South Dakota Secretary of State

Monae L. Johnson
Secretary of State

Thomas J. Deadrick
Deputy Secretary of State

December 11, 2025

Dear Chair Howard and Members of GOAC,

The list of questions for which follow up was agreed to during the most recent GOAC meeting on November 13th, 2025, is provided below:

1. **What recourse, if any, is provided in the contract should KNOWiNK fail to deliver a working and complete final product?**

   Under the contract, the State has multiple layers of recourse if KNOWiNK fails to deliver a working, complete final product. First, 15% of each Deliverable invoice—approximately $675,000 total—is contractually withheld until the System successfully goes live, so the State is not obligated to release full payment unless and until an operational system is accepted.

   Additionally, KNOWiNK provides system warranties requiring that, upon Acceptance and throughout the Warranty Period, the System conforms to the Contract, Specifications, Performance Criteria, Documentation, and SOW and be free from defects in material and workmanship. During the Warranty Period, KNOWiNK must, at no extra cost, make any necessary improvements to maintain ongoing system reliability and ensure the System conforms if issues arise. If KNOWiNK's failure to deliver constitutes a Breach, the Secretary of State (SOS) may issue a written notice, set a remedy period, and require KNOWiNK to submit and execute a corrective action plan (CAP). The SOS may withhold payments related to the breach.

   Additionally, the Secretary of State may exercise setoff rights to withhold and apply amounts to cover costs and expenses (including overtime) incurred due to KNOWiNK's unexcused breach. Collectively, these provisions provide the Secretary of State with financial leverage, a structured remediation process, and ultimately the right to terminate the Contract and recover certain costs if KNOWiNK fails to deliver the agreed-upon, working, and complete final product.

2. **Who owns KNOWiNK, including minority shareholders?**

   Managing Director Scott Leiendecker leads KNOWiNK, LLC.
   Ownership is split between KNOWCo Inc. (which is 100% owned by Scott Leiendecker) holding 65%, and HermCo-Invest (also known as Hermann Capital Management), holding the remaining 35%. KNOWiNK's headquarters are located in St. Louis, Missouri.

3. **The discussion around the continual testing to ensure the security of the system led to a question what kind of testing is planned.**

   Will this be more of an ongoing scanning process, or a series of tests conducted by individuals over time, or both?

   Under the BIT Required IT Contract Terms, the System's security is supported by both State-directed independent oversight and KNOWiNK's ongoing security program. The contract requires the Contractor to participate in audits performed by third-party security researchers identified by the South Dakota Secretary of State's Office and South Dakota BIT for System deployment. These independent reviews give the State direct assurance that security controls, configurations, and processes meet State and BIT expectations.

   In addition, KNOWiNK is contractually obligated to maintain a rigorous, ongoing security posture, which includes:

- Regular vulnerability management across operating systems, applications, and network configurations, with any identified vulnerabilities remediated promptly at the Contractor's expense.
- Periodic internal and external penetration testing of the voter registration system to validate that defenses are effective from both outside and inside the environment.
- Secure development practices, including integrated code scanning and routine review of third-party components for known vulnerabilities.
- Comprehensive audit logging and monitoring, with a full audit trail for user activity and voter-record access, and the ability to search, filter, and review changes by authorized State users.
- Alignment with recognized security frameworks, as well as adherence to the Secretary of State's IT Security Policy and Standards. Together, the third-party audits directed by SD SOS and SD BIT, combined with KNOWiNK's ongoing vulnerability management, penetration testing, monitoring, and policy compliance, create a continuous and repeatable security testing and oversight regime for the System.

4. **Sen. Howard asked a question (at the 5:47 timestamp in the recording) about who is included in the team of cloud providers and allies supporting this platform?**
5. **There will some kind of an audit framework. Who does the audit of the equipment, and how does that work? (5:48 timestamp)**

   In response to your questions 4 & 5 regarding SDVotes and its security posture, KNOWiNK is dedicated to providing clear, transparent assurance about how South Dakota's SDVotes infrastructure is protected, who has access, and how that access is governed.

   SDVotes is hosted exclusively on Microsoft's Azure Government Cloud (GCC High), a secure environment purpose-built for U.S. government workloads and aligned with stringent federal standards. This environment allows us to leverage advanced security tools for threat detection, monitoring, and mitigation. Importantly, this hosting arrangement does **not** grant Microsoft or any other external party direct access to South Dakota's data or systems.

Access to SDVotes is tightly controlled and limited to a small, vetted group of individuals. Only approved KNOWiNK employees, who are all U.S. citizens who have passed comprehensive criminal background checks—and authorized South Dakota state administrative users are permitted access. This configuration ensures there is no unauthorized access, including by Microsoft personnel or other external entities. KNOWiNK does not grant access to any federal government entity unless required by law (for example, pursuant to a valid subpoena, court order, or lawful investigation). In addition, KNOWiNK does not subcontract any infrastructure development or operational access to foreign nationals; all personnel operate under U.S. legal jurisdiction and are subject to rigorous background verification.

To safeguard data and provide a complete audit trail, all system and user activity logs from related servers and services are captured and stored redundantly for accountability and review. Voter registration and reporting data within the SDVotes system is encrypted both at rest and in transit. These protections are reinforced through continuous monitoring for suspicious activity, role-based access controls, and regular reviews of permissions to ensure that only the right people have the right level of access at the right time.

