliability, usability, and admissibility of evidence once it enters the judicial process.

2. **Intake and Submission**
   Evidence collected by justice partners or parties may be submitted to the court at case initiation, during the case, as an attachment to a motion, or during trial. To manage this process effectively, courts should define acceptable submission channels, file formats, and deadlines, and consider using flags for confidential or graphic content to trigger appropriate display safeguards, while recognizing that submission requirements may vary depending on the stage of the case. If procuring a DEMS solution, courts should ensure the system can manage evidence submitted with motions and evidence admitted at trial, including presentation to the jury during deliberations.

3. **Review and Triage**
   Court staff verify that evidence is properly associated with the correct case, meets technical requirements, and complies with submission rules. This includes checking file integrity, labeling, metadata, and whether submitted materials appear to contain protected, confidential, or personally identifiable information that may require redaction, restricted access, sealing, or other corrective action. Judicial reviewers may conduct early reviews to determine whether exhibits meet standards or require corrective action before the hearing. Because redaction responsibilities often begin with the filer but may also arise later through court review or court order, courts should be prepared to manage redaction issues at multiple points in the evidence life cycle.

4. **Proceeding Preparation** (Before Hearings and Trials)
   Evidence is organized, labeled, and made available to the court and parties in advance of hearings. Late submissions must be handled under defined rules to ensure fairness. Judicial reviewers may issue pre-hearing rulings or instructions to ensure that evidence is properly labeled, accessible, and ready for presentation. Evidence offered during trials may not be provided to the court in advance. However, attorneys or parties need to be familiar with how to present digital evidence during the trial, including how to mark it, share it with the court and opposing party, testifying witness, and jury if a jury trial. If using a digital evidence presentation solution, the attorneys and parties should be provided with detailed instructions and training about how to use the system to avoid problems during the trial. This may include comprehensive website instructions, short video tutorials, and even a practice session using the system.

5. **Proceeding Presentation** (During Hearings and Trials)
   At hearings and trials, digital evidence becomes exhibits that must be authenticated, admitted or excluded, and displayed to the judge, jury, and parties. Court policies and local rules should define pre-hearing exhibit exchange requirements, deadlines, acceptable formats, and procedures for raising objections. Workflows must address exhibit marking, checks for completeness, and contingency plans for technical failures.

   Effective exhibit handling is essential to ensuring fairness, maintaining an accurate record, and supporting efficient proceedings. As digital evidence becomes exhibits, courts must authenticate, mark, admit or exclude, and present materials in ways that are consistent, reliable, and accessible to all participants. Court policies, local rules, and workflows should define how exhibits are exchanged, reviewed, objected to, and displayed, while courtroom and virtual hearing technology must support clear presentation

and accurate capture of what is shown. The judicial reviewer, or the presiding judge, rules on objections and admissibility and ensures that the record accurately reflects the evidence presented.

Courtroom technology must reliably display, play, and record what was shown so that the record accurately reflects the evidence for appeal. During the proceeding, evidence is displayed or otherwise made available to the judge, parties, testifying witness, and the record, using presentation methods that function consistently across in-person, virtual, and hybrid hearings. A judge rules on objections and admissibility and ensures that the record accurately captures what was presented.

6. **Post-Hearing Storage and Access**
   The court preserves admitted exhibits and maintains access rules for parties, other courts, and the public, as appropriate.

7. **Final Disposition and Retention**
   Evidence is retained or destroyed according to schedules and legal requirements, with audit logs and chain-of-custody records maintained.

Mapping these stages for each case type and hearing format helps courts identify bottlenecks, redundant steps, and security risks.

Operational Processes: Submissions, Storage and Sharing

Operational processes define how digital evidence enters the court, how it is preserved, and how it is shared with authorized users. Policies establish the rules; workflows and technology ensure those rules are followed consistently and securely.

Submission Processes

Policies must specify who is authorized to upload digital evidence, acceptable formats, required metadata, and any chain-of-custody documentation. These requirements ensure that evidence arrives in a usable, verifiable form and that the court receives the information needed to associate it with the correct case and event.

Workflows and technology must enforce these policies through user authentication, standardized naming and tagging conventions, and automated audit trails for every upload, modification, or deletion. These controls maintain accountability, support chain-of-custody integrity, and reduce the risk of misfiled or altered evidence. Back-up requirements are essential to ensure digital evidence is maintained if there is a system outage or cybersecurity event.

Policies must also address discovery obligations, privilege, protective orders, and limits on use, for example, prohibiting parties from reposting sensitive evidence on social media or distributing it beyond the scope of the case. Workflows and technology should support these requirements by enabling secure submission channels, validating required metadata, and preventing unauthorized sharing.

Courts must also plan for exceptions. Judges need clear procedures for handling late submissions, technical failures, or parties who cannot access the system, ensuring that no participant is disadvantaged because of technology limitations. This may include alternative submission methods, extensions, or technical assistance.

Storage Processes

Storage processes ensure that digital evidence is preserved with integrity and protected from unauthorized access. Systems must maintain complete audit logs, track version history, and enforce retention and destruction rules that align with court policy and statutory requirements.

Evidence must be associated with the correct case, hearing, and exhibit number, with metadata preserved throughout its lifecycle. Storage systems should support encryption, role-based access, and monitoring for unusual activity to protect sensitive or confidential materials.

Courts should ensure that storage processes support continuity across the lifecycle, including transitions from pre-hearing review to in-hearing presentation and post-hearing retention. An adequate back up system is required to ensure the preservation of digital evidence.

Sharing Processes

Sharing mechanisms must allow authorized users, including judges, clerks, attorneys, justice partners, and, where appropriate, the public, to access evidence securely and efficiently. Policies should define how evidence is shared with parties, how sealed or confidential materials are handled, and how access is logged or restricted.

Workflows and technology should provide robust search, filtering, annotation, and role-based access controls so that teams can review large volumes of evidence without compromising confidentiality or chain of custody. Systems should support time-limited links, controlled downloads, user authentication, and in-system viewing to reduce the risk of unauthorized distribution.

