

Request for Information (RFI):
Digital Preservation Repository Systems for Restricted and Confidential Digital Records
Connecticut State Library/State Archives/State of Connecticut
June 24, 2024

1. RFI Overview

The Connecticut State Library seeks information on the availability, capabilities, and costs associated with a secure digital preservation repository (SDPR) system for storing and preserving long-term CT government records containing personally identifiable information (PII), personal health information (PHI), records generated for or received/derived from the Criminal Justice Information Services (CJIS), or other sensitive or confidential information in the State Archives. The digital preservation system that the State Archives currently uses does not meet state or federal security requirements for storing confidential and sensitive information.

Please note that this Request for Information (RFI) is for informational purposes only, and no contract will be awarded as a result. A firm or organization's response to the RFI—or lack thereof—will not affect the evaluation of responses to any subsequent Request for Proposals (RFP) or Invitation to Bid (ITB) released. Responses will be used solely for information and planning purposes.

Please note that all responses will be public record and generally available to the public. If you have proprietary, trade secret, or other confidential information you wish to submit as part of your response to this RFI, please send it in a separate document clearly marked as containing the confidential information.

1.1. RFI Contact

We have designated the following individual to serve as the official point of contact for this RFI. This individual is the only authorized contact permitted to communicate on behalf of the Connecticut State Library/State Archives about this RFI.

Contact information for RFI point of contact:

Mark Conrad, Information Management Consultant (contractor)

Connecticut State Library/Connecticut State Archives

Mark.Conrad@ct.gov

1.2. Submission Details

Please submit your responses to this RFI via email to the RFI point of contact before the due date identified in Section 1.3. *When submitting your response, please use RFI# CSL2024-01 as the subject for your email.* The total size of your message and any attachments should not exceed 20 megabytes. Please consult the RFI point of contact if you need to send larger files. If you have more than one possible solution, please submit a separate response for each solution.

Physical (paper) copies of RFI responses are *not allowed*.

If you have any questions about this RFI, please direct them to the RFI contact during the appropriate period identified below in Section 1.3.

1.3. RFI Timeline

Please review the RFI timeline below. Dates may be modified or amended by the Connecticut State Library/State Archives, which will post an amendment to this RFI notifying prospective respondents of any change.

- RFI Released: June 24, 2024
- RFI Information Session: July 1, 2024
- Deadline for Questions: July 8, 2024
- Answers to Questions: July 15, 2024
- RFI Responses Due: July 22, 2024

1.4. RFI Information Session

We will hold an Information Session for this RFI to answer questions from prospective respondents. This information session will be virtual. A registration link for the Information Session can be found here: <https://events.gcc.teams.microsoft.com/event/9a7eb180-6209-4e1e-923c-8d925be29ce3@118b7cfa-a3dd-48b9-b026-31ff69bb738b>. During the Information Session, Connecticut State Library/State Archives staff will summarize the goals of the RFI, and the information requested. Connecticut State Library/State Archives staff will take questions from prospective respondents and community members during the Information Session. Any answers given at the Information Session are tentative, and final answers will be provided via a Q&A document released after the Deadline for Questions identified in Section 1.3. We will make available a recording of the RFI Information Session.

2. Background Information

2.1. Background

Since 1855 the Connecticut State Library has acquired historical records from the three branches of State government. In 1909, the General Assembly made the State Library the official State Archives. These records, dating from 1629 to the present, document the evolution of state public policy and its implementation, the rights and claims of citizens, and the history of Connecticut and

its people. The Archives also contains municipal and church records, photographs, and manuscript collections.

In the 1990s the State Archives formulated its first policies concerning digitization and born digital records. Since 2013 the State Archives has utilized the Connecticut Digital Archive (CTDA) repository¹ to preserve and provide access to non-sensitive records. Multiple organizations, in addition to the State Library and the State Archives, store and make accessible archival digital records in the CTDA. As currently configured the CTDA does not meet security requirements for storing sensitive records. The State Archives must have access to a secured repository for archival records with sensitivities that prevent their full release. Partially releasable (redacted) records will be preserved in the CTDA. Further information about the CTDA can be found in Appendix B.

