



City of Castlewood
Meeting Agenda - City Council

Wednesday, October 8, 2025

6:00 PM

City Hall

1. Call to Order/Pledge of Allegiance
2. Approval of Agenda
3. Public Comment
4. Approval of Meeting Minutes
5. Approval of Bills
6. Reports

Old Business

1. Banner Drainage Study Update & Proposal
2. Third Avenue Drainage Project Update
3. Facility Plan Banner September Report
4. Code Enforcement
5. 2nd Reading 2026 Budget Appropriations Ordinance 25-3
6. Community Center Sewer Back Up & Progress Billing
7. 2026 Election Date Confirmation
8. 10x12 Shed at City Building American Legion
9. Other Old Business

New Business

1. Golf Course Trade 5 Carts & Advertise for position
2. InControl Cybersecurity Quote
3. SecureSD Cybersecurity Agreement
4. Dog Running at Large Alice Street
5. December Meeting Date Change
6. Fall Newsletter
7. Tim Popham Alice Street Preliminary Replat
7. Executive Session Personnel SDCL 1-25-2(3)
8. Adjournment

City of Castlewood – Council Members

***Mayor – Brian Ries**

***Council Members – Ward I – Stef Goldhorn & Jeannette Bohls**

Ward II – Heather Schmit & LeeAnne Dufek

Ward III – Chad Ries & Beau Schooley



Banner Associates, Inc.
409 22nd Ave S
Brookings, SD 57006
Tel 605.692.6342
Toll Free 855.323.6342

October 2, 2025

City of Castlewood
Brian Ries
204 E Main St.
Castlewood, SD 57223

RE: Engineering Services Contract for City of Castlewood Stormwater Drainage Study - 2025

Mayor Ries:

Thank you for the opportunity to present this agreement for engineering services for the above referenced project. This stormwater drainage study agreement is for the level of effort associated with the preparation of a Preliminary Engineering Report (PER). The PER will identify improvements that can be incorporated into future improvement projects.

This study is intended to be a comprehensive evaluation of the existing stormwater drainage that contributes runoff within the city limits. This comprehensive overview will be completed using LiDAR data to determine general overland flow. Locations with concentrated flow or areas with known drainage deficiencies will have a field survey performed, if determined necessary. The watershed and sub-watershed runoff flows will be determined for each delineated area within the study boundary. Localized areas, identified to have drainage issues will be evaluated further to determine options for drainage improvements. Focus will be placed on known areas of concern, including along Main St between 1st Ave and 3rd Ave and on 3rd Ave from Market St to Alice St. This plan will not effectively address private property drainage issues arising from adjacent property improvements; however, it will attempt to address public and/or street drainage that discharges through private property.

We are providing the following scope and estimate costs for a Preliminary Engineering Report (PER) drainage study.

SCOPE OF SERVICES

Task No. 1 – Data Collection

- For the identified study area, use the available LiDAR surface data to delineate watersheds and use survey points identified by the drainage problem locations to determine sub-watershed flows.
- Determine impervious area percentage, slope, and soil type for each watershed contributing to the study area.
- Survey areas of existing storm sewer infrastructure
 - Assume five (5) days of limited survey field work with a two-man crew.
 - Topographic survey at drainage issue locations.
 - Existing drainage infrastructure.
 - Pertinent house or structure elevations where needed.



- Road centerline and edges.
- Outfall locations.
- Download survey data for use in mapping and stormwater model.

Task No. 2 – Stormwater Analysis

- We understand that the City of Castlewood may not have detailed storm water design criteria. We will initially plan to use the City of Brookings, SD design criteria and may amend the criteria after discussion with the City staff during preliminary analysis.
 - Drainage systems will be analyzed for both the minor (5-year) and major (100-year) storm. Minor drainage systems are typically designed to provide protection against regularly recurring damage, to reduce street maintenance costs, and to provide an orderly urban drainage system. Storm sewer systems consisting of underground piping and drain inlets are considered part of the minor storm drainage system. The major storm drainage systems, such as drainage channels, street conveyance, or other overland flow routes, are typically designed to prevent major property damage or loss of life.
- Stormwater model, Evaluate Capacity of Existing System.
 - Using the survey data gathered and watershed delineations, a stormwater model will be developed of the drainage issue locations to determine the existing system capacity, or the peak flows generated at each location.
 - A general model will be developed over the remaining areas (areas not surveyed) to quantify the storm flows for future planning purposes.
- Stormwater model, Evaluate Capacity of Proposed Alternatives.
 - Develop alternatives using the stormwater model that will alleviate the drainage problems at previously identified locations and consider any downstream improvements that will be required.
 - Discuss alternatives with City Staff and determine if more investigation is necessary.
 - Stormwater model results will be prepared to show comparisons between the existing and proposed alternatives.
- An updated storm sewer map will be provided.
- Four (4) On-Site Meetings are included in this task:
 - (2) Meet with City Staff and identify drainage issue locations.
 - (2) Discuss alternatives with City Staff and determine if more investigation is necessary.

Task No. 3 – Drainage Report

- A Preliminary Engineering Report will be prepared which will include the following:
 - Assess which alternatives are most economical or reasonable to include in cost estimates.
 - Create report figures of the alternatives.
 - Comparison of alternatives including a "no action alternative."
- One (1) On-Site Meeting to discuss Report with City Staff and present report to City Council
- Address any comments and prepare final copy of Report for approval by City Council



Information to be Provided by the City

It is understood that the City of Castlewood will provide the following:

- City Staff to assist in identifying existing stormwater infrastructure
- City Staff will provide access to manholes, inlets or other parts of the stormwater system necessary for this study
- Permission for safe Right-of-Entry by Banner employees onto private property where survey data is to be gathered.
- Base Map identifying locations of known drainage problems
- Water, Sanitary Sewer and Storm Sewer Utility maps, if available

EXCLUSIONS

Based on our understanding of the project, the following items are excluded from our Scope of Services:

- Grant Application Assistance.
- Private property drainage issues.
- Facility Plan Document.
- Final design plans.
- Geotechnical Investigation.
- Hazardous Materials.
- Permitting.

DELIVERABLES AND SCHEDULE

The project deliverable for this project will be a Preliminary Engineering Report level drainage study.

The report will include a priority list for drainage improvements and current year budget estimates for the costs of those improvements. The report will be useful as a planning tool for long range capital improvements planning for the City of Castlewood. Completion of the Stormwater Preliminary Engineering Report will require a total of 10 to 12 months including the data collection, cost estimating, evaluation of alternative, and preparation of the report. Based on our current knowledge of the schedule for the project, Banner agrees to complete the drainage report according to the following schedule:

Task 1 – Data Collection	3 months
Task 2 – Stormwater Analysis	3 months
Task 3 – Drainage Report	4 months



COMPENSATION

Banner Associates proposes to provide the services on an hourly rate basis with an aggregate (Not-to-Exceed) limit of **\$64,900** plus applicable taxes. These costs do not include cost for any permits required by agencies for review. Any work that falls outside this scope will be billed separately base on our hourly rates accordance with the attached free schedule. Billings will be provided on a monthly basis and will be based on the "Schedule of Labor Rates and Expenses", dated January 2025 and subsequent updates. This Letter of Contract incorporates and includes Banner's Schedule of Labor Rates and Expenses and General Conditions.

If you required any additional information or want to discuss the project further, please contact our office at 605-692-6342.

Sincerely,

A handwritten signature in black ink that reads "Pat Carey".

Pat Carey, PE
Sr. Vice President

A handwritten signature in black ink that reads "Justin Bucher".