Courts must also define how evidence is made available during hearings and trials, ensuring that presentation methods function reliably across in-person, virtual, and hybrid proceedings. Especially for hybrid hearings, it is important that all parties and attorneys have the same view.

Courts should implement presentation safeguards to prevent the inadvertent display of inadmissible or sensitive content, including controlled display modes and optional blurring features for graphic or sensitive materials. Responsibility for display should default to the submitting party, with alternative arrangements available for sensitive proceedings, while judges or clerks retain gating authority over what appears on jury and public-facing screens.

Virtual and Hybrid Hearing Workflows

Virtual and hybrid hearings introduce unique challenges for managing digital evidence. Courts must ensure that remote participation does not compromise fairness, access, or the integrity of the record. Rather than treating virtual workflows as temporary or exceptional, courts should integrate them into standard operating procedures.

Court Proceeding Procedures

Courts should define:

- Deadlines for electronic submission of exhibits
- Requirements for testing file compatibility
- Instructions for parties and self-represented litigants
- Procedures for resolving technical issues before the hearing

Clear communication reduces delays and ensures that all participants understand expectations.

Court Proceeding Management

Courts must establish procedures for:

- Displaying exhibits so all participants, remote or in-person, can view or hear them clearly
- Marking exhibits for identification and admission
- Ensuring the record captures what was seen or heard
- Handling objections in a manner consistent with due process
- Managing restricted access for sensitive content

Virtual and hybrid hearings require reliable tools for screen sharing, document display, and audio/video playback. Courts should ensure that judges and staff are

trained to use these tools effectively and assist self-represented litigants and attorneys if they experience problems to ensure their meaningful participation. Especially in jury trials, litigants or attorneys who look incompetent in presenting their evidence due to struggles in using the DEMS could adversely impact their cases.

Proceeding Management and Access

Courts must define how admitted exhibits are managed and accessed after the hearing, including:

- Whether exhibits are available through a portal
- Whether recordings and exhibits are linked or synchronized
- How long exhibits remain accessible to parties
- Whether digital evidence is maintained in the digital evidence system after the time for appeal has expired

When procuring a digital evidence solution, it is important to understand the capacity to store evidence, for what duration and at what cost. Post-hearing access rules should align with retention schedules and confidentiality requirements.

Quality Assurance and Chain of Custody

Reliable digital evidence management depends on maintaining a clear chain of custody and implementing strong quality assurance practices. Courts must ensure that evidence remains authentic, unaltered, and properly documented throughout its lifecycle.

Key Quality Assurance Practices

- **Logging and Auditing**:
  Systems should record who accesses or alters digital evidence, when, and for what purpose. Logs should be reviewed periodically.
- **File Integrity Checks**: Courts may use hash values or other tools to verify that files have not been corrupted or altered during transfer or storage.
- **Periodic Audits**: Courts should conduct sample reviews of cases to ensure adherence to policies on submission, labeling, access, and retention.
- **Training and Documentation**: Staff and users should receive clear instructions, checklists, and reference materials on digital evidence procedures.

Quality assurance ensures that digital evidence remains reliable and that courts can demonstrate compliance with legal and operational requirements.

Technology and Platforms

Technology is a critical component of effective digital evidence management. Courts rely on multiple systems, some internal, some shared with justice partners, to receive, store, organize, present, and preserve digital evidence. A well-designed technology environment reduces manual work, improves security, enhances user experience, and supports consistent workflows across in-person, virtual, and hybrid proceedings. This section outlines the technology landscape, integration priorities, procurement and implementation considerations, mechanisms for sharing evidence, and the security and reliability requirements necessary to protect sensitive information.

Technology Landscape and Integration

Courts typically operate several systems that intersect with digital evidence. These systems must work together to support the full evidence lifecycle, minimize redundant steps, and ensure that evidence is handled securely and consistently. A well-integrated technology environment enables courts to manage submissions, review, presentation, storage, and sharing without compromising chain of custody or confidentiality.

Core Components of the Technology Environment

- **Digital Evidence Management System (DEMS)**
  The central repository for storing, organizing, and managing digital exhibits and related files. A DEMS should provide robust audit logging, role-based access controls, metadata management, secure sharing capabilities, version history, and chain-of-custody tracking. Integration with other court systems reduces manual steps and ensures evidence remains linked to the correct case. It should be capable of retaining admitted and non-admitted evidence for possible review in an appeal.

- **Case Management System (CMS)**
  The court's system of record for case data, events, and documents. Integration between the CMS and DEMS reduces duplicate data entry, ensures that evidence is properly associated with case records, and supports automated workflows such as exhibit lists, hearing preparation, and judicial review.

- **eFiling Portal**
  The platform used by attorneys and parties to file documents and, in some configurations, submit digital evidence. Courts must determine whether exhibits are submitted through the eFiling system, a separate evidence portal, or both. Integration should ensure that metadata, case identifiers, and user authentication remain consistent across systems.

- **Online Evidence Portal**
  A secure web-based interface where authorized users, such as parties, attorneys, or justice partners, can upload, view, or download digital evidence. The portal should enforce standardized naming/tagging, required metadata, and automated audit trails for every upload or change. It should also support role-based access, time-limited sharing, and compliance with protective orders (i.e. injunctions against domestic violence) or privilege restrictions.

- **Virtual Hearing Platform**
  Video- or audio-conferencing tools are used to conduct remote or hybrid proceedings. These platforms must reliably display and play digital evidence, support screen sharing or integrated playback, and ensure that remote participants can view exhibits with the same view as those in the courtroom without compromising confidentiality or the record.

- **Presentation and Playback Tools**
  Courtroom and virtual-hearing tools used to display or play digital evidence during hearings and trials. These tools must support common file formats, allow controlled presentation by parties or the court, and ensure that what is shown is accurately captured in the record for appeal. Presentation using the application should be intuitive and easy to learn so that courtroom use does not cause undue stress if users do not regularly use the application. It is essential that the system is easy to use to minimize the likelihood that users appear incompetent when presenting to avoid harming their case, especially in front of a jury.