In 2022 the Connecticut State Library received a Congressionally Directed Spending grant of \$948,000 through the efforts of Senator Richard Blumenthal and Senator Christopher Murphy to support the automatic transfer and preservation of historic digital records from state agencies. The grant was awarded by the National Historical Publications and Records Commission (NHPRC). Part of the grant is designated for planning the acquisition of a secure digital preservation repository. This RFI is one of the information-gathering tools the Connecticut State Library is using for this planning process.

2.2. Goals and Outcomes

We will use the information collected from this RFI to develop an estimated total solution cost for a possible future budget request and to prepare a Request for Proposals for acquiring a secure digital preservation repository system for Connecticut government records that contain sensitive information. Depending on the information gathered and the availability of funding, it is anticipated that the Connecticut State Library will issue an RFP for an SDPR within 12 to 24 months. The ultimate goal is to ensure that all historically significant digital records from 161 state agencies at over 4,000 locations throughout the state can be transferred to and preserved by the State Archives.

2.3. Minimum Requirements

The desired solution should meet these **minimum requirements**:

The SDPR will contain only archival records that have sensitivities that prevent their full release. Partially releasable (redacted) records will be preserved in the Connecticut Digital Archive (CTDA) – not the SDPR. The system will contain no National Security Classified materials.

Approximately 230 people will potentially need access to the SDPR. It is highly unlikely that all of these personnel will need access to the SDPR.

Anticipated user roles for the SDPR with estimated numbers include:

1. Public Records Administrator (PRA): 1
2. Records Management Analyst (RMA): 6

¹ <https://ctda-dev1-lib.grove.ad.uconn.edu/node/431849>

3. Records Management Liaison Officer (RMLO): 109
4. Assistant Records Management Liaison Officers (ARMLO): 101
5. State Archivist (SA): 1
6. Assistant State Archivist (ASA): 6
7. IT staff from Department of Administrative Services' Bureau of Information Technology Solutions (DAS BITS): 6
8. Compliance Officers: 2

Permissions for users of the SDPR will need to be configurable to a very granular level in order to enforce a least privilege policy when assigning access controls. (See, for example, CJIS Security Policy, Section 5.5 and Appendix G.5. for more information on least privilege and access controls.)

Descriptions of each user role and the anticipated technical skills of persons in each role can be found in Appendix C.

At some point in the future personnel from some of the organizations listed below may need to use the SDPR:

- 169 municipalities (cities, towns, boroughs, etc.)
- 9 regional council of governments
- 6 regional education councils
- K-12 schools both public and private
- Public libraries that are not under municipal governments (i.e., association libraries)
- Other regional government and consortium (see Secretary of the State Register and Manual page, <https://portal.ct.gov/SOTS/Register-Manual/Section-VII/Regional-Councils-of-Governments>)

The SDPR must restrict access to authorized state agency personnel, ensuring they can only access records from their agency unless explicitly authorized to view records from other agencies.

All use of the SDPR will be monitored with full audit trails.

Copies of the SDPR will be geographically dispersed and synchronized.

The SDPR must comply with legal requirements found in legislation and regulations including, but not limited to:

Connecticut General Statutes, including but not limited to, sections contained within:

Chapter 3, Public Records: General Provisions
(https://www.cga.ct.gov/current/pub/chap_003.htm)

Chapter 14, Freedom of Information Act
(https://www.cga.ct.gov/current/pub/chap_014.htm)

Chapter 47, State Property and Funds (https://cga.ct.gov/current/pub/chap_047.htm)

Chapter 55, Personal Data (https://cga.ct.gov/current/pub/chap_055.htm)

Chapter 188, Libraries and Museums
(https://www.cga.ct.gov/current/pub/chap_188.htm)

