SW SOCIALWORK
LICENSURE COMPACT

Request for Proposal (RFP)
Centralized Data System for Social Work Licensure Compact

Release Date: April 22, 2025
Proposal Due Date: June 16, 2025

1. Overview & Purpose

The Social Work Licensure Compact Commission (the “Commission”) seeks proposals for the design, development, and maintenance of a **Centralized Data System** to enable secure exchange of licensure and disciplinary information among Compact member states. This system will support multistate licensure, regulatory oversight, and real-time information sharing across participating states.

This system must:

- Facilitate **real-time licensure verification** and disciplinary tracking.
- Provide secure, seamless integration with state licensing systems.
- Comply with state and federal data security standards (e.g., FedRAMP, NIST 800-53, SOC 2).
- Be scalable and flexible to support new member states.

This RFP follows an earlier RFI (completed March 2025). The selected vendor will collaborate with the Commission and with the administrative support of the Council on State Governments (CSG) to implement the solution based on the Compact’s business and regulatory requirements.

Note: For detailed background on the Home State vs. Remote State model, required data flows, and disciplinary processes, please see **Appendix A: Data System Overview**.

2. Scope of Work

2.1 Functional Requirements

1. **Licensure Verification & Tracking**
    - A searchable, centralized database with **real-time** or near-real-time updates on active/inactive licenses and disciplinary actions.
    - Distinction between the Home State license (multistate) and Remote State actions (impacting only that remote state).
2. **Supervision Proof & Tracking**
    - Ability to monitor supervision requirements for different licensure categories, with the possibility of capturing state-specific supervision rules.
3. **Interstate Data Sharing**

   - Secure **API-based** and **batch** integration options to accommodate each member state's technical capabilities.
   - Notification system for all relevant licensing or disciplinary updates.
4. **Disciplinary Action Sharing**
   - Timely, automated updates on enforcement actions to **all** Compact member states.
   - Must differentiate whether the discipline originates from the Home State or a Remote State.
5. **Multi-State License Management**
   - Support issuing and tracking the **multistate** license, with centralized status checks for any subsequent changes.

2.2 Security & Compliance

- **Data Encryption:** Protect data (in transit & at rest) using industry standards.
- **User Access Controls:** Role-based security, multi-factor authentication (MFA), and auditing for compliance.
- **Regulatory Compliance:** Must adhere to FedRAMP, NIST 800-53, SOC 2, and other applicable standards.
- **Disaster Recovery & Business Continuity:** The Vendor must provide a documented Disaster Recovery (DR) plan and Business Continuity (BC) strategy, specifying how the system will meet the following objectives:
- **Recovery Time Objective (RTO):** 4 hours – The maximum duration that the system can be offline following an incident.
- **Recovery Point Objective (RPO):** 30 minutes – The maximum acceptable amount of data loss measured in time.
- The **DR/BC** plan must include:
   - Procedures for data backup and restoration.
   - Redundant infrastructure setup (e.g., geo-redundancy, failover procedures).
   - Regular testing schedules for verifying DR readiness.
   - Escalation and notification protocols.
- **Data Sovereignty:** All data, including backups and disaster recovery locations, must remain within the geographic boundaries of the United States at all times to comply with state and federal regulations.
- **Privacy and Confidentiality Compliance:** The vendor must comply with applicable privacy regulations including, but not limited to, HIPAA, and other state-specific privacy statutes. Vendors must explicitly manage sensitive personal information and protected health information (PHI) in full compliance with these standards.
- **Third-Party and Open-Source Software:** Vendors must disclose all third-party and open-source software dependencies explicitly. Use of non-open-source software must receive prior written approval from the Commission, and vendors must ensure compliance with the license agreements of all incorporated software components.

2.3 Technical & Integration Requirements

1. **Cloud-Based Deployment**

    - System hosted in Azure GovCloud (or a comparable secure environment meeting government standards).
2. **Integration Flexibility**
    - **API-first** design for real-time data exchange.
    - Batch file processing for states not ready for APIs.
3. **Interoperability**
    - Compatibility with a variety of state licensing systems, avoiding duplication of existing solutions or data.
4. **User Interface & Accessibility**
    - Intuitive, modern UI design.
    - ADA-compliant accessibility.
    - Multi-device compatibility (desktop, tablet, mobile).
5. **Reporting or analytics**
    - Reports on the number of new licenses, disciplinary actions, etc.