Justin Bucher, PE
Project Engineer

Enclosure:

1. Schedule of Labor Rates/General Conditions

ACKNOWLEDGMENT OF ACCEPTANCE

Accepted this _____ day of _____

Client: _____

Business: **City of Castlewood**



Banner Associates, Inc.
409 22nd Ave S
Brookings, SD 57006
Tel 605.692.6342
Toll Free 855.323.6342

SCHEDULE OF LABOR RATES AND EXPENSES

January 2025

Administrative	\$60.00 to \$195.00/Hour
Surveying/Geomatics	\$80.00 to \$180.00/Hour
Technicians.....	\$75.00 to \$140.00/Hour
Environmental Scientist.....	\$80.00 to \$185.00/Hour
Staff Engineer	\$100.00 to \$160.00/Hour
Project Engineer	\$120.00 to \$185.00/Hour
Project Manager	\$145.00 to \$285.00/Hour

1. Meals at State Rates.
2. Lodging at actual cost.
3. Reimbursables:
Mileage..... \$0.85/mile
4. All other direct project expenses at actual cost of materials.

Rates are subject to change annually.

GENERAL CONDITIONS

Agreement. The entire Agreement between the Client and Banner shall consist of the Letter of Contract, the Schedule of Labor Rates and Expenses and these General Conditions ("Agreement"). The Agreement represents the entire, integrated Agreement and supersedes all other negotiations, representations or agreements, either written or oral. The Agreement may be amended only by written agreement of the Parties. Banner's services are limited to those specifically identified in the Agreement.

Authorization to Proceed. Execution of this Agreement by the Client will be authorization for Banner to proceed with the Services, unless otherwise provided in the Agreement.

Cost Opinions. Any opinion of cost provided by Banner will be on a basis of experience and judgment, but, since construction costs are dependent upon many market and other conditions over which Banner has no control, Banner shall not be responsible for variations between actual costs and any opinion of cost.

Standard of Care. In the performance of its professional services, Banner will use that degree of care and skill ordinarily exercised by similarly situated professionals under like and similar circumstances. No express or implied warranties are applicable to, or provided with, any of Banner's services

Payment. Monthly invoices will include charges incurred during the preceding month. Payment of the invoice is due within thirty (30) days following the date of the invoice. A charge of one and one-half percent (1 1/2%) per month, or the maximum legal rate for commercial accounts, whichever is less, will be charged for late payment. Client shall be responsible for reimbursing Banner for all costs incurred in collecting delinquent amounts owed by Client.

Termination. This Agreement may be terminated for convenience upon 30 days' written notice, or for cause, if either party fails to substantially perform as required under the Agreement through no fault of the other party and does not commence to diligently correct such nonperformance within 5 days of receipt of written notice. Upon termination, Banner will be paid for all services authorized and performed up to the termination date plus reasonable termination expenses incurred by Banner as a result of the termination.. This Agreement will otherwise terminate upon completion of all applicable requirements of the Agreement. The Indemnity and Limitation of Liability Provision shall survive any termination of this Agreement.

Indemnity and Limitation of Liability. The Client agrees to defend, indemnify and hold Banner and its professionals, officers, employees representatives and agents harmless from and against all claims, costs, expenses (including attorney's fees and expenses) asserted against Banner in connection with the Project, including, but not limited to claims involving hazardous substances, except to the extent caused by the sole negligence of Banner. Banner's liability to the Client for losses, damages or injuries arising out of the performance of Banner's services or the Project will be limited to a sum not to exceed the greater of \$50,000 or Banner's fee (to a maximum of \$1,000,000 or the amount of any insurance available to cover such liability if less than \$1,000,000).

Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remainder of the Agreement shall not be affected and shall continue to be valid and enforceable to the fullest extent permitted by law.

Hazardous Substances. Unless specifically stated in this Agreement, Banner shall have no responsibility for the discovery, presence, handling, removal or disposal of, or exposure of persons to, hazardous materials or toxic substances in any form at the Project site

Interpretation. This Agreement and any claims or disputes arising out of, or relating to, the Agreement shall be governed by the laws of the State of South Dakota, other than any choice of law provisions under South Dakota law.

No Third Party Beneficiaries. This Agreement is for the sole benefit of Client and Banner and nothing contained in this Agreement shall create a contractual relationship with, or a cause of action in favor of, any third party against either Client or Banner.

Responsibility for Construction. The Client agrees that in accordance with generally accepted construction industry standards, Banner shall not have control over, charge of, or responsibility for the construction means, methods, techniques, sequences or procedures, or for safety precautions and programs in connection with the Project, since they are solely the responsibility of the contractor, and Banner shall not have control over or charge of, and shall not be responsible for, acts or omissions of the contractor, including, but not limited to the contractor's failure to perform its work in accordance with industry standards and the requirements of any plans and specifications.



ENGINEERING REPORT

TO	City of Castlewood, SD
DATE	October 2, 2025
SUBJECT	City Engineer's Report

24504.00 Castlewood Wastewater Facility Plan (Project Manager – Christa Timmer)

Project Summary:

- Complete televising assistance and prepare a wastewater facility plan. This work includes evaluating existing conditions of the collection system and WWTF, projection of future flows and loading, an evaluation of improvements needed for ongoing use of the sanitary sewer and WWTF, and Report Preparation. This work also includes providing bidding or other documentation for the city to complete televising of their sanitary sewer system.

Project Status:

- Banner continues to prepare televising plans and specifications and advance the facility plan with the information currently available.
- Televising Plans and Specifications were provided on October 2nd for City review along with some last questions before they are finalized.
- Banner is working with City staff to finalize the bidding schedule and contacting local contractors to ensure the project schedule is feasible before finalizing.

Project Schedule:

- The project schedule will likely have some adjustments as work progresses; Banner is currently ahead of schedule for some work items.
 - Kickoff Meeting - Complete
 - Finalizing televising bid documents – October 2025
 - Collection System Televising – January 2026 through May 2026
 - Data Collection - March 2026
 - Alternative Evaluation - May 2026
 - Submit Draft Facility Plan for Review - August 2026
 - Submit Final Facility Plan and Present Findings to Council - September 2026
 - State Water Plan Application - October 1, 2026
 - Public Hearing - December 2026
 - Project Funding Application - January 1, 2027

Council Action for Consideration:

- Provide permission to advertise.
- Provide the mayor with permission in advance to sign project documents.



Pending Contracts / Proposals

Banner has prepared a proposal for a comprehensive city-wide drainage study. A copy of the proposal was provided at the September Council meeting for review.

In the past month, Banner has researched the following funding opportunities:

- Small Community Planning Grant – City of Castlewood is not eligible. A stormwater PER was completed in 2011 by SPN & Associates.
- SD Emergency Management – No grants are available until a disaster is declared.
- East Dakota Water Development District – EDWDD has indicated that they are willing to cost share in the study. In the past, they have covered up to half of the engineering cost for a drainage study.

Council Action for Consideration:

- Approve Engineering proposal.

Banner Associates, Inc.