Chapter 961a, Criminal Records
(https://www.cga.ct.gov/current/pub/chap_961a.htm)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) (<https://www.govinfo.gov/content/pkg/USCODE-2022-title20/html/USCODE-2022-title20-chap31-subchapIII-part4-sec1232g.htm>); and related regulations at 34 CFR Part 99) (<https://www.ecfr.gov/current/title-34/subtitle-A/part-99?toc=1>)

Protection of Pupil Rights (20 U.S.C. § 1232h) (<https://www.govinfo.gov/content/pkg/USCODE-2022-title20/html/USCODE-2022-title20-chap31-subchapIII-part4-sec1232h.htm>)

Health Insurance Portability and Accountability Act (HIPAA) (<https://www.hhs.gov/hipaa/index.html>)

Health Information Technology for Economic and Clinical Health Act (HITECH) (<https://www.hipaajournal.com/what-is-the-hitech-act/>)

The Americans with Disabilities Act (ADA) <https://www.ada.gov/law-and-regs/ada/>

Genetic Information Nondiscrimination Act of 2008 <https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008>

The Family and Medical Leave Act of 1993, as amended <https://www.ecfr.gov/current/title-29/subtitle-B/chapter-V/subchapter-C/part-825?toc=1>

The SDPR must be in full compliance with, but not limited to:

The Criminal Justice Information Services (CJIS) Security Policy version 5.9.4 or more recent (<https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>)

The CJIS Requirements Companion Document (<https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/requirement-companion-document-pdf/view>)

Connecticut CJIS Security Policy V. 1.0
(https://www.ct.gov/cjis/lib/cjis/publications/CT_CJIS_Security_Policy_Final.pdf)

Criminal Justice Information Systems, 28 CFR 20 (<https://www.ecfr.gov/current/title-28/chapter-I/part-20?toc=1>)

Federal Information Security Modernization Act of 2014 (Public Law 113-283; December 18, 2014).

28 USC § 534, authorizes the FBI to exchange Criminal History Record Information (CHRI) with, and for the official use of, authorized officials of the Federal Government, the States, Indian tribes, cities, and penal and other institutions. The exchange of CHRI made available pursuant to this authority is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

28 CFR § 50.12 also sets forth requirements for the exchange of CHRI for noncriminal justice purposes authorized by federal law to include Public Law 92-544. This section of the C.F.R. mandates that CHRI obtained under these authorities may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

The Compact, pursuant to 42 USC § 14616, Article IV(c), requires that any CHRI obtained under the Compact may be used only for the official purposes for which the CHRI was requested. Further, this section establishes procedures to protect the accuracy and privacy of CHRI by requiring that CHRI must only be used by authorized officials for authorized purposes and that subsequent record checks be requested to obtain current information whenever a new need arises.

The SDPR must be able to ingest, process, preserve and provide access to the following types of files:

- Audio
- Video
- Text
- Images
- Geospatial
- CAD/CAM/CAE
- E-mail
- Databases
- Spreadsheets
- Presentations

For preservation purposes, the Connecticut State Library (based on the Library of Congress Recommended Formats Statement) strongly suggests records be saved as:

- Images – tiff, jpeg, jp2, png, gif, svg
- Documents – txt, rtf, doc, docx, odt, PDF, or PDF/A
- Spreadsheets – csv, txt, PDF, PDF/A, ods
- Databases – sql (with CREATE and INSERT statements), SIARD (Software Independent Archiving of Relational Databases), csv, xsl, xslx
- Presentations – ppt, PDF, PDF/A, odp

- Audio – Broadcast wave (bmf, wav), mp3
- Video – avi (lossless), mov, mp4
- Email – eml, html, mbox, msg, pst
- Compressed folders – zip

The above list (with the exception of the SIARD format) is from Public Records Standards 04-1: Electronic Records (12/2022), page 6, <https://ctstatelibrary.org/wp-content/uploads/2022/12/PRS04-1ElectronicRecordsStandards2022.pdf>.

The initial volume of records to be ingested into the SDPR will be approximately 100 TB. Subsequent years will see additional accumulations depending on state agency activity and any changes to restrictions implemented by the state or federal government.