2.4 Implementation & Support

1. **Deployment Phases**
    - **Design & Development**
    - **Testing & Data Migration**
    - **State Integrations**
    - **Go-Live & Post-Launch Support**
2. **Training & Documentation**
    - Vendor to provide user training materials, online webinars, and a helpdesk or ticketing system.
3. **Ongoing Support & Maintenance**
    - SLA-driven support with specified response times.
    - Ongoing performance monitoring and security patching.
    - Regular updates (including any required compliance or feature enhancements).

   The vendor must provide year-round support under a formal SLA. Response time for critical issues must be 1 hour or less, with resolution within 8 hours. Additional details are set forth in **Appendix B: Service Level Agreement Requirements.**

3. Proposal Submission Requirements

3.1 Company Profile & Experience (10 Points)

- Cross reference to the RFI is acceptable so as not to repeat information.
- Brief overview of the company, including years in operation.
- Experience with government or multi-state regulatory systems.
- Previous relevant project examples (licensure or enforcement systems).

3.2 Technical Capabilities & Solution (25 Points)

- Proposed system architecture (cloud, hybrid, etc.).
- Integration approach (APIs, batch), including example workflows.
- Security & compliance measures (encryption, access controls, DR).
- **Suggested**: Provide a sample or reference architecture diagram if possible.

3.3 Functionality & Features (20 Points)

- Strategy for licensure tracking, disciplinary data, and supervision monitoring.
- Analytics and reporting capabilities.
- User experience and accessibility compliance.

3.4 Implementation Approach (20 Points)

- Proposed deployment timeline (development, testing, go-live milestones).
- Project management methodology (Agile, waterfall, or hybrid).
- Training & user documentation plan.

3.5 Cost Structure & Pricing Model (20 Points)

- Please provide a line-item budget in a separate document, including initial implementation costs, licensing fees, and ongoing support and maintenance fees.
- Vendors must provide a detailed, line-item cost proposal broken down by project phase, at minimum addressing the following categories:

1. **Phase 1: Design & Development (3-6 months)**
    - Project Management & Planning:
        - Personnel roles and hours (e.g., Project Manager, Business Analyst)
        - Associated costs or overhead.
    - System Architecture & Configuration:
        - Software development labor (Senior Developer, Mid-Level Developer, etc.)
        - Configuration, customization, or integration tasks
    - Initial Testing & Data Migration
        - Testing tools, QA personnel, data migration procedures, etc.
    - Deliverables (e.g., prototypes, sandbox, pilot environment)
2. **Phase 2: Production Rollout & Final Integration (3 months)**
    - Full Production Go-Live:
        - Final testing, security hardening, performance tuning
    - Additional Integrations with State Systems:
        - APIs, batch file processes, or other integration labor
    - Training & Documentation:
        - Development of training materials (online webinars, user guides)
        - Live or virtual training sessions for state administrators and staff
    - Deliverables (e.g., final production environment, official launch)
3. **Phase 3: Long-Term Maintenance & Support**
    - Maintenance & Patching:
        - Recurring monthly or annual maintenance fees, inclusive of security updates
    - SLA-Driven Support:
        - Helpdesk or ticketing system costs
        - Defined response times for critical, high, medium, and low priority issues.
    - Enhancement & Change Requests:
        - Optional hourly rates or bundles of hours for new feature requests or expansions

- Ongoing Hosting & Licensing Fees (If Applicable):
    - Any cloud hosting charges, third-party licensing, or subscription-based elements
- Renewal Options:
    - Pricing for additional years of support or optional extension phases

Notes on Cost Proposal Formatting:

- Provide a summary table for each phase, showing total cost and subtotals for major categories (personnel, software, data storage, training, travel, etc.).
- Include labor rates (e.g., hourly or FTE costs) for each key role, along with an estimate of total hours or days allocated.
- Clearly indicate which items are one-time costs vs. recurring (annual or monthly).
- If any discounts, rebates, or cost-sharing apply across phases, specify them in detail.