- **Judicial Viewer**
  A judge-facing interface that allows judges or judicial reviewers to securely access, review, and evaluate digital evidence before and during proceedings. The viewer should support playback of audio and video, display documents and images, metadata inspection, annotation tools, and access to sealed or confidential materials. It must provide a consistent experience across in-person, virtual, and hybrid hearings and integrate with both the DEMS and CMS.

- **Identity and Access Management (IAM)**
  Systems that authenticate users, manage permissions, and enforce role-based access across all digital evidence platforms. IAM ensures that only authorized individuals can upload, view, or modify evidence and that access aligns with court policy, protective orders, and confidentiality requirements. It is essential that the application incorporates foolproof features to avoid users sharing files that were not intended to be shared.

- **Storage and Archival Systems**
  Secure storage environments, whether cloud-based, on-premises, or hybrid, that preserve digital evidence with integrity throughout its lifecycle. These systems must support encryption, redundancy, retention schedules, and secure destruction processes, and must integrate with the DEMS to maintain chain-of-custody continuity.

- **Audit Logging and Monitoring**
  Comprehensive logging of all user actions, including uploads, downloads, modifications, deletions, and access to sealed materials. Monitoring tools should detect unusual activity, support investigations, and provide transparency for appeals or compliance reviews. Audit logs must be tamper-resistant and retained according to policy.

Integration Priorities

Integration reduces friction, improves accuracy, and enhances user experience across the digital evidence lifecycle. Courts should prioritize:

- Linking case and exhibit records between the CMS and DEMS to ensure evidence is consistently associated with the correct case, motion, hearing or trial, and exhibit number.

- Single sign-on (SSO) and consistent identity and access management so users authenticate once and retain appropriate permissions across all systems.

- Automated metadata exchange between systems to reduce manual entry, improve accuracy, and maintain chain-of-custody continuity.

- Judicial dashboards or judicial viewers that allow judges and judicial reviewers to access, review, and evaluate evidence from within familiar systems, including metadata, annotations, and playback tools.

- APIs and standardized data formats to support interoperability with justice partner systems, enabling secure evidence transfer and reducing redundant uploads.
- Centralized audit logging and monitoring across all integrated systems to ensure that every access, upload, modification, or deletion is captured in a tamper-resistant record.

A cohesive technology environment ensures that digital evidence is accessible, secure, and easy to manage throughout its lifecycle, while giving judges, court staff, and justice partners a consistent and reliable experience.

Key Implementation and Procurement Considerations

Procuring or upgrading technology to support digital evidence requires careful planning. Courts should base procurement decisions on clearly defined requirements derived from policy and workflow needs, not solely on vendor offerings.[8]

Security and Privacy

Courts must ensure that DEMS and presentation technology solutions support:

- Role-based access controls.
- Encryption of data in transit and at rest.
- Detailed audit logging.
- Support for sealed or confidential materials.
- Compliance with court defined classifications and restrictions.
- Inability for jurors to alter the admitted evidence when reviewing during deliberations.

[8] Mission Critical Partners. (2023, November 1). *Key takeaways from the 2023 Courts Technology Conference – Part 3.* Mission Critical Partners. https://resources.missioncriticalpartners.com/insights/key-takeaways-from-the-2023-courts-technology-conference-part-3

Usability and Accessibility

Systems should be intuitive for judges, staff, attorneys, litigants, jurors and external users. It is essential that presentation mode be easy to use to avoid attorneys or litigants struggling before the jury. It should be clear whether the court expects the system to be used without court employee assistance or whether a court employee will be required for different steps in the process for loading or presenting evidence. Courts should consider:

- Clear, simple interfaces.
- Support for self-represented litigants.
- Language access features.
- Accessibility for users with disabilities.
- What equipment will be needed for evidence presentation and jury deliberation, i.e., are large screens, individual tablets, speakers, or other equipment required?

Scalability and Performance

Digital evidence, especially video, can be large and resource intensive. Systems must:

- Handle growing volumes of evidence.
- Maintain performance during peak usage.
- Support high volume case types such as criminal, juvenile, or traffic.

Configuration and Flexibility

Courts should prioritize systems that allow configuration without extensive custom development. This includes:

- Customizable workflows, including different workflows for attachments to motions and evidence submitted and admitted during a trial, and for jury deliberations.
- Metadata fields.
- User roles and permissions.
- Retention and access rules.

Reporting and Analytics

Courts benefit from tools that provide:

- Usage metrics.
- Processing times.
- Storage trends.
- Workflow bottleneck identification.

The insights gained from reviewing reports and analytics inform management decisions and continuous improvement.

Data Ownership and Portability

Contracts must clearly define:

- Who owns the data.
- Who may edit, redact, seal, restrict access to, or delete data, and under what authority.
- How data can be exported.
- Acceptable formats for export.
- Where data will be stored and whether additional costs apply.
- How long data will be stored and whether different retention periods carry additional costs.
- Whether retention, deletion, or destruction must be suspended because of appeals, legal holds, or other preservation obligations.
- How and when data will be returned, deleted, or destroyed, including treatment of backups and any certification of destruction.
- The ability to export data for appeals, including format and whether it will be bundled or indexed.
- Requirements for data return upon contract termination.

Courts should avoid vendor lock-in and ensure long-term control over their data, including control over retention, redaction, access restrictions, return, and final disposition.

Vendor Viability and Risk

Courts should evaluate:

- Financial stability.
- Incident history.
- Use of subcontractors or third-party cloud services.
- Support models and response times.
- Uptime, availability commitments, maintenance windows, and remedies for service outages.
- Other courts' experiences using the product in different contexts, including attachments to motions, trial use, and jury deliberations.

Implementation Support and Change Management

Successful implementation requires:

- Training for judges, staff, and justice partners; attorneys and self-represented litigants will require ongoing training if not regular users of the system, so it is important to either plan for online training videos or training by court staff as needed.
- Configuration assistance.
- Pilot testing.
- Go-live support.
- Ongoing maintenance and updates.
- Clear prioritization criteria and vendor meeting cadence to keep momentum.
- A judicial champion, conduct targeted outreach to bar associations, and provide hands-on demos.