The initial number of files to be ingested into the SDPR will be approximately 70,000. Subsequent submissions should be at least 1,000 files per month.

Most, if not all, of the records stored in the SDPR will come from CT executive branch agencies.

Only permanent archival and life of structure retention records will be preserved in the SDPR.

Anticipated workflows for the SDPR include:

Ability to securely ingest records directly from FileNet, Microsoft 365 (SharePoint, OneDrive, Teams, Outlook/Exchange), Microsoft Azure, AWS S3, Google Cloud, Laserfiche, and physical storage media.

Ability to run virus checking, malware detection, checksum generation/verification at time of ingest.

Ability to securely submit and ingest records from network storage spaces through a web browser interface (like a drop box/mail box).

Ability to create metadata through automated data capture, machine learning, and manually by archivists or authorized agency personnel.

For each record transferred to the SDPR the submitting agency must provide administrative, descriptive, and technical metadata. At a minimum, the SDPR should accommodate the metadata described in Public Records Standards 04-1: Electronic Records (12/2022), pages 6-10, <https://ctstatelibrary.org/wp-content/uploads/2022/12/PRS04-1ElectronicRecordsStandards2022.pdf>

Ability to securely allow for a copy of an ingested record or records to be downloaded for authorized agency personnel to fulfill business needs (e.g., re-opened State Police investigations; state forensics lab needs a case file for litigation; student transcripts to fulfill a transcript request; etc.). The turnaround time for downloading records will need to be tiered depending on the records/records retention series. Some records will need to be retrieved in 12 to 24 hours. Others will need to be retrieved in 24 to 120 hours.

Ability to pass data in a secure manner between the SDPR and other systems – including, but not limited to, our AWS S3 bucket, other instances of the SDPR, and systems contributing records to the SDPR. CSL has access to Microsoft Azure including OneDrive, Teams, and SharePoint; Box; and AWS S3 to facilitate the migration of records to the SDPR.

Ability to run reports to share metrics and statistics on the SDPR with stakeholders and funders.

3. Information Requested

3.1. Who We're Looking For:

The Connecticut State Library/Connecticut State Archives is especially interested in receiving feedback on this proposed project from vendors providing all or parts of a secure digital preservation repository system that best meets the needs outlined in Section 2.3 (above).

3.2. What We're Looking For:

In addition to describing how your proposed solution meets the minimum requirements outlined in Section 2.3. (above), please include all pertinent information such as:

- (a) Technical specifications including software requirements and hardware requirements;
- (b) Workflows including, but not limited to the following
 - 1) Identification and Preservation of Data;
 - 2) Collection of Data;
 - 3) Processing;
 - 4) Review and Redaction of Data;
 - 5) Production of Data;
- (c) Features & Functionality;
- (d) Scalability/flexibility/customization (e.g., granularity of permissions, roles, groups);
- (e) Data migration process of existing data to the vendor environment;
- (f) Storage;
- (g) Backup process and frequency;
- (h) User administrative responsibilities;
- (i) System administrative functions;
- (j) Policies for and availability of third-party add-ons;
- (k) Data hosting location(s) (All SDPR data must be stored in the United States. (See, for example, CJIS Security Policy, Section 5.10, SC-28 and Appendix G.3));
- (l) User license fees/terms/conditions/restrictions;
- (m) Login procedures/protocols (e.g., Azure active directory, firewalls, RSA tokens, multi-factor authentication, etc.);
- (n) Pricing structures/models (one-time fee, recurring fees, SaaS subscription, add-on features/functionality fees, per user/seat fees, per document fees, etc.) [See Appendix A];
- (o) Third party arrangements (installation, configuration, commissioning, resellers, etc);
- (p) Maintenance coverage, technical support, and warranty including support/upgrades/updates/patches;
- (q) Security, privacy & compliance (See especially the CJIS Security Policy and related documents cited in 2.3, above.);

- (r) System audit and intrusion tracking;
- (s) Onboarding process;
- (t) Training, including, but not limited to, user training, knowledge transfer sessions and support for DAS BITS teams providing technical support, etc.;
- (u) Service lifespan;
- (v) Cost estimate for the total solution cost [Please use the table found in Appendix A or a similarly detailed document, to prepare your response.];
- (w) Contact information for existing customers who are willing to discuss their experience with the solution (We are especially interested in talking with customers who have a CJIS compliant solution.); and
- (x) Availability and extent of documentation for the solution.