Optional: You may also provide an alternative pricing approach if you believe it better reflects your solution or offers additional value. If doing so, please still include the required line-item budget to facilitate comparison among proposals.

3.6 References & Case Studies (5 Points)

- Cross reference to the RFI is acceptable so as not to repeat information.
- At least two references from similar licensing or regulatory system projects.
- Case studies that highlight successful large-scale system implementations.

4. Proposal Submission Criteria

- **Format:** PDF or Microsoft Word
- **Length:** Maximum 20 pages (excluding appendices detailed diagrams, comprehensive cost breakdowns, SLA documentation, relevant certifications, and extended references as clearly labeled appendices.)
- **Deadline:** June 16, 2025
- **Submission Method:** Email **kbison@csg.org** with the subject line “Proposal: Social Work Compact Data System”
- **Public Records and Confidentiality:** Vendors should clearly mark any proprietary or confidential information at the time of submission. All responses are subject to public records laws.

5. Contract Terms & Conditions

5.1 Period of Performance:

- **Phase 1**: 3-6-month design, initial deployment, and pilot,
- **Phase 2**: 3-month full production and maintenance
- **Phase 3**: Long term maintenance**.** Phase 3 will begin upon successful completion of Phase 2 and covers long-term maintenance and support for an agreed-upon duration up to 5 years. Additional renewals or extensions may be negotiated if both parties agree to response times for critical issues, security updates, patches, user training refreshers, additional feature

requests (as approved by the Commission), helpdesk support & issue resolution, etc.

5.2 Ownership & Data Rights: All software, data, and documentation developed must be owned by the Social Work Compact Commission.

5.2 Foreign Government Disclosure: Vendors must disclose any foreign government interests in their ownership or operations.

5.6 Public Records Compliance: Proposals are subject to public records laws.

5.7 Payment Tied to Milestones:

- Vendor payments will be clearly tied to specific deliverables and project milestones. Retainage of up to 10% may be withheld from payments until satisfactory completion and acceptance of each milestone.

5.8 Termination:

- The Commission reserves the right to terminate the contract for convenience with thirty (30) days written notice.
- The Commission reserves the right to terminate the contract immediately for cause, including but not limited to persistent SLA violations, security breaches, or non-performance of key obligations. Upon termination for cause, the vendor may be required to reimburse the Commission for damages incurred.

5.9 Indemnification and Liability:

- The Vendor agrees to indemnify, defend, and hold harmless the Social Work Licensure Compact Commission ("Commission"), its officers, directors, employees, agents, representatives, and member states, from and against any and all claims, demands, suits, liabilities, losses, damages, penalties, fines, judgments, awards, settlements, costs, expenses, and attorney fees arising from or related to:

1. Data Breach and Security Violations:
   Unauthorized disclosure, breach, loss, or compromise of data, including personally identifiable information (PII) and protected health information (PHI), due to the Vendor's negligence or failure to adhere to the specified security standards, regulatory requirements, or contractual obligations.
2. Intellectual Property Rights:
   Allegations or claims that the system, software, applications, documentation, or other deliverables provided by the Vendor infringe upon any third-party intellectual property rights, including copyrights, trademarks, trade secrets, or patents.
3. Privacy and Compliance Violations:
   Failure of the Vendor to comply with applicable federal, state, and local privacy laws and regulations, including but not limited to HIPAA, FedRAMP, SOC 2, and state-specific privacy and data protection statutes.
4. Negligent Acts and Omissions:
   Negligent acts, errors, omissions, misconduct, or wrongful acts by the Vendor, its employees, agents, subcontractors, or representatives in the performance of services under this contract.
5. Regulatory Non-compliance:
   Vendor's non-compliance with any federal, state, or local laws, regulations, or

licensing requirements applicable to the operation and maintenance of the Centralized Data System or the services provided herein.

6. Third-Party Claims:
   Claims from third parties arising from the Vendor's obligations under this agreement, including disputes with subcontractors, suppliers, or other entities engaged by the Vendor.