As part of implementation planning, courts should distinguish minimum required capabilities from desired features, recognizing that some functions may be implemented in phases. Courts should also define the intended use of the system, including whether it will support attorneys and litigants in managing, exchanging, and storing evidence; submitting digital evidence with filings; presenting and admitting evidence during proceedings; and displaying admitted evidence to juries during deliberation.

Platforms and Mechanisms for Sharing Evidence

Sharing digital evidence securely and efficiently is essential for fairness, transparency, and operational effectiveness. Courts must ensure that sharing mechanisms align with policies on access, confidentiality, and public transparency.

Common Sharing Mechanisms

- Secure portals where authorized users log in to upload or view exhibits.
- Access and use from mobile devices.
- Time-limited links or tokens that provide controlled access to specific files.
- In-court display systems for use during hearings or trials.
- Integrated document viewers within judicial dashboards or CMS interfaces.

Supporting Self-Represented Litigants

Courts must ensure that self-represented litigants can participate fully and fairly in digital evidence processes. Policies should require that individuals with limited technology access, limited English proficiency, or disabilities can submit and view digital evidence on equal terms, including providing alternatives when they cannot upload files themselves. Workflows and technology must support accessible interfaces, multilingual instructions, and accommodations that comply with disability-access requirements.

Courts should offer practical support such as:

- In-court kiosks with accessible interfaces and multilingual guidance.
- Assisted scanning or upload services provided by clerks or designated staff.
- Alternative submission methods, such as physical media or in-person assistance, which maintain security, integrity, and chain of custody.
- Accessible viewing options for audio, video, and documents, including captioning, transcripts, screen-reader compatibility, and interpreter support.
- Clear instructions and help/resources written in plain language and available in multiple formats for use on mobile devices.

This support ensures that no litigant is disadvantaged because of technology limitations, language barriers, or accessibility needs, and that digital evidence processes remain fair, inclusive, and consistent with court obligations.

Cross-Agency Sharing

Courts must define when and how digital evidence is securely shared or accessed with authorized justice partners and users, including:

- Law enforcement
- Attorneys
- Jurors
- Witnesses
- Child welfare and social-services agencies
- Appellate courts
- Judicial reviewers, when they are distinct from the presiding judge and require access for pre-hearing evaluation.

Sharing processes must protect confidentiality, comply with privilege and protective orders, and preserve chain of custody. Policies should specify what materials may be shared, under what conditions, and with which roles. Workflows and technology must enforce role-based access, time-limited links, and audit logging so that every access, download, or transfer is recorded. Systems should also support standardized formats and metadata to ensure that evidence remains usable and verifiable across agencies.

A well-defined cross-agency sharing framework ensures that justice partners can access the evidence they need while maintaining security, integrity, and accountability throughout the evidence lifecycle.

Security, Privacy, and Reliability

Digital evidence systems often contain sensitive personal, medical, and law enforcement information. In addition, digital evidence tools must scan submitted evidence for malware and viruses. Courts must treat these systems as critical infrastructure and implement robust security and reliability measures similar to other essential technology systems and platforms.

Access Control and Authentication

Courts should implement:

- Strong identity management
- Multi-factor authentication where appropriate

- Least privilege access policies
- Regular access reviews

Data Protection

Courts must ensure:

- Encryption in transit and at rest
- Secure backups
- Protection against unauthorized copying or removal
- Secure handling of removable media (if allowed at all)

Monitoring and Incident Response

Courts should maintain:

- Tools for detecting unusual activity
- Incident response plans
- Notification procedures for affected parties
- Regular security assessments

Business Continuity and Disaster Recovery

Courts must plan for:

- System outages
- Cyberattacks
- Natural disasters
- Failover and recovery procedures

These plans should be documented, tested, and updated regularly. In the event of system unavailability to present digital evidence, back up plans should be in place to avoid the need to reschedule hearings and trials.

Obstacles, Opportunities and Roadmap

Courts face a range of challenges when modernizing digital evidence practices. These obstacles often stem from resource constraints, fragmented systems, inconsistent local practices, varying levels of staff readiness, and judicial and attorney resistance to usage, especially presentation. At the same time, modern digital evidence tools and workflows create significant opportunities to improve efficiency, fairness, and access to justice. This section outlines common challenges, strategies for overcoming them, and a maturity-based roadmap to guide courts at different stages of digital evidence modernization.

Common Obstacles and Mitigation Strategies

Digital evidence modernization is complex, and courts frequently encounter similar challenges regardless of jurisdiction or size. Understanding these obstacles helps governance bodies and project teams plan realistic strategies, timelines, and resource needs.

1. **Funding and Procurement Complexity**
   Courts often operate with limited budgets and must navigate lengthy procurement cycles. Integrated digital evidence solutions may require multi-year investments, coordination with justice partners, and compliance with statewide procurement rules. Security, accessibility, integration requirements, and the need for extensive customization can further increase complexity.

   Mitigation Strategies:

   - Pursue phased implementation to spread costs over time.
   - Leverage statewide or regional procurement opportunities.
   - Prioritize high-impact case types or locations for early deployment.
   - Develop clear business cases that quantify operational, security, and access-to-justice benefits; include court-defined security, privacy, and accessibility requirements in procurement documents, not just vendor claims.

2. **Legacy Systems and Fragmentation**
   Many courts rely on multiple unconnected systems, manual workarounds, and outdated and unsecure tools such as CDs, DVDs, USB drives, or email. Fragmentation increases risk, reduces efficiency, and complicates chain-of-custody tracking by spreading digital evidence across multiple systems and handoff points. It can also expand the court's security exposure by increasing opportunities for unauthorized access, cyber incidents, and the introduction of malware through file transfers or unmanaged storage locations.

   Mitigation Strategies:

   - Map current workflows to identify redundancies, risks, and manual steps.
   - Prioritize integration between CMS, DEMS, eFiling, and judicial-review tools.
   - Replace high-risk manual processes with standardized digital workflows.
   - Use APIs and standardized data formats to support interoperability with justice partners.
   - Implement centralized audit logging and monitoring across systems.