4. Appendices

Appendix A. Total Solution Cost Estimate

CSL is seeking to gather cost information that provides enough detail to serve as the basis for a budget request to acquire an SDPR. Describe the contract and cost breakdown structure of the recommended solution(s), identifying types of costs associated with the solutions and variables that contribute to the costs to acquire, operate, and maintain the solution for a minimum of three years.

For each relevant variable, please insert an estimated cost range into the table below and include the table in your response. More precise estimates are welcome, if available.

Cost Variables	Estimated Cost
Purchase price	
Per-seat costs	
Per-transaction costs	
SaaS subscription fees	
Hardware costs	
Software costs	
Licensing fees	
Labor costs	
Storage costs	
Custom development costs	
Operations & maintenance costs	
Other (please insert)	

Please indicate if any or all components of the proposed solution are available from the National Association of State Procurement Officials (NASPO) contracts for Connecticut (<https://www.naspo.valuepoint.org/participants/participant-results/?state=Connecticut>). If so, please indicate which contracts and items cover the components in the proposed solution.

Please indicate if any or all components of the proposed solution are available on GSA schedules that are open to state agencies. If so, please indicate which contracts and items cover the components in the proposed solution.

Appendix B. Information about the Digital Preservation Repository Currently used by the CT State Archives

Since 2013 the State Archives has utilized the Connecticut Digital Archive (CTDA) repository to preserve and provide access to non-sensitive records. Over 100 organizations, in addition to the State Library and the State Archives, store and make accessible archival digital records in the CTDA. Each organization maintains ownership of its digital materials and decides what metadata it will maintain for its collections.

As currently configured the CTDA does not meet security requirements for storing sensitive records. Some of the reasons CTDA cannot be used for this purpose are:

The CTDA staff do not believe their system can meet the requirements for storing CJIS information.

Connecticut State Library staff are concerned that the use of the CTDA by multiple organizations may not allow the State Library to meet the state and federal security requirements for storing sensitive records.

The CTDA does not currently allow records to be embargoed from public release for an indefinite period of time.

The State Archives must have access to a secured repository for archival records with sensitivities that prevent their full release. Partially releasable (redacted) records can be preserved in the CTDA.

Technical information about the CTDA includes:

- CTDA's current management and presentation platform is Islandora².
- It implements the Handle System to provide persistent and unique identifiers for digital assets.³
- Any format can be deposited into CTDA. However, CTDA through Islandora provides services such as the creation of derivatives and technical metadata extraction for the following formats: doc, docx, ods, txt, html, sxc, csv, tsv, odp, sxi, ppt, pptx, xls, xlsx, warc, PDF, tiff/tif, jp2, jpg/jpeg, png, bmp, wav, mp3, ogg, mp4, mov, qt, m4v, and avi.⁴

² <https://www.islandora.ca/>

³ <https://www.handle.net/>

⁴ Detailed information is available at: <https://uconn.atlassian.net/wiki/spaces/CTDA/pages/5384504031/CTDA+Technology>

Appendix C. Information about the Proposed User Roles

Listed below are descriptions of the anticipated user roles and their expected technical skills.

Public Records Administrator (PRA) - Responsibilities of the Public Records Administrator include: overseeing the life cycle of public records in all formats from creation to use to maintenance to disposition; publishing and editing records retention schedules; producing manuals, policies, and guidelines to keep state and local government agencies informed about new records management issues and requirements; training government employees on a wide range of records management issues; developing standards for records creation; overseeing the disposition of public records; identifying and preserving records needed to continue government operations in case of a disaster or emergency; publishing regulations for land and property records, as well as for the construction of town record storage vaults; conducting the annual examination of land record indexes; running a grant program for towns to enhance and improve the preservation or management of local historic documents; and managing the State Records Center for the safe storage of state agency records.