Procedure for Indemnification:

- Notification:
  The Commission will promptly notify the Vendor in writing of any claim or legal action for which it seeks indemnification.
- Control and Cooperation:
  The Vendor shall have sole control of the defense and settlement of any claim, provided that the Vendor shall not settle any claim without the Commission's prior written consent (not to be unreasonably withheld), particularly if the settlement involves admission of fault or imposes obligations upon the Commission.
- Costs:
  All reasonable costs incurred by the Commission in cooperating with the Vendor's defense of any claim, including legal costs, shall be reimbursed by the Vendor.

Insurance Requirements:
In support of the above indemnification obligations, the Vendor shall maintain adequate insurance coverage throughout the contract period, including but not limited to:

- Professional Liability (Errors & Omissions) Insurance.
- Cyber Liability and Data Breach Insurance.
- General Liability Insurance.

The Vendor will provide proof of such insurance coverage prior to contract execution and upon the Commission's request at any time during the term of the contract.

6. Timeline & Next Steps

- **RFP Release Date:** April 16, 2025
- **Deadline for Vendor Questions:** May 21, 2025
- **Proposal Submission Deadline:** June 16, 2025
- **Final Selection & Contract Award:** Aug 2025
- **Project Kickoff:** 2-4 weeks after contract award

Note: Written vendor questions will be answered and published on the Commission's website to ensure equal access to all respondents.

7. Contact Information

For questions regarding this RFP, please contact:
Kaitlyn Bison
Interim Executive Director
kbison@csg.org