Tel | 605.692.6342 Toll Free | 1.855.323.6342

www.bannerassociates.com

ORDINANCE #25-3 2026 APPROPRIATION ORDINANCE

Part I: Be it ordained by the City of Castlewood that the following sums are appropriated to meet the obligations of the municipality:

GENERAL FUND

General Government

Mayor, Council, General	31,530	
Elections	800	
Attorney Services	5,000	
Finance Office	117,848	
Gov't Building	41,650	196,828

PUBLIC SAFETY

Police	50,000	50,000
--------	--------	--------

PUBLIC WORKS

Street and Alleys	195,911	195,911
-------------------	---------	---------

CULTURE & RECREATION

Parks and Recreation	21,785	
Library	8,468	30,253

SOLID WASTE

Garbage	106,200	
Rubble Site	7,188	113,388

HEALTH & WELFARE

West Nile	1,500	1,500
-----------	-------	-------

TOTAL GENERAL FUND		587,880
---------------------------	--	----------------

TOTAL TAX SUPPORTED FUNDS

BUSINESS IMPROVEMENT DISTRICT		10,000
--------------------------------------	--	---------------

MUNICIPAL STREET		120,000
-------------------------	--	----------------

SELF SUPPORTING FUNDS

Water Fund	171,600	
Sewer Fund	207,780	
Golf Fund	296,794	
Wellness Fund	96,968	

TOTAL APPROPRIATIONS		1,492,022
-----------------------------	--	------------------

2026 APPROPRIATION ORDINANCE

PART II: The following designates the fund or funds that money derived from the following sources is applied to:

GENERAL FUND

Cash on Hand	0
General Property Taxes	377,000
Licenses & Permits	3,450
Bank Franchise	2,500
Motor Vehicle Comm. Prorate	3,000
Liquor Tax Reversion	4,000
Motor Vehicle Licenses	10,000
Local Gov't Highway & Bridge	21,000
County Road Tax	1,500
County Wheel Tax	230
Concessions Revenue	3,000
Rec Program Fees	6,000
Interest	40,000
Rentals	5,000
Garbage Charges	100,000
Garbage Non Operating Income	6,200
TOTAL MEANS OF FINANCE	587,880

MUNICIPAL STREET REVENUE

Cash on Hand	
Sales Tax Revenue	120,000
Total Expenditures	120,000
Estimated Surplus	0

BUSINESS IMPROVEMENT DISTRICT

Cash on Hand	
Sales Tax Revenue	120,000
Misc Income	20,905
Investment Earning	11,758
Total Expenditures	10,000
Estimated Surplus	142,663

ENTERPRISE FUNDS

	Water	Sewer	Golf	Wellness
Cash on Hand		73,380		
Estimated Unappropriated Fund Balance				
Estimated Revenue	171,600	134,400	296,794	96,978
Less Estimated Appropriations	171,600	207,780	296,794	96,978
Estimated Surplus	0	0	0	0
Estimated Surplus transferred	-0-	-0-	-0-	-0-

PART III: The following is a summary of those funds for which spending authority has been approved by the Electorate:

PART IV: The Finance Officer is directed to certify the following dollar amount of tax levies made in this ordinance to the County Auditor: **FOR GENERAL PURPOSES: \$377,000.00**

Mayor

ATTEST:

Logan Ruesink, Finance Officer

First Reading: September 10, 2025
Second Reading: October 8, 2025

Post 250 potential shed installation location.

- I have visited with the county assessor. No building permit is required to bring the shed in as it will reside on land that is currently assessed under the Fire Departments 5.01, tax exemption status.
- I have visited with Justin Heyn regarding the use of a portion of their lot to place the shed. He will be attending his district authority meeting on Wednesday, October 8th. He will see if there are any issues with the shed residing at this location. (Note the location was previously offered to the Post to use by the fire department under the previous Fire Chief.
- The Post would need to have its own insurance on the 10x12' shed.
- There will be no water, sewer, or electricity at the structure with exception of some solar powered LED light used for both internal and external safety and security.
- The shed will be placed on running boards to elevate it so that the bottom of the door would reside just above the concrete curb that runs north to south, on the east side of the Community Centers right of way.





Automation & Cybersecurity Service Plan Semi-Annual Network Components Report 1

Customer Information		Service Information	
Customer Name	City of Castlewood	Project Number	25111MPlan
Address	45703 176th St.	Plan Start Date	9/1/2024
	Watertown, SD 57201	Plan Renewal Date	9/1/2025
Requested By	John Schmit	Engineer	TJL
Phone Number	(605) 793-2290	Date Survey Performed	7/30/2025

In Control has developed an **Automation & Cybersecurity Service Plan** collaborating with WatchGuard, a leader in network security. This Service Plan provides regular inspection, testing, and maintenance of your control system and its cybersecurity defenses.

This report summarizes the work that was done during the Remote Inspection of the industrial control system, conducted semi-annually by In Control SCADA engineering.

Cybersecurity & Software Assurance - Ongoing Services

1. Check firewall firmware, logs, and install required security updates semi-annually.
2. Renew licensing for covered subscription software.
3. Conduct an annual EPA Cybersecurity Assessment, complying with state and federal regulatory requirements for public water and wastewater systems.

Implementing the hardware and support features contained in this proposal along with following internal best practices will provide a strong defense to cybersecurity threats.

Recommendations

- 1) No issues found during semi-annual Network Components maintenance review.



Description of Work Performed

Firewall

WatchGuard	Model: Firebox T25
Backup Firewall Config	Backup was made on 7/30/2025. A copy of the backup was placed on the file server at In Control.
Update Firmware in Watchguard(s)	The firmware has been updated. From: v12.10.B685791 To: v12.11.3.B719894 (Latest Version) These releases include fixes to resolve Watchguard detected security issues that were found by their engineers. New versions of firmware are often released to fix bugs and security vulnerabilities that may have been discovered in the previous version. No major bugs between these two releases. Updating Firmware ensures that your firewall is functioning optimally.
Check firewall software, security logs. Identify and install required firmware updates.	After reviewing the logs of the firewall device, no security threats were detected. This indicates that the device is functioning properly and providing effective protection for the network. <u>Points of reference:</u> Botnet Scans - 129.7K - 500 blocked. Intrusion Prevention Scans - 0 - 0 Detected. Malware - 0 Detected.
Unified Threat Management (UTM) maintenance	The security standards of the unified threat detection device are up to date and no major changes have been made to its configuration. This device is also being maintained and updated to ensure that it continues to provide effective protection for the network. Some of the services that are being used and maintained on this device include URL filtering, intrusion prevention, gateway antivirus, APT blocker, DNS filtering, threat detection and response, and cloud data retention. These services help to protect against a wide range of security threats and provide valuable insights into network activity.
Multi-Factor Authentication (MFA)	Users are using multi-factor authentication (MFA) for remote access to enhance the security of their accounts. This is a good practice because it provides an additional layer of protection against unauthorized access. By requiring users to provide multiple forms of authentication, such as a password and a security token, MFA helps to ensure that only authorized individuals can access the system. This can help to prevent unauthorized access and protect sensitive information from being accessed by unauthorized users.
MFA Users	1 users configured for MFA. - John Schmit
Monthly Report Email	John Schmit (schmitt6213@gmail.com)
Total Security	Total security in support and enabled on the device gives us access to many services that help provide security to the network, these include but are not limited to URL filtering, intrusion prevention, gateway antivirus, APT blocker, DNS filtering, threat detection and response, and cloud data.

Other Software

Application	Application Version	Renewal Date
AuthPoint	N/A	6/17/2026
Total Security	N/A	6/17/2026

Notes:

- 1) One year of AuthPoint and Total Security Suite was purchased and will be renewed yearly by In Control.



In Control, Inc.
5301 E River Rd Suite 108
Fridley, MN 55421

Cybersecurity Assessment

John Schmit
City of Castlewood
45703 176th St,
Watertown SD 57201

August 1, 2025

Dear John,

In Control has prepared this third-party cybersecurity assessment of your public water or wastewater system's Operational Technology (OT) system. This assessment uses the Environmental Protection Agency's (EPA) template. The EPA based this template on the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals framework. This assessment is intended to comply with state regulatory requirements that public water and wastewater systems complete an annual cybersecurity assessment.

In Control reviewed the OT systems for the **City of Castlewood** including the meter building RTU and utility building control panel.