3. **Variability in Local Practices**
   Different courthouses, judges, and case types may use different processes for submitting, reviewing, and presenting evidence. This variability complicates training, technology configuration, quality assurance, and support for judicial reviewers.

   Mitigation Strategies:

   - Establish statewide or district-wide policies, standards, and naming conventions.
   - Provide clear training, documentation, and role-specific guidance.
   - Use configuration, not customization, to support necessary variations.
   - Ensure judicial reviewers have consistent tools and workflows across locations.

4. **Staff and User Readiness**

   Judges, clerks, attorneys, justice partners, self-represented litigants, and jurors may have varying levels of comfort with digital tools. Without adequate training and support, even well-designed systems can fail. Accessibility, language support, and accommodations for disabilities must also be addressed.

   Mitigation Strategies:

   - Offer role-specific training and hands-on practice for judges, judicial reviewers, clerks, and attorneys.
   - Provide checklists, quick-reference guides, and responsive help-desk support.
   - Conduct pilot programs to build confidence before full rollout.
   - Ensure accessible interfaces, multilingual instructions, and accommodations for users with disabilities.
   - Provide alternatives for users with limited technology access, including assisted submission options.
   - Be aware of attorney concerns about looking incompetent before the jury if they use digital evidence platforms for presentation and consider carefully whether the court will require the platform's usage.

5. **Security and Privacy Concerns**

   Digital evidence often contains sensitive information, including personal data, medical records, law-enforcement materials, and information protected by privilege or protective orders. Courts must ensure that systems, policies, and workflows protect confidentiality, integrity, and availability throughout the evidence lifecycle. Security requirements should align with applicable standards, such as CJIS for criminal-justice data, and must be defined in court policy rather than relying solely on vendor assurances.

   Mitigation Strategies:

   - Implement strong identity and access management.

     Enforce role-based access controls, multi-factor authentication, and least-privilege principles across all systems that handle digital evidence.

- Require encryption and secure sharing mechanisms.

  Mandate encryption of data in transit and at rest, secure file-transfer methods, and time-limited or controlled-access links for sharing evidence with authorized users.

- Conduct regular security assessments.

  Perform penetration tests, vulnerability scans, and third-party audits to ensure systems meet court-defined security requirements and remain resilient to emerging threats.

- Establish clear incident-response procedures.

  Define how breaches, unauthorized access, or system failures are detected, reported, investigated, and remediated. Ensure staff understand their role in responding to incidents.

- Ensure vendors meet court-defined security and privacy requirements.

  Contracts and procurement processes should require compliance with applicable standards (e.g., HIPAA, CJIS), encryption requirements, audit-logging expectations, and data-retention and destruction rules.

- Maintain comprehensive audit logging and monitoring.

  Capture all access, uploads, downloads, modifications, and deletions in tamper-resistant logs. Monitor for unusual activity and ensure logs are retained according to policy.

A robust security and privacy framework ensures that digital evidence remains protected throughout its lifecycle and that courts can meet their legal, ethical, and operational obligations.

Opportunities for Improvement and Innovation

Despite the challenges, modern digital evidence practices offer significant opportunities to improve court operations, strengthen fairness, and enhance public trust. When implemented thoughtfully, digital evidence systems can streamline workflows, support judicial decision-making, and expand access to justice.

1. **Improved Access and Efficiency**
   Digital evidence systems allow judges, judicial reviewers, clerks, and attorneys to access exhibits quickly and reliably, reducing delays and improving the quality and timeliness of decisions. Standardized workflows and integrated tools reduce manual handling, minimize errors, and support consistent practices across locations.

2. **Enhanced Support for Virtual and Hybrid Hearings**
   Integrated systems enable smoother presentation of exhibits during remote and hybrid proceedings. Reliable playback, synchronized viewing for all participants, and judge-facing review tools improve fairness, accessibility, and the overall hearing experience, especially for self-represented litigants and participants joining remotely.

3. **Reduced Physical Storage and Handling**
   Digital evidence reduces the burden of storing, tracking, and retrieving physical exhibits, particularly in high-volume case types. Automated retention schedules, secure destruction workflows, and centralized storage environments improve compliance and reduce operational overhead.

4. **Better Data for Management and Policy**
   Digital systems generate valuable metrics on evidence volumes, processing times, user activity, and workflow bottlenecks. Courts can use this data to improve resource allocation, refine policies, evaluate technology performance, and support data-driven decision-making at local and statewide levels.

5. **Future Ready Capabilities**
   As technology matures, courts may explore advanced capabilities that further enhance efficiency and access, including:

   - Automated transcription and captioning.
   - Assisted search, indexing, and metadata extraction.
   - Video editing by attorneys or litigants before submission so that only relevant evidence is submitted.
   - Artificial intelligence (AI)–supported redaction and pattern detection.
   - Statewide or multi-agency digital evidence platforms.
   - Enhanced judicial review tools that support annotation, comparison, and metadata inspection.

   These innovations must be evaluated carefully to ensure they align with legal, ethical, accessibility, and governance requirements, and that they preserve fairness, transparency, and due process.

Roadmap for Courts at Different Maturity Levels

Courts vary widely in their starting point for digital evidence management. A one-size-fits-all approach is not practical. Instead, courts can use a staged roadmap for a pilot to prioritize actions that match their current capabilities, resources, and readiness. This roadmap helps courts plan incremental steps, track progress, and maintain alignment among policy, process, and technology decisions over time.

Foundational Stage

Courts at this initial stage receive digital evidence but lack standardized processes, integrated systems, or consistent practices. The focus is on establishing governance, defining minimum expectations, and reducing immediate risks.

Key Actions:

- Establish governance structures with representation from judges, clerks, IT, and justice partners.
- Identify team members to address issues at the foundational stage and plan for the development stage.
- Identify and approve core policies (access, retention, security, confidentiality, self-represented litigant (SRL) accommodations, training capabilities and expectations).
- Document current workflows and identify risks, including manual handling and inconsistent practices, differential viewing of evidence in hybrid hearings, and cybersecurity vulnerabilities.
- Define minimum technical requirements for submissions, storage, and presentation.
- Plan whether to use the DEMS for attorneys and litigants to store and exchange evidence, submit digital evidence attached to motions, submit, admit, and present evidence during hearings or trials, and provide admitted evidence to juries during deliberations.
- Begin planning for accessibility, language support, and alternatives for users with limited technology knowledge or capability.
- Plan for training support, including ongoing opportunities for new users.
- Identify early opportunities for judicial reviewers to support pre-hearing consistency.