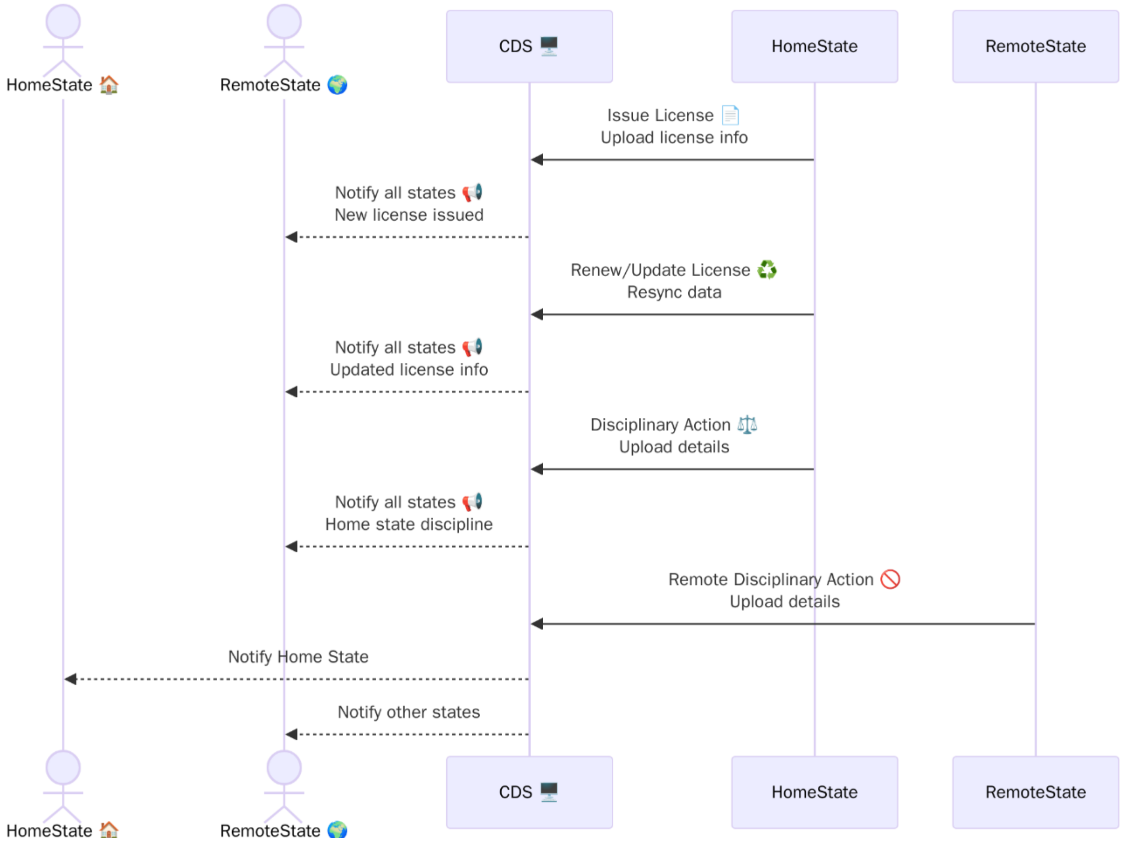
Appendix A: Data System Overview

1. Introduction

The Social Work Licensure Compact expands the mobility of social workers by recognizing one Home State license, which grants practice privileges in multiple Remote States. Because each state may initiate or update license records and disciplinary actions, a centralized data system is critical for real-time information sharing and notification. This document outlines key processes—license issuance, renewal, and disciplinary actions—along with the data flows, notifications, and technical requirements needed for a robust, secure, and user-friendly solution.

2. High-Level Process Flow Diagram

Below is a simplified view of how states, licenses, and disciplinary actions interact with the Central Data System:



Key Steps:

1. Home State issues the multistate license and uploads data to the Central Data System.
2. Central Data System notifies all member states of the new license or any status changes. (Dashboard for state administrators; email option)
3. Home State updates or renews license information and re-syncs with Central Data System.
4. If there is a Home State disciplinary action, it is immediately uploaded, triggering notifications across all states.
5. All other states consult the Central Data System to verify or respond to the updated license status.
6. If a Remote State disciplines a licensee (applies restrictions in that state only), it also uploads details to the Central Data System, which alerts all states of the change.

3. License Issuance Under the Social Work Licensure Compact

3.1 Home State Issuance

- Each licensee holds a “home state” multistate license, granted by that state’s statutory and regulatory requirements.
- Once issued, the licensee may practice in all other Compact Member States (referred to as “remote states”).
- If the Home State license is invalidated (restricted, revoked, suspended), the licensee’s privileges in other member states are automatically impacted.
- License types -Bachelor, Master, Advanced Generalist, Clinica

3.2 Remote State

- Each Remote State verifies the licensee’s home state license status via the Central Data System.
- Remote States do not issue a separate license; they accept the multistate license for practice privileges.

3.3 Central Data System Upload & Verification

- As soon as the Home State issues or updates a license, it synchronizes this information with the Central Data System.
- Remote States rely on these uploads to confirm license status (active, expired, suspended, revoked, etc.).
- Vendors must support real-time or near-real-time data uploads and display.

3.4 License Renewal & Status Changes

- The Home State handles license renewals and updates expiration dates or other status changes.
- The Central Data System notifies all Remote States if a license lapses or a licensee becomes ineligible.

3.5 Role of the Central Data System in Issuance

- Stores and displays the definitive record of each licensee’s Home State License and any adverse actions.
- Facilitates quick lookups to confirm if a Home State license is unencumbered or if a Remote State has imposed an action.
- Maintains an audit trail of all changes (who, when, and what was changed).

4. Adverse Action & Notification Requirements

Adverse actions can originate from either the Home State (affecting practice in all member states) or a Remote State (affecting practice in that remote state only). All disciplinary data must be centrally stored, with notifications to all states in real-time or near-real-time.

4.1 Home State Discipline

- The Home State is the primary licensing authority.
- Disciplinary action (e.g., suspension, revocation) in the Home State may affect the licensee's ability to practice Compact-wide.
- Must be uploaded to the Central Data System immediately so each member state is informed.

4.2 Remote State Discipline

- A Remote State may restrict or prohibit practice within its jurisdiction alone.
- Remote State actions do not automatically affect other states unless the Home State or other Remote States also impose additional measures.
- All such Remote State actions must be uploaded to the Central Data System for transparency and potential follow-up.

4.3 Clarification on Disciplinary Actions:

- Vendors must clearly demonstrate how their systems will categorize, report, and manage disciplinary actions originating from Home States versus Remote States, ensuring legal clarity and proper notification across all member states.

5. Central Data System Functionality & Notifications

5.1 Data Upload and Verification

- Each state (Home or Remote) uploads disciplinary details, specifying whether the action comes from the Home State or a Remote State.
- Supports both manual entry and automated transfers (APIs, batch file uploads) to match each state's technological capabilities.