This review does not evaluate the Information Technology (IT) your organization may use for email, customer billing, accounting, or other office purposes. As you evaluate your overall cybersecurity, we encourage consulting whichever vendor or department provides traditional IT services to ensure you are following IT security best practices, especially around email security.

The attached **EPA Cybersecurity Assessment Report** provides a response and explanation to thirty-four questions on the cybersecurity of your OT system.

As your system is covered by In Control's **Automation & Cybersecurity Service Plan**, the vast majority of recommended cybersecurity best practices are already in place. In the near future, In Control will be developing OT-specific cybersecurity training for operators, developing written procedures for reporting cybersecurity incidents, and working to develop template incident response plans.

Lastly, we recommend you confirm and/or maintain the following policies in the operation of your system.

- Identify one person responsible for cybersecurity within your public water or wastewater system.
- Permit only designated system administrators to install new software on the OT system.
- Prohibit unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) from connecting to the OT system. Where use of such devices is necessary, minimize that use as much as possible.

- Include cybersecurity as an evaluation criterion in procuring OT and IT assets and services and require those vendors notify you of any security incidents or vulnerabilities.

Please let us know if you have any questions.

Sincerely,

Trevor Locke

In Control Inc

Cybersecurity Assessment Report

Utility ID: City of Castlewood
Assessment Date: 7/31/2025
Print Date: 8/1/2025

Contents

Identify
Protect
Detect
Respond
Recover

Purpose

This Cybersecurity Assessment Report provides a summary of results for City of Castlewood from the completed assessment using the EPA Cybersecurity Checklist (the Checklist). The table below includes all questions, responses, and explanation of responses from the Checklist including 'Yes', 'No', and 'In Progress' responses. Drinking Water and Wastewater System (WWS) representatives can use this Assessment Report as a record of the assessment and their responses.

Questions marked with an “**” indicate EPA’s priority cybersecurity practices for water and wastewater systems.

Identify			
Checklist Number	Question	Response	Explanation of Response
1.A.	Does the W/WS maintain an updated inventory of all OT and IT network assets?*	Yes	In Control maintains a list of all OT assets by IP address. This list is reviewed and updated semi-annually.
1.B.	Does the W/WS have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the W/WS?*	Yes	John Schmit - Operator
1.C.	Does the W/WS have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities?	Yes	In Control acts as the formal advisor for planning, resourcing, and execution of OT systems' cybersecurity.
1.D.	Does the W/WS provide regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?	Yes	Meetings between OT and IT personnel are held when issues arise requiring their coordination.
1.E.	Does the W/WS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?*	Yes	In Control conducts semi-annual maintenance and patching of OT systems. In Control monitors state and federal advisories for vulnerabilities with more time-sensitive patch requirements.
1.G/H.	Does the W/WS require that all OT vendors and service providers notify the W/WS of any security incidents or vulnerabilities in a risk-informed timeframe?	Yes	Require vendors and service providers to notify the W/WS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.
1.I.	Does the W/WS include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?	Yes	In Control evaluates all new hardware and software components for integration into the overall security of the OT system.

Protect			
Checklist Number	Question	Response	Explanation of Response
2.A.	Does the W/WS change default passwords?*	Yes	In Control's practice is to change all manufacturer's default username and passwords for devices on the OT network.
2.B.	Does the W/WS require a minimum length for passwords?*	Yes	In Control configures firewall credentials to require a minimum six-character password.
2.C.	Does the W/WS require unique and separate credentials for users to access OT and IT networks?*	Yes	User credentials for the OT network are established and managed separately from those on the IT network.
2.D.	Does the W/WS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?*	Yes	In Control facilitates user administration, removing credentials for the OT network when a user leaves.
2.E.	Does the W/WS separate user and privileged (e.g., System Administrator) accounts?*	Yes	In Control has different groups for Watchguard users and In Control engineers in the Watchguard management systems.
2.F.	Does the W/WS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?	Yes	In Control configures firewall to separate OT networks from all IT networks and systems.
2.G.	Does the W/WS detect and block repeated unsuccessful login attempts?	Yes	In Control configures the firewall and multi-factor authentication (MFA) solution (WatchGuard) to allow/block after 10 unsuccessful attempts to remotely login to the OT network.
2.H.	Does the W/WS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access W/WS Operational Technology (OT)/Information Technology (IT) networks?*	Yes	In Control provides a firewall that requires MFA for all remote access to the OT network.
2.I.	Does the W/WS provide/conduct annual cybersecurity awareness training for all W/WS personnel that covers basic cybersecurity concepts?*	No	In Control does not provide basic cybersecurity training to system personnel.

2.J.	Does the W/WS offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?	No	In Control does not provide OT-specific cybersecurity training to system personnel.
2.K.	Does the W/WS use effective encryption to maintain the confidentiality of data in transit?	Yes	In Control configured all remote access to the OT network via SSL or TLS (IKEv2) encryption through a VPN.
2.L.	Does the W/WS use encryption to maintain the confidentiality of stored sensitive data?	Yes	All credentials are stored in an encrypted means.
2.M.	Does the W/WS use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?		Unknown by In Control.
2.N.	Does the W/WS disable Microsoft Office macros, or similar embedded code, by default on all assets?	Yes	In Control's SCADA software uses MS Office macros and similar embedded code for reporting and other functions.
2.O.	Does the W/WS maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?*	Yes	In Control maintains a complete configuration of the OT system. This documentation is reviewed and updated semi-annually.
2.P.	Does the W/WS maintain updated documentation describing network topology (i.e., connections between all network components) across W/WS OT and IT networks?	Yes	For OT network, In Control maintains and semi-annually reviews network diagram and device list.
2.Q.	Does the W/WS require approval before new software is installed or deployed?	Yes	By policy, the end owner must approve any new software or hardware additions to the system.
2.R.	Does the W/WS backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?*	Yes	In Control provides on-site backup media for the SCADA system. In Control conducts semi-annual off-site backups of SCADA systems. For PLC and other OT devices, off-site backups are refreshed annually and as changes are made.

2.S.	Does the W/WS have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated?*	In Progress	In Control has practices in place to assist W/WS's in quickly recovering from a catastrophic loss of OT systems.
2.T.	Does the W/WS collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?	Yes	In Control uses WatchGuard's Total Security Suite which stores security log data for 365 days.
2.U.	Does the W/WS protect security logs from unauthorized access and tampering?	Yes	Security logs are stored in a secure WatchGuard Cloud environment.
2.V.	Does the W/WS prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?*	Yes	By policy, the end owner prohibits unauthorized, personal hardware from being connected to the OT system.
2.W.	Does the W/WS ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?*	Yes	The OT network is configured so that only ports necessary for operation are exposed.
2.X.	Does the W/WS eliminate connections between OT assets and the Internet?*	Yes	The OT network is separated from the public Internet via a firewall.

Detect			
Checklist Number	Question	Response	Explanation of Response
3.A.	Does the W/WS keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the W/WS?	Yes	In Control monitors state, federal, and manufacturers' advisories for time-sensitive vulnerabilities and notifies end owners in a risk-informed timeframe. In Control monitors the list of TTPs relevant
Respond			
Checklist Number	Question	Response	Explanation of Response
4.A.	Does the W/WS have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, Internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)?* Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA is required to issue regulations, through notice-and-comment rulemaking, requiring covered entities to report covered cyber incidents and ransom payments made as a result of a ransomware attack to CISA. CISA's Notice of Proposed Rulemaking proposes applying these requirements to at least some entities in the Water and Wastewater Sector. This recommendation will be revised as necessary when the CIRCIA Final Rule is issued.	In Progress	In Control is registered and maintains contact with federal and state law enforcement and cybersecurity agencies. In Control has experience reporting cybersecurity incidents on behalf of its customers.
Recover			
Checklist Number	Question	Response	Explanation of Response
5.A.	Does the W/WS have the ability to safely and effectively recover from a cybersecurity incident?	In Progress	In Control has experience recovering OT (SCADA) systems for customers that were disrupted by cybersecurity incidents.