Developing Stage

Courts have some digital evidence processes in place but need greater consistency, integration, and support for judges, staff, and litigants. The focus is on standardization and building reliable, repeatable workflows, resulting in a pilot project.

Key Actions:

- Identify development team members, including staff with expertise in both technical and business process aspects of the project, making sure to include staff very familiar with criminal and civil evidence rules, criminal and civil hearing and trial practices and offering and admitting evidence. Standardize submission, storage, and sharing processes across locations and case types.
- Implement or configure systems (DEMS, portals, judicial viewers) to support consistent workflows. Consider piloting with specific use cases such as allowing attorneys and litigants to submit digital evidence with motions, submitting, admitting, and presenting evidence during hearings or trials, providing admitted evidence to juries during deliberations.
- Provide training, documentation, and quality assurance for all user roles.
- Begin integrating DEMS with CMS, eFiling, and identity-management systems.
- Rigorously test DEMS usage from various user perspectives, including attorneys and litigants, judicial officers, jurors, and other planned users. If any issues surface, work with vendor to address concerns. If concerns cannot be addressed without great expense or because of time limitations, rethink the project's scope and evaluate whether it is possible to continue development.
- Expand support for virtual and hybrid hearings, including reliable presentation tools.
- Improve accessibility features and self-represented litigant support, including assisted submission options.
- Establish audit logging and monitoring practices.

Advanced Stage

Courts have established digital evidence practices and are ready to optimize, expand, and innovate. The focus is on full integration, analytics, and statewide or multi-agency coordination.

Key Actions:

- Determine if different or additional team members are needed to expand the usage of the DEMS for additional workflows.
- Fully integrate DEMS, CMS, eFiling, judicial viewers, and virtual hearing platforms.
- Expand use of portals and secure sharing mechanisms for justice partners and appellate courts.
- Expand usage of DEMS beyond initial workflows, adding full range of digital evidence management and presentation; this may include attorneys and litigants storing and exchanging evidence, submitting digital evidence attached to motions, submitting, admitting, and presenting evidence during hearings or trials, and providing admitted evidence to juries during deliberations.
- Rigorously test all workflows from various user perspectives, including attorneys and litigants, judicial officers, jurors, and other planned users. If any issues surface, work with vendor to address concerns. If concerns cannot be addressed without great expense or because of time limitations, rethink the project's scope and evaluate whether it is possible to continue development.
- Provide training support for all staff and judicial officers and external users and ensure opportunities for ongoing training for new users, highlighting issues that have arisen during prior usage.
- Use reporting and analytics to refine policies, allocate resources, and identify bottlenecks.
- Strengthen cross-agency interoperability using APIs and standardized data formats.
- Enhance security and privacy compliance (HIPAA, CJIS, encryption, incident response).
- Explore advanced capabilities such as automated transcription, assisted search, AI-supported redaction, and statewide or multi-agency digital

evidence platforms.

- Continuously evaluate accessibility, equity, and user experience across all roles.

Conclusion

Digital evidence is now central to the work of modern courts. As documents, images, audio, video, and structured data become increasingly common across all case types, courts must adopt practices that ensure evidence is handled securely, consistently, and efficiently. Fragmented or ad hoc approaches, once sufficient when digital evidence was rare, are no longer sustainable in an environment where virtual and hybrid hearings are routine, digital evidence volumes continue to grow, and expectations for accessibility and fairness are higher than ever.

This integrated bulletin brings together the foundational lifecycle concepts introduced in 2016, the virtual-hearing practices developed in 2020, and the procurement and implementation guidance published in 2023. By unifying these resources, courts gain a comprehensive framework that aligns policy, process, and technology decisions across the entire evidence lifecycle, including the needs of judges, judicial reviewers, staff, justice partners, and self-represented litigants.

The path forward requires strong governance, well-defined workflows, and technology platforms that are secure, scalable, interoperable, and accessible. It also requires ongoing training, quality assurance, and a commitment to continuous improvement as technology, law, and court practices evolve. Courts that invest in these areas will be better positioned to ensure fairness, maintain public trust, and deliver efficient and accessible justice.

As digital evidence continues to grow in volume and complexity, courts that adopt an integrated, lifecycle-based approach, supported by clear policies, consistent processes, and modern technology, will be best equipped to meet the demands of the modern justice system and support the needs of all participants.

For more information, visit:

TECHNOLOGY at NCSC

Appendix A: Example Functions and Capabilities Worksheet Provided by the Alaska Court System (ACS)

INSTRUCTIONS:

For each function/capability listed, the offeror should indicate if the function/capability is provided by the proposed software system. The offeror should mark an "X" in the appropriate column indicating if the function/capability has been developed and deployed, is currently in development or if the offeror can develop it. A blank in all three columns indicates the function is not developed and is not being offered for development. If the offeror indicates their proposed system has a function/capability, the ACS may expect to see that function/capability successfully demonstrated. Where the offeror is asked to describe their approach to a function or capability, the offeror should provide their response in the space provided. Inaccurate claims on a proposal may disqualify an offeror's entire proposal from further consideration.