Anticipated Use of the SDPR: oversight of and sign off on records transfers and compliance with the records management program; and ability to run reports as necessary.

Expected Technical Skills: Familiarity with Microsoft Office applications and records management software.

Records Management Analyst (RMA) - Responsibilities of the Records Management Analyst include records appraisal and analysis, records scheduling and disposition, records storage, file and database management, policy development, and reference; develops records retention schedules for state agencies and municipalities; develops and revises records management policies, procedures, manuals and regulations governing public records; assists state agency records management liaison officers and municipal officials with records retention and management issues; identifies records management training needs and develops and presents training to state agency and municipal officials; conducts agency site visits and facility inspections.

Anticipated Use of the SDPR: assist state agencies with questions and compliance with the records management program, and ability to run reports as necessary.

Expected Technical Skills: Familiarity with Microsoft Office applications and records management software.

Records Management Liaison Officer (RMLO) - Each state agency must appoint a Records Management Liaison Officer (RMLO) to coordinate records management activities for the agency and to serve as a liaison with the Office of the Public Records Administrator. Typical duties and responsibilities for the RMLO position include: implement and maintain the agency records management program; create internal guidelines for maintaining and using agency records; conduct regular reviews of existing agency records schedules; identify out-of-date and inaccurate schedules; prepare and submit draft agency schedules; review and sign records disposition authorizations; disseminate records management information to agency personnel; supervise records inventories; identify essential operating records for inclusion in the agency Continuity of Operations Plan; coordinate the implementation of records technology; coordinate transfers of inactive records to the

State Records Center or other approved public records storage facilities; coordinate transfers of permanent/archival records to the State Archives; identify areas of need and arrange for staff training; and maintain control files of records retention schedules, disposition authorizations, and records transfers.

Anticipated Use of the SDPR: ability to submit digital archival records for ingest, download a copy of their agency's records for the business needs of record custodians or to fulfill Freedom of Information Act (FOIA) requests, and run reports on metrics pertaining to their records.

Expected Technical Skills: Familiarity with Microsoft Office applications, records management software, and software for preparing and transferring records to the State Archives.

Assistant Records Management Liaison Officer (ARMLO) - An agency head may designate appropriate individuals to serve as Assistant RMLOs. Typical duties and responsibilities for the ARMLO position include: assist the RMLO with implementing and maintaining the agency records management program; assist in the preparation of draft agency records retention schedules; assist with reviewing disposition authorizations and resolving any questions or issues with the records custodian prior to submitting the form to the RMLO for approval; assist in distributing records management information within the agency; and oversee transfers of inactive records approved by the RMLO to the State Records Center or other approved public records storage facilities.

Anticipated Use of the SDPR: ability to submit digital archival records for ingest, download a copy of their agency's records for the business needs of record custodians or to fulfill FOIA requests, and run reports on metrics pertaining to their records.

Expected Technical Skills: Familiarity with Microsoft Office applications, records management software, and software for preparing and transferring records to the State Archives.

State Archivist (SA) - The State Archivist is accountable for supervising all activities relating to the acquisition, organization of, and accessibility to, archival and manuscript materials. Typical duties and responsibilities include: planning, coordinating, and overseeing archival projects; surveying records of Connecticut State agencies to determine their potential value to State Archives; appraising records and other materials offered or available for acquisition for their archival value and accessions those determined to be appropriate for State Archives; preparing or supervising preparation by others of guides, registers, calendars, lists and indexes to archival and manuscript materials; and preparing or assisting in the preparation of exhibits based upon items from the State Archives.

Anticipated Use of the SDPR: oversight of and sign off on records transfers; and ability to run reports as necessary.