5.2 Real-Time or Near-Real-Time Notice

- Upon entry of a disciplinary action, the system automatically notifies all member states with:
  - Licensee identifying information.
  - Nature of the discipline (Home vs. Remote)
  - Effective dates or terms/conditions
- Notifications can be made via email, dashboard alerts, or other secure channels.

5.3 License Record Updates

- The system must visually and programmatically distinguish between Home State actions (impacting the core license) and Remote State actions (impacting only that one state).
- Must display a comprehensive history of actions, including the status or outcome (e.g., suspension completed, appeal in progress).

5.4 Follow-Up Actions by Other States

- The system should enable any state to pursue reciprocal or additional actions if warranted.

- States can log their decisions (e.g., “Reciprocal suspension initiated,” “No additional action,” etc.) and track subsequent investigations.

5.5 Reporting & Audit Trails

- Timestamps and user IDs are stored for each disciplinary action and notification.
- Robust reporting allows member states, commissioners, compact authorized personnel) to run on-demand or scheduled reports of license data and disciplinary events.
- Provide a secure portal for licensees to view their records and a public portal for license lookup, both fully auditable.

6. Desired Outcomes & Vendor Expectations

1. **Clear Data Structures**
   - Outline how the system will store, tag, and display Home vs. Remote State disciplinary information in one repository.
2. **Automated Alerts & Workflows**
   - Detail how real-time or near-real-time alerts are triggered for all states upon new or updated records.
3. **Role-Based Access & Security**
   - Demonstrate how **authorized personnel** can add, edit, or view data, with logging for compliance and data integrity.
   - Role based display control of licensee and disciplinary information.
4. **State-by-State Configuration**
   - Handle data uploads via API or CSV to accommodate different technology stacks.
   - Ensure secure communications for uploading licensing data and adverse actions.
   - Provide redundant backups, a disaster recovery plan, and minimal downtime.

Notes

This flow ensures each state understands when it must contribute data, how it is shared in real-time, and what steps others can take based on added information. By combining streamlined license issuance with a clear approach to disciplinary actions, vendors can design a centralized data system that is secure, scalable, and user-friendly for all Compact Member States.

Appendix B: Service Level Agreement (SLA)

Between:

- Social Work Licensure Compact Commission ("the Commission")
- [Vendor Name] ("the Vendor")

1. Purpose & Scope

This Service Level Agreement (SLA) outlines the performance metrics, incident classifications, and response times the Vendor must meet in delivering and maintaining the Centralized Data System for multistate social work licensure. It applies to both implementation and ongoing maintenance phases.

2. Definitions

- **System**: The Centralized Data System for Social Work Licensure, including software, servers, databases, APIs, and other related components under the Vendor's control.
- **Incident**: Any unplanned event that disrupts or diminishes System performance or availability.
- **Resolution**: A permanent fix or workaround restoring System functionality to acceptable levels.
- **Response Time**: Time from when the Vendor is notified of an Incident to the time the Vendor begins active remediation.
- **RTO (Recovery Time Objective)**: The maximum allowed downtime following a major outage.
- **RPO (Recovery Point Objective)**: The maximum acceptable data loss measured in time.

3. Service Availability

1. Uptime Goal: The Vendor must maintain at least 99.9% system uptime on a 24/7/365 basis, excluding scheduled maintenance.
2. Scheduled Maintenance:
   - The Vendor provides at least five business days' notice prior to scheduled downtime.
   - Maintenance is scheduled during low-usage periods, as jointly agreed upon.

4. Incident Priority Levels

Incidents are classified according to impact and urgency:

Priority	Description	Examples
P1	Critical – System-wide outage or severe impact.	Complete system failure, major security breach, critical data corruption.
P2	High – Major functionality impaired.	Key modules down, severe performance degradation.
P3	Medium – Partial functionality or minor issues.	Certain features are not working, intermittent slowdowns.
P4	Low – Cosmetic or non-urgent.	Minor UI bugs, small enhancements, text edits.

5. Response & Resolution Times

Priority	Response Time	Resolution Time
P1	Within 1 hour	8 hours (or workable workaround)
P2	Within 2 hours	24 hours
P3	Within eight business hours	Five business days
P4	Within two business days	Next scheduled update or as agreed

- Response Time: Time to acknowledge the incident and begin investigating.
- Resolution Time: Time to permanently fix or provide a stable workaround.