Our cybersecurity model is intentionally collaborative, built on strategic alliances that strengthen, rather than dilute, South Dakota's control and data sovereignty.

- **Government Allies:** KNOWiNK works closely with entities such as the U.S. Election Assistance Commission (EAC) and the Cybersecurity and Infrastructure Security Agency (CISA), including participation in the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). KNOWiNK's EI-ISAC membership enhances our ability to receive timely threat intelligence, share best practices, and align to established cyber security standards.
- **Private Allies:** KNOWiNK also partners with industry experts and specialized cybersecurity firms to conduct penetration testing, vulnerability assessments, and related security reviews. Specific vendor and tool details are not publicly disclosed to protect operational security, but all such engagements are focused on strengthening SDVotes through independent validation, monitoring, auditing, and rapid response capabilities.
- This "teamwork approach" includes proactive participation in system audits, integration of real-time Security Information and Event Management (SIEM) tools, and coordinated threat hunting activities. These efforts **do not** involve sharing operational control or granting external entities administrative access to SDVotes. All infrastructure and operations remain U.S.-based, under U.S. jurisdiction, and governed by strict role-based access controls with no foreign-national involvement.

Taken together, this framework ensures that SDVotes benefits from the collective expertise of leading election-security stakeholders while keeping South Dakota firmly in control of its systems and data. KNOWiNK's priority is to maintain secure, U.S.-based operations that are transparent, compliant with applicable standards, and tightly aligned with South Dakota's commitment to protecting the integrity of its elections.

6. **What other vendors are out in the market that provide comparable products and services to those promised in this contract?**

   Civix, MTX, Reframe, Stonewall, Tenex, and Runbeck are vendors commonly present at NASS. However, South Dakota was not seeking a brand-new system. Pursuing a different vendor would require evaluating entirely different platforms and determining which modules would need to be built or customized to meet our requirements. That process would be lengthy, and unnecessary. We were simply upgrading the system that has served the state reliably for more than 13 years.

7. **Are there plug-ins that will be used in the new system? Does this contract allow plug-ins?**

   Yes. The System will use tightly integrated components (similar to "plug-ins") where needed to support required functionality. These include modules for document scanning (voter registration forms), printing (label printers and paper voter rosters), reporting tools, voter notices (mailings and registration updates), multi-factor authentication (MFA), and GIS tools for voter addressing. All such components are permitted under the contract so long as they comply with State security, integration, and performance requirements, and are managed and supported by KNOWiNK within the overall System architecture.

8. **Representative Moore asked questions regarding HAVA:**
   a. 4.5 million was paid with Federal HAVA grant funds and $313,170 from General Funds (SB161-2023).
   b. Do the counties pay for their own equipment on a state election or any election?
   c. Can you walk me through the breakdown of costs of equipment?
   d. Do the county auditors pay for their own equipment?

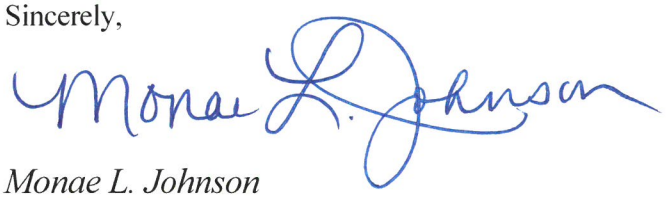
   Some equipment is mandatory by law, some equipment is discretionary. The counties are officially responsible for purchasing all county-owned election equipment used in performing their elections duties. The HAVA funds are provided by the Federal government to supplement the administration of elections, the acquisition of new equipment and the costs of maintaining it. The Secretary of State's Office makes decisions on how to best use the Federal HAVA funds in purchasing maintenance items such as new batteries, upgrades and/or new equipment. The competing priorities include funding the substantial ongoing expenses associated with staff hours spent working on administering Federal election activities and on county-wide software maintenance and upgrade costs.

2018 Equipment Purchase Totals

Row Labels	Count of Purchase Price	Sum of Purchase Price2
450	1	80,510.00
Auto Mark	17	89,675.00
AutoMARK	314	1,660,140.00
Collapsible Bin	6	4,170.00
DELL Printer S2810dn	1	-
DS200	48	265,775.00
DS450	24	1,076,220.00
DS650	1	45,500.00
DS850	10	1,091,873.00
ePollbook	58	100,025.00
e-Pollbook	44	16,245.00
ExpressVote	549	1,834,880.00
Jogger	1	450.00
Jogger 400	1	450.00
Kiosk	1	3,000.00
M100	34	171,205.00
M100	2	9,900.00
M650	20	738,905.00
M650	1	45,500.00
OKI Printer 420	1	-
OKI Printer 520	2	-
Okidata Printer	2	-
(blank)	3	10,260.00
Grand Total	**1141**	**7,244,683.00**

Thank you.

Sincerely,



Monae L. Johnson
South Dakota Secretary of State
500 East Capitol Avenue
Pierre, SD 57501
Office: 605.773.3537
Fax: 605.773.6580
Monae.Johnson@state.sd.us