Expected Technical Skills: Familiarity with Microsoft Office applications, records management software, software for preparing and transferring records to the State Archives and the CTDA.

Assistant State Archivist (ASA) - responsibilities of the Assistant State Archivist include appraising materials to determine archival value and suitability for inclusion in the State Archives; performs accessioning of records and authority work on finding aids and digital collections for archival materials; developing and maintaining a sustainable program for the long-term preservation of

permanent born-digital and digitized materials including related policies, procedures, and workflows; appraising, transferring, processing, describing, and providing access to digital records and manuscript materials; and collaborating with records creators, records management, information technology, Connecticut Digital Archive (CTDA) staff, and donors on the long term preservation of public records and manuscript materials.

Anticipated Use of the SDPR: administer the day to day operations of the SPDR including reviewing submissions of digital archival records transferred by state agencies to ensure the State Archives received the correct records and metadata; determine, develop, and implement program policies, procedures, processes, standards, and manuals in accordance with program objectives and goals; onboard state agencies to allow them to submit records to the system (i.e., through a web based platform or across cloud); manage the records in the system such as setting up an area for each state agency, ingesting records submitted on physical storage media (i.e., external hard drives), and adding or removing RMLOs, ARMLOs, RMA's and Compliance Officers from the system; add or correct metadata submitted with records as necessary; serve as a liaison with the appropriate DAS BITS teams; and provide complex reference services to state agency RMLOs and ARMLOs to respond to questions.

Expected Technical Skills: Familiarity with Microsoft Office applications, records management software, archival collection management systems (i.e., ArchivesSpace), software for preparing and transferring records to the State Archives and the CTDA.

IT staff from Department of Administrative Services' Bureau of Information Technology Solutions (DAS BITS) – responsibilities include providing technical support for systems/applications/solutions employed by the Connecticut State Library during all phases of the system development lifecycle (SDLC).

Anticipated Use of the SDPR: provide support to ensure the system is operating as expected, reduce any downtime, and provide enhancements as necessary.

Expected Technical Skills: Experienced in all phases of the SDLC.

Compliance Officers - The Compliance Officers from the Offices of the Attorney General, State Auditor, State Comptroller, and Office of Policy and Management (OPM) will work with the agency RMLO, Public Records Administrator, and the State Archivist to conduct research (i.e., be able to run available reports) and monitor content for governance and risk compliance. For example, an auditor could ask the State Archives to show that an agency transferred a particular record to the SDPR. Failure to provide such proof could result in an audit write-up.

Anticipated Use of the SDPR: provide compliance oversight, run reports on available data such as formats of records preserved, or to compare random samples of records requested against searching the system metadata.

Expected Technical Skills: Familiarity with Microsoft Office applications.

Appendix D. Specific, Measurable, Achievable, Relevant, Time-bound (S.M.A.R.T.) criteria

S.M.A.R.T. Criteria:

Broad Goal:

Make Confidential Digital Records Preservation Happen

Specific Goal:

Achieve and maintain full compliance with security and preservation requirements for confidential permanent archival digital records transferred from Connecticut executive branch agencies to the State Archives.

S.M.A.R.T. Goal Statement:

Achieve full compliance with all state and federal security requirements for preserving confidential permanent archival digital records, including criminal justice information (CJI), personally identifiable information (PII), and personal health information (PHI), within 12 months of implementing a compliant digital preservation repository system by conducting regular security audits, performing fixity checks, and training staff on compliance and security protocols. Progress will be measured by aiming for zero security breaches, 100% compliance rate, transfer records from one permanent archival record series, 100% fixity check success rate, and 3% increase in confidential permanent archival digital records transferred from state agencies to the State Archives over each fiscal year.

Specific

What will be accomplished?

Implementation of a secure digital preservation repository system that complies with all state and federal security requirements for storing confidential digital archival records, including criminal justice information (CJI), personally identifiable information (PII), and personal health information (PHI).

Who is responsible?

The Connecticut State Library, specifically State Archives staff; executive branch state agency Records Management Liaison Officers (RMLOs), and Department of Administrative Services (DAS) Bureau of Information Technology Solutions (BITS) staff.