6. Disaster Recovery Objectives

- RTO: 4 hours – System must be restored following a major incident (data center failure, etc.).
- RPO: 30 minutes – Maximum data loss in the event of a disaster.

The Vendor's DR plan must explain how these objectives will be met, including backups, redundancy, and restoration methods.

7. Monitoring & Reporting

1. Incident Tracking: The Vendor maintains a ticketing system to log and track incidents.
2. Monthly SLA Report: Summaries of uptime, incidents, resolution times, and any DR testing must be provided to the Commission monthly.

8. Escalation Procedures

Should the Vendor fail to meet SLA metrics or if repeated issues occur:

1. Escalation to Vendor's Technical Lead
2. Escalation to Vendor's Project Manager
3. Involvement of Vendor's Executive Sponsor and the Commission's Primary Contact
4. Potential contractual remedies if unresolved

9. Remedies & Penalties

1. Chronic SLA Violations: Failing three or more times per quarter to meet P1/P2 metrics may result in:
    - Service credits (e.g., refunding a portion of monthly fees).
    - A written remediation plan submitted to the Commission.
2. Prolonged Outages: Excessive downtime or breaches of RTO/RPO requirements can lead to:
    - Contract renegotiation or termination, per the primary Agreement.

10. Maintenance Windows

- Scheduled Maintenance: Announced at least five business days in advance, timed for minimal user disruption.
- Emergency Maintenance: Performed with immediate notice if critical to protect data/system integrity.

11. Change Management

- Major Changes require Commission approval, along with updated documentation.
- Minor Fixes do not require prior approval but must be logged in the Vendor's change management system.

12. Term & Review

- This SLA remains in effect from system go-live through the duration of the Master Contract or until otherwise terminated.
- Annual review or mutual agreement ensures it stays aligned with operational needs and regulatory changes.
- 90 day notice of termination by either party.

13 Financial Remedies for SLA Violations

1. Service Credits for SLA Non-Compliance

In the event the Vendor fails to meet the agreed-upon SLA metrics outlined in Appendix B, the following service credit structure shall apply:

Incident Severity	**Occurrence per Quarter**	**Service Credit (as % of monthly fees)**
Critical (P1)	1st Violation	10%
	2nd Violation	20%
	3rd and Subsequent Violations	30%
High (P2)	1st Violation	5%
	2nd Violation	10%
	3rd and Subsequent Violations	15%

Note:

- Service credits shall be applied as a refund or deducted as a credit from future payments at the Commission's discretion.
- Service credits will not exceed 30% of the Vendor's monthly invoiced fee in any given month.

2. Persistent Non-Compliance Penalties

Should the Vendor consistently fail to meet SLA obligations (defined as three or more Critical or High-priority SLA violations within two consecutive months), the Commission may, at its sole discretion, invoke one or more of the following remedies:

- Require submission of a written remediation plan within 15 days outlining corrective actions.
- Increase the service credit penalties to a maximum of 50% per month for any subsequent SLA violations until compliance is restored.
- Withhold milestone payments or retain a portion of fees (up to 10%) until compliance is verified through documented SLA adherence over a period of at least 90 days.

3. Severe Non-Compliance

Severe non-compliance, including but not limited to:

- System downtime exceeding double the agreed-upon Recovery Time Objective (RTO) without adequate communication or mitigation efforts.
- Security breach due to Vendor's negligence or failure to adhere to security requirements.

In such cases, the Commission reserves the right to:

- Withhold payments equivalent to up to one month's service fees.

- Seek reimbursement for actual, documented damages incurred as a direct result of the Vendor's failure.
- Immediately terminate the contract for cause with no further obligation for payment beyond services satisfactorily delivered and accepted up to the termination date.

14. Signatures

____
Vendor Representative
Title, Organization
Date

____
Commission Representative
Title, Organization
Date

Disclaimer on SLA Terms:
The SLA set forth in Appendix B represents the Commission's desired service levels and response metrics. These terms may be revised or negotiated based on vendor proposals, state regulatory requirements, or mutual agreement during contract negotiations. The final SLA will be incorporated into the executed contract to reflect any updates or changes agreed upon by both the Commission and the selected vendor.