In Control, Inc.
5301 E River Rd, Suite 108
Fridley, MN 55421

PROPOSAL # QM25081703-01

To: City of Castlewood

Date: August 17, 2025

From: Jeff Iverson

Valid: 30 days

Page: 1 of 5

Attn: John Schmit - Utility/Streets Superintendent

Re: Automation & Cybersecurity Service Plan Renewal

In Control presents our proposal for recurring inspection, testing, and maintenance services under our **Automation & Cybersecurity Service Plan**. Public water and wastewater systems rely on an increasingly complex array of Operational Technology (OT), including Programmable Logic Controllers (PLC), Operator Interface Terminals (OIT), Supervisory Control and Data Acquisition (SCADA) systems, and cellular and radio telemetry communications. These industrial control systems provide critical functions in water and wastewater treatment systems, ensuring processes are safe, reliable, and of the highest quality.

Regular inspection, testing, and maintenance of your control system improves its reliability and longevity, reduces the need for emergency service, and ensures quality operation. A well-maintained system often lasts twenty or more years. As the total replacement value of the engineering and components that make up the control system of a water and wastewater utility run into millions of dollars, regular preventative maintenance reduces long-term operating and capital replacement expense. This service plan provides the regular on-site and remote inspection and testing necessary to maintain your control system and inform planning and budgeting for future upgrades and investments.

Cybersecurity threats have increased in recent years. Criminals and nation-state-affiliated hackers are attacking water and wastewater utilities as vulnerable, poorly defended targets. Implementing and maintaining basic cybersecurity defenses will help prevent, detect, respond, and recover from these cyber incidents. This service plan provides multi-factor authentication to ensure account security, encrypts all remote access and logs all network activity to address data security, maintains an OT asset inventory and network map to address device security, and makes regular backups of all SCADA, PLC, OIT, and communication devices, which are necessary for recovering quickly after a cyberattack. Recognizing the importance of cybersecurity, In Control voluntarily underwent the Environmental Protection Agency's (EPA) Cybersecurity Evaluation Program, ensuring our controls engineering practices align with EPA and the Department of Homeland Security's recommendations.

By providing this regular inspection, testing, and maintenance, our **Automation & Cybersecurity Service Plan safeguards the long-term system integrity of your critical infrastructure.**



Proposed Ongoing Services

A. Industrial Control Panels - Inspection, Testing, and Maintenance - Annual On-Site

1. Visually inspect control panels and radios for abnormalities (frayed wires, moisture, seals, alarms)
2. Load test operation of Uninterruptible Power Supply (UPS) and check for alarms.
3. Check PLC diagnostic information for errors and low battery conditions.
4. Verify electrical schematics are present and are up to date.
5. Test critical alarms including communication-fail alarms.
6. Vacuum enclosure, lube hinges, and check pilot light function.
7. Backup Programmable Logic Controller (PLC) and Operator Interface Terminals (OIT) programs.
8. Review spares inventory condition and count.

B. Cybersecurity & Software Assurance - Ongoing Services

1. Check firewall firmware, logs, and install required security updates semi-annually.
2. Unified Threat Management (UTM) system including:
 - a. URL filtering, Intrusion Prevention System (IPS), and Gateway Antivirus (GAV).
 - b. DNS Filtering – Detects and blocks dangerous connections using DNS-level filtering.
 - c. Extended Detection & Response – Identifies and isolates infected computers on the network.
 - d. Cloud Data Retention – Monitoring and one year retention of all network activity logs.
3. Secure Remote Access through a VPN and Multi-factor Authentication Service:
 - a. Virtual Private Network (VPN) – Limit remote connections to IPsec and/or SSL encryption.
 - b. Multi-Factor Authentication – Verify all remote connections with a second means of authentication through a separate smartphone application.
 - c. Provide user administration support as requested, including creating and removing user accounts, resetting passwords, and supporting multifactor authentication and remote access.
4. Renew licensing for covered subscription software.
5. Conduct an annual **EPA Cybersecurity Assessment**, complying with state and federal regulatory requirements for public water and wastewater systems.

C. Controls System Planning Meeting – Annual meeting with Controls Engineer to develop and review multi-year control system and cybersecurity defense posture.

D. Five-Year Extended Warranty – Extends In Control's warranty term to five years for controls engineering services and equipment purchased under a separate contract with In Control. This extension only applies to UL-listed industrial control panels and SCADA computer equipment that was provided by In Control and is still within the first twelve months of its original warranty. This extended warranty remains in effect so long as this Automation & Cybersecurity Service Plan remains in place.

E. Discounted Engineering – 10% Discount on In Control's current Rate Schedule for all scheduled, unscheduled, or emergency service calls.

F. Scope of Automation & Cybersecurity Service Plan - Ongoing services, maintenance inspections, and warranty coverages apply only to these named control panels and devices:

Control System Components Covered

Main Facility Control Panels

1. Utility Building Control Panel
2. Meter Valve Building Control Panel

Remote Site Control Panels (Comprehensive Plan only)

1. N/A

SCADA Computer, Servers, and other Significant Network Equipment

1. N/A

Cybersecurity Devices (Firewalls)

1. Utility Building Control Panel – WatchGuard Firebox T25

Recurring Software and Services Provided

1. WatchGuard Total Security Suite
 - a. Firebox T-25 (Qty: 1)
2. AuthPoint Multi-Factor Authentication (Up to 5 users)

Agreement Duration & Invoicing – Plan coverage begins on the Term Start Date and automatically renews each year. Invoices will be due Net 30 and submitted on a quarterly basis at the beginning of the period. Plan may be terminated in writing at any time with 14 days' notice.

Renewal Start Date*: 9/1/2025

Next Renewal Date: 7/1/2026

* Plan renewal date is on the first of a calendar quarter. For agreements where the Plan Start Date is before the first of a quarter, a partial invoice will be submitted for the partial quarter.

Proposal Summary

Automation & Cybersecurity Service Comprehensive Plan Renewal – Provides maintenance, cybersecurity, and extended warranty coverage for identified Control Panels, SCADA Computers, Cybersecurity Devices, and recurring software and services. Pricing excludes sales and use taxes.

Automation & Cybersecurity Service Plan

\$ 2,902.00 (annualized cost)

Invoice Date	Amount	Coverage Period	
9/1/2025	\$ 242.00	9/1/2025	9/30/2025
10/1/2025	\$ 725.50	10/1/2025	12/31/2025
1/1/2026	\$ 725.50	1/1/2026	3/31/2026
4/1/2026	\$ 725.50	4/1/2026	6/30/2026
7/1/2026	Renewal		
Term Total:	\$ 2,418.50		

Thank you in advance for the consideration of our offer and for the opportunity to work together. This proposal is valid for thirty (30) days. Should you have any questions regarding this proposal, please contact me directly at your convenience.

Best Regards,

Jeff Iverson

Sr Technical Sales Engineer

Mobile: 612.802.8875

Office: 763.783.9500 x3001

E-Mail: jeff.iverson@incontrol.net

AUTOMATIC RENEWAL: This Service Plan automatically renews on the Renewal Start Date listed above. This proposal provides final scope and pricing for the coming annual term. Please reach out with any questions. Thank you!