What steps will be taken to achieve this?

- Assess current digital preservation repository systems and identify gaps.
- Secure resources including funding and personnel.
- Plan, select and implement a compliant secure digital preservation repository system.

- Conduct regular security audits and fixity checks.
- Provide training for staff on compliance and security protocols.
- Provide knowledge transfer sessions and training for BITS resources to support the system.

Measurable

How will progress be measured?

- Number of security breaches (aiming for zero).
- Percentage compliance with state and federal security requirements (aiming for 100%).
- Number of confidential archival digital records transferred and ingested into the preservation system (aiming for records from a minimum of one permanent archival records retention series).
- Fixity check success rate (aiming for 100%).
- Percentage increase in confidential archival digital records transferred over each fiscal year (aiming for 3%).

Achievable

Is the goal realistic and attainable?

Yes, with proper assessment, selection of the right preservation system, regular audits, and staff training, achieving full compliance is realistic.

Do we have the resources and capabilities?

Yes, with the involvement of dedicated personnel, appropriate budget resources, and access to necessary technologies and training programs.

Relevant

Does this goal align with broader objectives?

Yes, it directly supports the objective of preserving confidential digital records securely and in compliance with legal standards, ensuring the protection of sensitive information in and accessibility to archival digital records for hundreds of years.

Why is it important?

It is crucial for maintaining the integrity and confidentiality of state government archival records, avoiding legal penalties, and fostering and maintaining public trust.

Time-bound

What is the deadline for achieving this goal?

Achieve full compliance within 2 years of implementing a secure digital preservation repository system.

Are there any milestones along the way?

- Initial assessment and gap analysis within the first 6 months.
- Selection and implementation of the new system within 12-18 months.
- Staff training and initial audit within 18-24 months.
- Final compliance check and adjustment period by the end of 24 months.

Appendix E. Questions concerning vendors from the Cloud Services Questionnaire from DAS BITS Enterprise Architecture Division.

The questions listed below are questions that the Connecticut State Library will have to answer about the solution chosen for the SDPR. The questions presented here are for informational purposes and do not need to be answered in your response to this RFI. These questions will only need to be answered when a solution has been selected in response to an RFP. NOTE: These questions will not replace/supersede the more rigorous requirements in this RFI, such as those found in the CJIS Security policy.

- Is secure (authenticated) access required? If so, how is user authentication and authorization handled? Who is responsible for administering end-user security? [We strongly recommend SaaS solutions procured be capable of authenticating against States' IAM platforms using modern protocols like SAML or OIDC]
- What mechanisms does the contractor offer, if any, to assist the state in migrating data off their solution in the event that your agency desires to terminate your relationship with the contractor?
- Will the contractor's solution need to send outbound emails in the context of any business transactions? This would mean that any business emails sent by the solution would use the state's "@ct.gov" email domain.
- Does the contractor run their own data center or do they rely on the use of a separate cloud services provider (e.g., Amazon Web services, Microsoft Azure, etc.)?
- Does the solution require any contractor appliances and/or software to be installed on state or agency systems? If so, please describe.
- Does your solution require multifactor authentication? If so, can the contractor support that requirement?
- How does the contractor secure and protect state data?
- What is the contractor's obligation to the state if they miss their service levels or availability commitments?
- Where will the data reside, geographically? This includes not only any primary data centers, but any other data centers that may provide replication and/or failover support.
- How does the contractor communicate to their customers on outages?
- How does the contractor handle breach identification and notification (C.G.S § 4e-70)?
- If the contractor does not provide service resiliency by means of physically separate data centers or failover environments, how does the contractor meet your agency's business continuity goals (availability, time to recovery, etc.) for the solution you seek to use?
- Does the contractor allow employees and/or subcontractors to access customer data? If so, in what cases is this allowed and how does the contractor monitor this activity for appropriateness?

- How does the contractor communicate to their customers on routine maintenance that may impact availability?