



Merry Celeste, CPPB
Division Director

October 9, 2019

TO: ALL INTERESTED PROPOSERS

REQUEST FOR PROPOSAL: SCADA System Master Plan Update – Professional Engineering Services

PROPOSAL NUMBER: 189-0464-NC (SS)

PROPOSAL SUBMITTAL IS DUE: October 22, 2019 @ 3:00 P.M.

ADDENDUM NO. 1

Following is additional information, clarifications, questions and responses relative to referenced Request for Proposal (RFP):

CHANGE(S): Exhibit D has been revised and is attached to this Addendum to include an additional initiative listed for the following: **Develop and/or document formal SCADA policies and procedures.**

All other specifications, terms and conditions remain the same.

Please remember to acknowledge receipt of this Addendum in Section G, Page 25 under Addendum No.1 and return with completed proposal package.

Sincerely,

Merry Celeste, CPPB
Division Director of Purchasing and Risk Management

PLEASE ADDRESS REPLY TO:
400 South Ft. Harrison, Sixth Floor
Clearwater, Florida 33756
Phone: (727) 464-3311
FAX: (727) 464-3925
Website: www.pinellascounty.org/purchase



Revised Attachment D

Upcoming/Desired SCADA Projects

Several major initiatives have been implemented following third party assessments.

- **Reporting System Evaluation and Overhaul**
Examine acceptance and effectiveness of third party information software such as Hach WIMS and determine if it should be our primary reporting system, and at what level it should be supported by SCADA personnel or supplemented using vendor or custom reporting.
- **Assess Physical Security System with an eye towards leveraging SCADA technology to improve remote access, control, notification and reporting.**
- **Accelerate Pump Station PLC Replacement**
- **Remote Site PLC Version Control**
May be utilized at the plant level as well
- **Backup Communication paths for Critical Remote Sites**
- **DNP3 Communications Protocol for Remote Sites**
Define needs and capabilities. Expand testing if warranted. Rollout as needed.
- **Additional Virtual Machines**
 - File Server
 - Backup Jump Server
 - Historian Client Access
- **Next Level Disaster Recovery Options**
 - Quick Response on full UCS failure.
 - All in One - Single Portable Plant Server?
 - Alternate Comm. Paths within the plant
- **Develop Protocols to Verify System Functionality and Data Collection – Proactively**
 - Increased monitoring and alerting on all communication paths
 - Historian Data Verification for early gap detection
 - Automate wherever possible
- **Isolated Development or Testing Environment**
 - Segregate Contractor work
 - Pretest WSUS and Vendor Updates.
- **Reduce Software Licensing and Support Costs by utilizing Thin Client and Software Features.**
- **Deeper HMI Security Implementation**
 - Segregation by plant or role
 - Global Operator vs Supervisor Access Levels

- **EAM/Cityworks Integration**
 - Work/Service Request Initiation from HMI
- **Wonderware System Platform Object/Graphical Standards Definition and Documentation**
 - Complete graphical rework, leaning towards elements of High Performance or Situational Awareness models
 - Implement New Standards System Wide
 - Provide specifications for contract projects
- **Improved Documentation**
Drawings, SOPs, Knowledge Base, Training, and SharePoint.
- **Increase collaboration with plant process and technical personnel**
The goal is to reach a point in system development where SCADA can spend more time with operations and maintenance. We are at least advocating for the concept, even if it's too general to be included here.
 - Coordinate with EETs on PLC standards and logic
 - Poll Operations and Advise on Enhancements
- **Increase collaboration with Business Technology Services (BTS)**

Develop liaison relationship facilitating periodic reviews and recommendations on how to better utilize Information Technology.
- **Redundant Wonderware Licensing Servers**
- **Simplify galaxy objects by Utilizing .NET Controls for Station Information and minor Historical Data Queries.**
- **Evaluate new Physical Security Technology**
- **Develop and/or document formal SCADA policies and procedures**
Cyber Security
 - *Domain, Application, HMI Access, Laptops and mobile devices, Contractor/Vendor Communication, Data Access and Exchange, User Training*
 - *Disaster Preparedness and Recovery*
 - *System Integration – Projects and Modifications*