Proposal Number: QM25081703-01

Service Plan Terms and Conditions of Sale

- 1. ENTIRE AGREEMENT** – These Service Plan Terms and Conditions of Sale (“Terms”) govern the Automation Service Plan Services (“Services”) that In Control, Inc. (“In Control”) will provide to Purchaser pursuant to In Control’s Proposal attached hereto (“Proposal”). The Proposal, along with these Terms, constitute the sole and entire agreement between the parties with respect to the Services (the “Agreement”). This Agreement supersedes all prior understandings, discussions, representations, and warranties, both written and oral, regarding the Services. No change or modification to this Agreement is effective unless in writing and signed by each party.
- 2. TERMINATION** – Either party may terminate this Agreement for cause if the other party (i) materially breaches this Agreement; (ii) becomes insolvent or admits its inability to pay its bills as they become due; or (iii) files for or is forced into a bankruptcy, receivership, or liquidation. The party seeking to terminate this Agreement for cause will give the other party fourteen (14) days’ written notice and the other party will have 14 days to cure the stated default(s). If Purchaser desires to terminate this Agreement for its own convenience during the term of this Agreement, Purchaser may do so, provided that Purchaser gives In Control thirty (30) days’ prior written notice and pays In Control for all (i) Services performed before the termination date, prorated to the termination date using the annual cost plan amount set forth in the Proposal, and (ii) reimbursable expenses incurred before the termination date.
- 3. ATTORNEYS’ FEES** - If either party files a lawsuit to enforce this Agreement, the prevailing party in such lawsuit will be entitled to recover from the other party its reasonable attorneys’ fees, costs, and expenses incurred in connection with such lawsuit, as well as any appeal or enforcement of any judgment arising from the lawsuit.
- 4. INDEMNIFICATION / INSURANCE** - Purchaser will defend, indemnify, and hold harmless In Control from and against all claims, actions, proceedings, costs, expenses, losses and liability, including all reasonable attorneys’ fees, costs and expenses, arising out of or relating to goods or services not provided by In Control pursuant to this Agreement. These obligations include, but are not limited to, all product liability, personal injury, death, or property damage claims. These obligations will survive the expiration or termination of this Agreement. Each party is responsible for obtaining and maintaining appropriate insurance coverages and endorsements necessary to ensure the provisions of this paragraph and other insurable obligations under this Agreement while the Services are being performed and for a reasonable time thereafter.
- 5. WAIVER OF CONSEQUENTIAL DAMAGES / LIMITATION OF LIABILITY** - In no event will In Control be liable in contract, tort, strict liability, warranty or otherwise, for any special, incidental or consequential damages, such as delay, disruption, loss of product, loss of anticipated profits or revenue, loss of use of the equipment or system, non-operation or increased expense of operation of other equipment or systems, cost of capital, or cost of purchase or replacement equipment systems or power incurred by Purchaser as a result of In Control’s Services. Unless otherwise expressly set forth in the Proposal, In Control will not accept any liquidated damages. Furthermore, in no event will In Control’s total liability arising out of this Agreement exceed two (2) times the aggregate amount of all payments made by Purchaser to In Control for the Services under this Agreement.
- 6. FORCE MAJEURE** – The parties agree that In Control will not be responsible or liable for any failure or delay in the performance of its Services arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, strikes, work stoppages, supply chain disruptions, accidents, acts of war or terrorism, civil or military disturbances, health crises, nuclear or natural catastrophes, acts of nature, and interruptions of utilities, communications or computer services, or other incidents shown to be outside of In Control’s control (each a “Force Majeure Event”). In Control agrees, however, to use all commercially reasonable efforts to mitigate a Force Majeure Event and resume performance of the Services as soon as practicable under the circumstances.
- 7. WARRANTY** – In Control warrants that the Services will be of good quality, free from defects in material and workmanship, will conform to the specifications and drawings, and be suitable for their intended purpose. In Control will correct, at its own cost, any Services discovered within twelve (12) months of being performed to not be in compliance with these warranties. In Control reserves the right to terminate any warranty should Purchaser’s account be in arrears for more than thirty-one (31) days. Purchaser agrees that In Control’s warranties do not apply to and Purchaser will be responsible for paying In Control’s standard rates for any repair Services In Control performs as a result of damages, delays, or interruptions caused by: (i) reasonable wear and tear; (ii) pre-existing conditions at site; (iii) accidental damage caused by Purchaser; (vi) intentional damage, misuse, or abuse caused by Purchaser or a third-party; or (v) any Force Majeure Event.
- 8. ESCALATION** – This Agreement is conditioned upon the ability of In Control to complete the Services at present prices for material and at the existing scale of wages for labor. If In Control is, at any time during the term of the Agreement, unable to complete the Services at the present prices and wages, then In Control’s compensation will be equitably adjusted by change order to compensate In Control for significant price increases. A significant price increase is defined as a change of ten percent (10%) or more for a Service item between the date of the Proposal and the date the Services are performed.
- 9. PAYMENT TERMS** - The payment terms are net thirty (30) days upon invoice receipt. Any balance remaining over thirty-one (31) days beyond the invoice date will be subject to a 2.0% monthly service fee until paid. Should a payment default occur, In Control reserves the right to stop all Services, including but not limited to startup of equipment, and terminate any existing warranty. All reasonable attempts will be made between both parties to resolve the disputed portions of any invoice within the payment terms.
- 10. NONWAIVER** - The failure by In Control to enforce at any time, or for any period of time, any of the provisions hereof will not be a waiver of such provisions nor the right of In Control thereafter to enforce each and every such provision.
- 11. REMEDIES** - Remedies herein reserved to In Control will be cumulative and in addition to any other or further remedies provided in law or equity.
- 12. RELATIONSHIP OF PARTIES** – The relationship between the Parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the Parties, and neither Party shall have authority to contract for or bind the other Party in any manner whatsoever.

MEMORANDUM OF UNDERSTANDING

**Between
DAKOTA STATE UNIVERSITY
and
City of Castlewood**

This MEMORANDUM OF UNDERSTANDING (“MOU”) is entered into by and between the Dakota State University, Madison, South Dakota (“DSU”) and City of Castlewood (“CITY”), a political subdivision of the State of South Dakota, on this 6th day of October 2025.

WHEREAS, during the 2024 South Dakota Legislative Session, Senate Bill 187 (SB 187) was enacted which appropriated \$7,000,000 to the Office of the Attorney General (“OAG”) for the purpose of creating a cybersecurity initiative for counties and municipalities throughout the State of South Dakota; and

WHEREAS, DSU operates Madison Cyber Labs (“MadLabs”), which focuses on education, research, and cybersecurity development, including initiatives that help counties and municipalities mitigate cybersecurity risks; and

WHEREAS, DSU, in partnership with the OAG, created the SecureSD Cybersecurity for Counties and municipalities to strengthen cybersecurity resilience among counties and municipalities in South Dakota; and

WHEREAS, DSU, in partnership with the OAG, seeks to protect and enhance the cybersecurity posture of South Dakota’s counties and municipalities by leveraging SecureSD resources effectively; and

WHEREAS, CITY acknowledges the importance of cybersecurity mitigation and agrees to participate in SecureSD by providing the necessary cooperation, engagement, and local implementation efforts required to enhance security.

NOW THEREFORE, in consideration of the covenants and agreements contained herein, and the joint and mutual responsibilities flowing to each party as outlined in this Memorandum of Understanding, the parties agree:

1. PURPOSE

This Memorandum of Understanding (MOU) is undertaken by and between DSU and CITY to protect and enhance the cybersecurity posture of South Dakota’s counties and municipalities through the SecureSD Program. SecureSD is designed to support counties and municipalities by providing technical mitigation assistance to reduce cybersecurity risks,

delivering training and awareness programs for municipal and county staff, and enhancing cybersecurity resilience through the implementation of best practices and security tools through a secure email system.