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
1	**Access and Security**				
2	**User-Administrator Access**				
3	Solution offers ability for user-administrators to set roles and permissions (e.g., access to view, edit, and ability to delegate access, etc.) specific to certain users.				
4	Solution provides easily managed administrator definable multi-level security for access to files, information, and evidence based on roles in workflow.				
5	Solution provides security methods for creating folders and strictly limiting access for authorized users to certain folders or data within a folder based on folder-level or individual file -level permissions.				
6	Solution offers ability for user-administrator to customize data entry fields and configure main dashboard.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	**SYSTEM FUNCTIONS AND CAPABILITIES**	Developed and Deployed	In Development	Can be Developed	Comments
7	User administrator access includes authorized user access as below.				
8	**Authorized User Access**				
9	Solution accommodates no less than 25 concurrent separate Court staff users at initial implementation, with the option to increase to more than 100 concurrent Court staff users in the future, all without performance loss and without limitation. Or solution accommodates no less than 500 Court staff user licenses. **Offer or to describe what is being offered in Comments column and on Price Schedule.**				
10	Solution is scalable and flexible to allow for increasing the number of users with different permissions as authorized by user-administrators.				
11	Solution provides ability for judges and clerks to lock an exhibit or provide view only access to a user or jurors. This includes the ability to select specific evidence and move it to allow a profile/user to only view selected evidence. without the ability to modify any aspect of the evidence.				
12	Solution has ability to set an expiration date on access to externally shared case files.				
13	Solution has the option of a web browser - based viewer that allows authorized users to view and/or retrieve digital evidence via the web. This must be secure and encrypted according to CJIS standards, and with appropriate audit trail.				
14	**Public User Access**				
15	Solution accommodates no less than 1,000 public users at initial implementation, with the option to increase to more than 100,000 public users in the future, all without performance loss.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
16	**Security**				
17	Solution provides a database that is encrypted at rest and all transmissions to and from the database must be SSL encrypted.				
18	Solution allows all electronic evidence to be exported in an encrypted format for secure transmission.				
19	Solution provides all client data to be stored in a safe and secure environment and protected from unauthorized access, modification, theft, misuse or damage whether the data resides in a repository or during transmission over the network and must be stored in the United States.				
20	Solution provides virus/malware check on uploaded documents.				
21	Solution provides Single Sign-On for user-administrators and authorized users.				
22	Solution provides an audit trail that cannot be altered. The audit trail includes tracking all persons (using login and password) who accessed the system/file and the actions performed (upload, print, view, etc.). All audit trail items, including any document submitted as evidence, is time stamped with a system - generated time stamp provided as part of the solution.				
23	Solution uses Secure Hash so the Court staff will know whether evidence originals have been modified.				
24	Solution is maintained using a minimum of 99.9% uptime and security including parallel, redundant, and multi-tiered network architecture.				
25	Solution provides ability to ensure rapid recovery and seamless uptime in case of hardware malfunction.				
26	Solution is HIPAA compliant.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
27	Cost of all functional integrations assumed by contractor and/or included in priced offer.				
28	**Functionality**				
29	**Public Needs**				
30	Solution has ability to upload evidence, regardless of format, whether printed/handwritten, photograph, video, audio recording, etc.				
31	Solution has ability to upload regardless of file size.				
32	Solution allows for uploading from multiple devices, including without limitation, SD cards, hard drives, optical disks, thumb drives, mobile devices, etc.				
33	When uploading from any device, the solution allows files to be selected files for upload with previews using a simple import process/wizard.				
34	Solution provides drag-drop functionality for uploading multiple files (e.g. if Plaintiff has 150 exhibits to upload, can batch upload them through a drag/drop interface).				
35	Solution provides filename validation.				
36	Solution provides auto-numbering with unique identification for common reference.				
37	Solution provides ability to e-serve/electronically notify parties of uploaded documents.				
38	Solution provides secure external access for viewing and downloading of evidentiary data on computers (Mac and PC) and mobile devices including smart phones and tablets (Android, iOS, and Windows OS).				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
39	Solution provides a full screen viewing mode where multiple photos can be viewed easily from photo to photo or an entire PDF with scroll bars and can be viewed with a window frame.				
40	Solution offers ability to magnify any portion of a document or photo viewed.				
41	Solution provides multiple print options, including but not limited to: printed output with options to print at the user's option, documentation of the digital photo including title, notes, photographer's name, enhancement parameters, case number, authentication result, import time, camera clock time, photo resolution, flexible automatic sizing features, and autorotation.				
42	Solution offers secure cloud-based platform and data hosting.				
43	Solution offers closed captioning when playing videos for those that are hearing impaired or deaf.				
44	**Court Needs (includes Public Needs in addition to below)**				
45	Solution allows Court administrators to specify upload filetype or that any filetype may be uploaded, whether doc/docx, rtf, wpd, xls/xlsx, ppt/pptx, pdf, mp4, mov, m4a, m4v, mpg, avi, mp3, flv, ogg, wav, jpg, gif, heic, png.				
46	Solution allows upload by case number, case name, and party name.				
47	Solution provides that documents, typed or handwritten, be automatically OCR ready upon upload.				
48	Solution provides metadata, including identification of uploader/date/time uploaded.				
49	Solution retains uploaders email for use in exchanging exhibits.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	**SYSTEM FUNCTIONS AND CAPABILITIES**	Developed and Deployed	In Development	Can be Developed	Comments
50	Solution provides ability to send email alerts of new uploads or deletions.				
51	Solution provides ability to email links, whether to the main landing page or to specific evidence, with expiration dates for the links.				
52	Solution provides ability to support RAW format files without converting the RAW files into another format.				
53	Solution provides integrated preview/document viewer for common filetypes (e.g. doc/docx, rtf, wpd, xls/xlsx, ppt/pptx, pdf, mp4, mov, m4a, m4v, mpg, avi, mp3, flv, ogg, wav, jpg, gif, png).				
54	Solution provides ability to acquire, process, authenticate, store, and playback digital images, digital audio, and digital video in common formats defined as JPG, BMP, GIF, TIFF, MP3, MP4, WAV, DOC, and PDF.				
55	Solution provides ability for evidentiary video files to be stored with the associated players when applicable.				
56	Solution provides ability to restrict viewing of evidence before it is admitted, reject or admit evidence submitted to the Court, and to delete rejected evidence.				
57	Solution allows authorized users to seal and set deletion/retention parameters by case type and date, send alerts or flag evidence (admitted or denied) that is ready for deletion, and delete entire case with all evidence contents.				
58	Solution provides ability to create digital evidence case jackets.				
59	Solution provides ability to edit exhibits/files if incorrect.				
60	Solution provides ability to segregate exhibits by case and party.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	**SYSTEM FUNCTIONS AND CAPABILITIES**	Developed and Deployed	In Development	Can be Developed	Comments
61	Solution provides ability to reorder and categorize documents uploaded into a case (for example into customized folders).				
62	Solution provides built-in exhibit stamp functionality (so that documents can be marked electronically).				
63	Solution provides ability to reassign entire cases with all evidence included and send email alerts/notifications of reassignment.				
64	Solution provides ability to set exhibit status or case status (e.g., On Appeal, Case Closed, In Inventory, Returned, etc.).				
65	Solution allows multiple concurrent users to submit, receive, and update data, and view the same digital evidence simultaneously.				
66	Solution provides ability to present, display, and share uploaded evidence from database without having to first export.				
67	Solution provides ability to share video with audio in a MS Teams, Zoom or Webex meeting using screen share.				
68	Solution maintains/stores original copy of evidentiary files and has the ability for authorized users to make a working copy for internal annotations/bookmarks/notes on exhibits, even when a party submits multiple exhibits in a single file (both viewable to the court only, or to all parties).				
69	Solution has ability to create exhibit tags with different colors to differentiate between the Court staff, parties, exhibits, etc. for case specific evidence.				
70	Solution has ability to redact information and images on documents and videos submitted as evidence.				
71	Solution has ability to highlight and add key words, titles, notes, and bookmarks to digital evidence and to later index, search, and edit them.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	**SYSTEM FUNCTIONS AND CAPABILITIES**	Developed and Deployed	In Development	Can be Developed	Comments
72	Solution has ability to search digital files by using tagged metadata fields.				
73	Solution has ability to export the entire contents of a case file, regardless of file type.				
74	Solution has ability to export selected exhibits or segregate them into a packet for download (e.g. make available a copy of all marked exhibits to counsel).				
75	Solution allows the Court staff to acquire raw data through an export to Microsoft Excel (XLS/XLSX) or ASCII comma separated values (CSV) file formats at any time.				
76	Solution provides chain of custody reports.				
77	Solution provides ability for judges and clerks to easily view/examine selected evidence (regardless of format, whether printed/handwritten, photograph, video, audio recording, etc.) in a separate window/screen that easily allows for the full display of the evidence on a screen.				
78	Solution provides ability for judges and clerks to perform customized searches – search and filter for select data elements (any data field or combo of fields), such as ability to easily locate exhibits in the system by various criteria, numerical or alphabetical order, party, exhibit status, status on a case (e.g., On Appeal, Case Closed, In Inventory, Returned, etc.), exhibit name, key word, etc.				
79	Solution provides ability for judges and clerks to create customized system generated reports or use uploaded document/report templates.				
80	Solution provides ability for judges and clerks to customize appearance/format of exhibit list.				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
81	Solution provides ability for judges and clerks to print or save and export search results in PDF.				
82	Solution provides ability to grab a frame from a video and capture the image and save it and blur children or others who are not a part of the case.				
83	**Dashboard**				
84	Solution displays a main dashboard that shows alerts, notifications, and calendar view.				
85	Solution displays a dashboard per case that authorized users can configure using filters to view specific data elements within user specified date ranges. a. Results are shown graphically on the dashboard. b. Different case dashboards can be created for the same case based upon the role of the authorized user. c. Different case dashboards can be viewed separately by different authorized users.				
86	**System Data Exchange and Storage**				
87	Solution supports migration/integration from CourtView.				
88	Solution provides ability for all data to update automatically in real-time so that any searches do not need to be re-run.				
89	Solution provides ability for data to tie all to all case information, including closed cases.				
90	Solution is hosted on Microsoft Azure Government or AWS GovCloud; web-based; compatible with current web browsers (e.g., Chrome, Firefox, Microsoft Edge).				