2. **FUNDING**

- A. SecureSD is funded by the appropriation established by SB 187 during the 2024 legislative session. The CITY acknowledges that SecureSD does not provide direct financial payments for cybersecurity efforts, nor does SecureSD offer direct financial aid. As such, no direct financial payments will be made to CITY under this MOU.
- B. Nothing in the MOU may be construed as, or may be relied on, as a future promise or commitment to providing any future funding, services, or support.

3. **DSU RESPONSIBILITIES**

- A. Implementation of SecureSD
 - 1. Oversee and implement cybersecurity mitigation and email strategies for counties or municipalities.
 - 2. Engage with managed service providers (“MSPs”) to determine appropriate scopes of work, perform work, and/or review work as needed, based on DSU’s recommendation.
 - 3. Deploy technical resources to support and enhance cybersecurity defenses.
 - 4. Provide cybersecurity education and training for municipalities and counties on an as needed basis in the sole discretion of DSU.
- B. Compliance and Reporting
 - 1. Maintain records showing:
 - a. The counties and municipalities participating or planning to participate in this initiative.
 - b. Completed and planned cybersecurity improvements for each participating local government.
 - c. Current and expected expenses for each improvement, including the cost related to SB 187.
 - d. Expected timeframes for completing the improvements.
 - e. Monthly reports including activities conducted, detailed financial information, and all information necessary to justify approval of vouchers submitted for payment.
 - 2. Provide all necessary updates and reports to the OAG and request all necessary prior authorizations according to the tenor of the agreement between DSU and the OAG dated August 26, 2024.

4. **RESPONSIBILITIES OF CITY**

- A. CITY agrees to obtain a security assessment either through Project Boundary Fence or through a private vendor which is at least as technically comprehensive as the assessment conducted through Project Boundary Fence.
- B. Engagement and Participation

1. Actively participate in SecureSD initiatives, including mitigation activities and training.
 2. Designate a single point of contact for communication between CITY, DSU, and the OAG.
- C. Implementation, Maintenance, and Ownership
1. Actively participate with selected MSP and DSU to facilitate implementation of cybersecurity measures set forth in the scope of work approved by DSU and CITY.
 2. Provide reasonable cyber and physical access to CITY facilities to the selected MSP and DSU personnel to implement the approved cybersecurity measures and to DSU upon completion to ensure the scope of work was properly implemented and in good working order.
 3. Provide reasonable access to OAG for oversight purposes to ensure that any hardware purchased pursuant to the scope of work, if any, is implemented and in use.
 4. CITY is aware and understands:
 - a. The funds appropriated pursuant to SB 187 of 2024 are one-time funds.
 - b. As such, any hardware, licenses, or software purchased or implemented as part of the scope of work becomes the sole property of the CITY and the MSP, DSU, and the OAG has no ongoing responsibility for any further improvements, ongoing licensing, maintenance, or upkeep of the installed improvements.
 - c. There is no expectation, promise, or guarantee of any future funding to address cybersecurity risks through SecureSD or otherwise.
 - d. SecureSD does not and will not provide any direct financial compensation, reimbursements, or direct payments of any kind to the CITY.

5. **MISCELLANEOUS PROVISIONS**

- A. Confidentiality
1. DSU hereby acknowledges that any and all technical details including access information, technical data, and any personally identifiable information ("PII") housed on or accessible through the CITY systems is deemed "Confidential Information" and may not be shared among or between any other participant in this initiative, or to any third party except the selected MSP and the OAG as may be required.
 2. DSU will limit access to CITY cybersecurity data to authorized personnel only.
- B. Effective Period, Modification, and Termination
1. Effective Period of MOU: This MOU shall become effective upon the date last signed below. This MOU shall remain in effect until 6/30/28 unless sooner terminated pursuant to the terms set forth herein.

2. Modification of MOU: This MOU may not be amended except in writing, which writing shall be expressly identified as a part hereof and be signed by an authorized representative of each of the parties hereto.
3. Termination of MOU: Either party may terminate this MOU upon thirty (30) days written notice. The termination shall be effective thirty (30) calendar days from the date of such notice, or at a later date agreed upon by the parties, so long as such date does not exceed the date of termination of this MOU.

C. Notices

1. Any notice or other communication required under this MOU shall be in writing and sent to the email address set forth below. Notices shall be given by and to:

For SecureSD: Dakota State University
 917 N Washington Ave
 Madison, SD 57042
 Name: Mike Waldner
 Title: Director of SecureSD
 Email: mike.waldner@dsu.edu

For City: City of Castlewood
 PO BOX 17
 204 E Main St.
 Castlewood, SD 57223
 Name: Logan Ruesink
 Title: Finance Officer
 Email: castcity@itctel.com

2. Notices or communications to or between the parties shall be deemed to have been delivered one business day after the time at which it was sent if receipt is confirmed by the recipient.

D. Joint Powers

This MOU is not a Joint Powers Agreement or cooperative action agreement pursuant to SDCL Ch. 1-24, and it does not establish a separate legal entity under SDCL 1-24-4(2) or create a joint administrator or governing board, as contemplated by SDCL 1-24-5. Each party has responsibilities under the terms of this Agreement and no joint board or administrator will be used.

E. Governing Law and Venue

This MOU shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

F. Limitation Of Liability

In no event shall any party be liable to another party for any indirect, incidental, consequential, special, punitive, exemplary, or extra-contractual damages of any kind whatsoever arising from or connected with this MOU, including, but not limited to, lost profits, lost revenues, or loss of business, regardless of legal theory, whether or not foreseeable, even if either party has been advised of the possibility or probability of such damages and even if the remedies otherwise provided by this agreement fail of their essential purpose.

In Witness Whereof, the parties signify their agreement effective the date below last written by the signatures affixed below.

DAKOTA STATE UNIVERSITY

By: _____

Ashley Podhradsky

VP Research and Economic Development

Date: _____

DSU Director of SecureSD _____ (Initial) Date: _____

DSU VP for Businesses & Admin Services _____ (Initial) Date: _____

DSU Director of Budget & Grants/Contracts _____ (Initial) Date: _____

City of Castlewood

By: _____

Brian Ries, Mayor

Date: _____

ATTEST:

By: _____

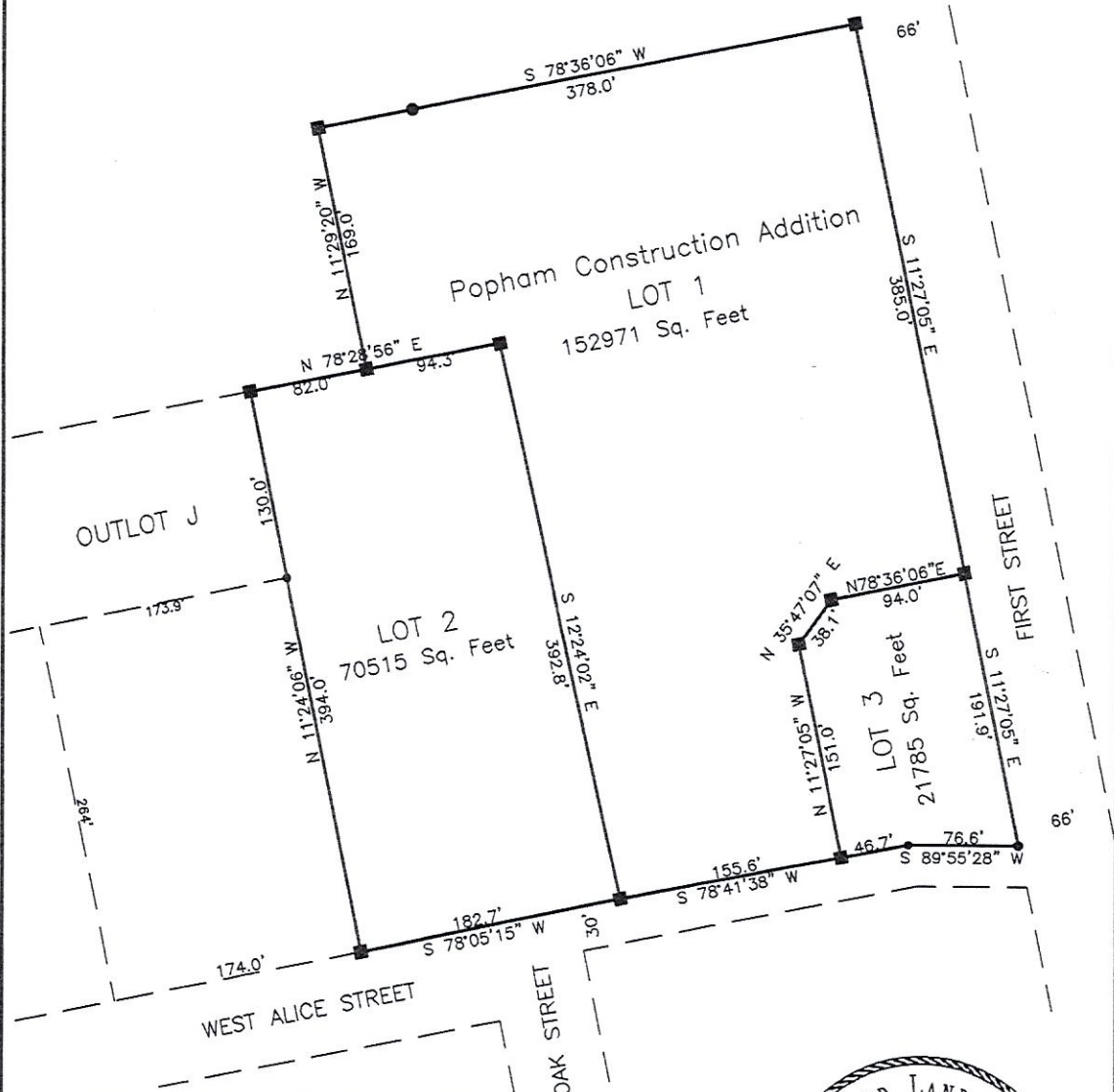
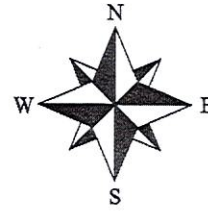
Logan Ruesink, Finance Officer

Date: _____

Popham Construction Addition
To the City of Castlewood, Hamlin County, South
Dakota.

October, 2025
Scale: 1"=100'

● Monument Recovered
■ Monument Set



MACK
Land Surveying LLC

Marty Mack
Registered Land Surveyor
Certified Federal Surveyor

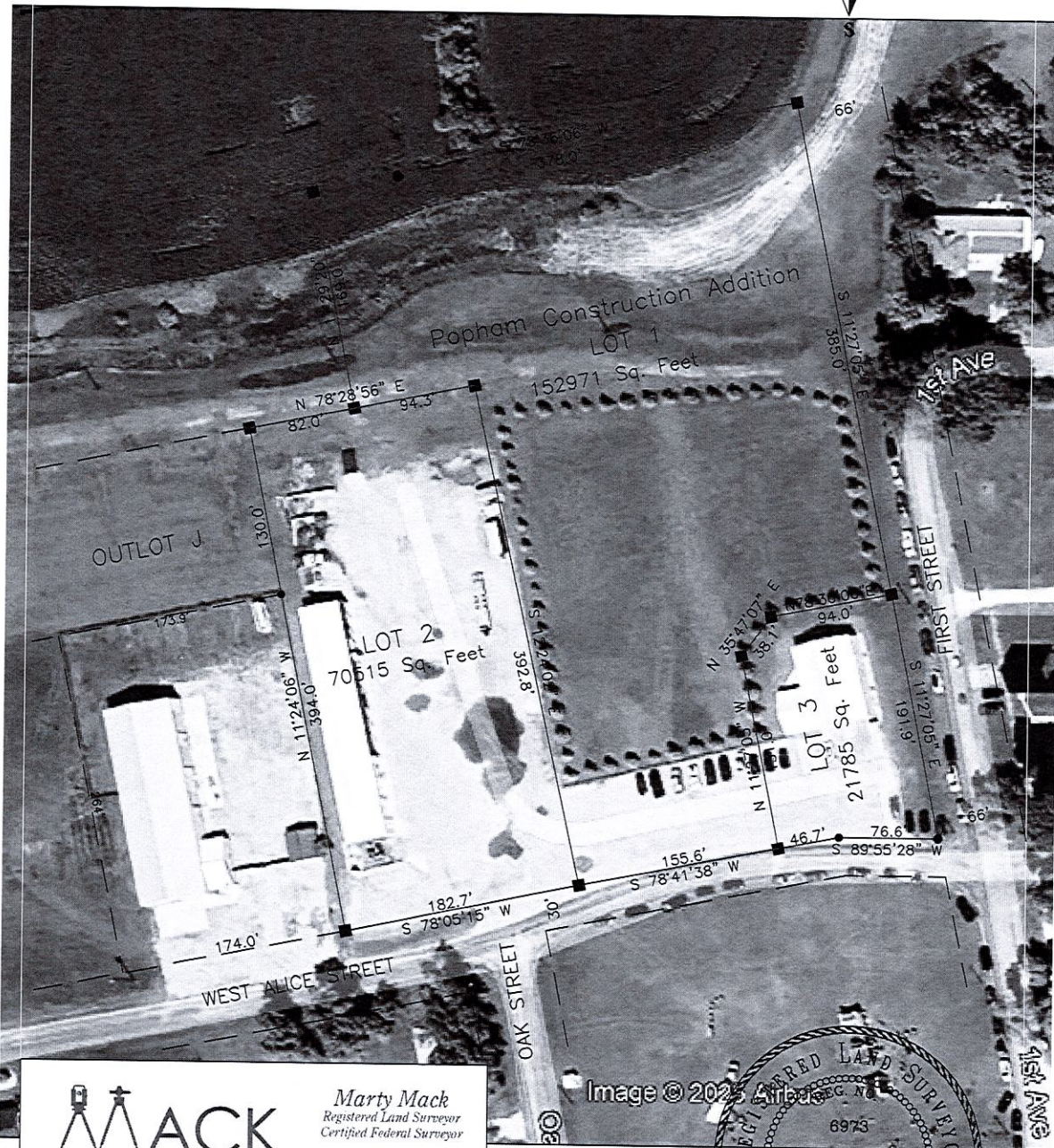
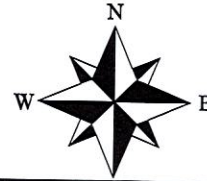
Cell: (605) 880-3108 • Phone: (605) 878-2007
808 South Maple • Watertown, SD 57201
macklandsurveying@gmail.com



Marty W. Mack
Registered Land Surveyor

Popham Construction Addition
To the City of Castlewood, Hamlin County, South
Dakota.

October, 2025
Scale: 1"=100'
● Monument Recovered
■ Monument Set



MACK
Land Surveying LLC

Marty Mack
Registered Land Surveyor
Certified Federal Surveyor

Cell: (605) 880-3108 • Phone: (605) 878-2007
808 South Maple • Watertown, SD 57201
macklandsurveying@gmail.com

Image © 2025 Airbus



Registered Land Surveyor