Appendix A: Functions and Capabilities		Put an X in one of the columns for each line item not grayed out. A blank in all three columns indicates the function is not developed and is not being offered for development.			If an 'X' is in the "In Development" Col.: Indicate anticipated BETA date If an 'X' is in the "Can Be Developed" Col.: Estimate development time in hours
ID #	SYSTEM FUNCTIONS AND CAPABILITIES	Developed and Deployed	In Development	Can be Developed	Comments
91	Solution provides a SaaS solution that has storage for at least the following case types in 2019: 1. Jury Trials:510 2. Non-Jury Trials:2,23 3. Total Cases Filed: 123,963				
92	**Customer Support**				
93	Support offered includes technical assistance on the installation, use, performance tuning, maintenance, and repair of the software/hardware necessary to meet the requirements of this RFP and/or contract. Offerors to describe the training method and number of hours included.				
94	Offeror provides administrator level and end-user level training.				
95	Offeror provides customer service support 24 hours per day, 7 days per week.				

Appendix B: Electronic Evidence Management Considerations

Following is a list of additional topics management may want to consider when considering a Digital Evidence Management System.

- Evidence management vs. evidence presentation
- Desired level of clerical involvement – do they need to send invitation to share evidence? Or can the parties initiate themselves?
- Can the parties exchange evidence with whom they want (prosecuting attorney and law enforcement) on their side or just between sides?
- Cloud based vs. premise servers
- Concurrent licenses vs. named users.
- Cybersecurity – no flash drives, emails, etc. on court computers from outside
- Data security?
- Retention of evidence – how long?
- Storage costs?
- Easy user interface
- Criminal and civil cases?
- Ability to transmit to appellate court if appeal?
- Ability to redact information?
- Ability to cut longer videos to a short relevant clip?
- Ability to blur identity of people if needed?
- Ability to make notes and annotations and not share or redact later?
- Can be used for evidentiary attachments to motions and also trial (different processes)?
- Admin dashboard?
- Integrations with CMS, eFiling, document management systems to exchange data instead of clerks doing the work?
- Customization – exhibit #s, rearrange order?
- Mobile device support?
- Who provides tech support?

National Center for State Courts
300 Newport Avenue | Williamsburg, VA 23185
(800) 616-6164 | **ncsc.org**