



**Austin City Council**

**Mayor**  
Lee Leffingwell

**Mayor Pro Tem**  
Mike Martinez

**Council Members**  
Chris Riley  
Randi Shade  
Laura Morrison  
Bill Spelman  
Sheryl Cole

**City Auditor**  
Kenneth J. Mory  
CPA, CIA, CISA

**Deputy City Auditor**  
Corrie E. Stokes  
CIA, CGAP

**Audit Report**

**Performance Audit of the  
Austin Water Utility SCADA System**

**August 6, 2010**

Office of the City Auditor  
Austin, Texas

### **Audit Team**

Gus Rodriguez, Auditor-In-Charge, CIA, CISA, CGAP  
Jojo Cruz, CICA  
Robert Elizondo, CIA, CGAP, CICA

### **Assistant City Auditor**

Russell Needler, CPA, CIA, CGAP

A full copy of this report is available for download at our website:  
<http://www.ci.austin.tx.us/auditor/reports>. You may also contact our office by email at  
[oca\\_auditor@ci.austin.tx.us](mailto:oca_auditor@ci.austin.tx.us).

Please request Audit No. AU10105.

OCA maintains an inventory of past audit report copies and we encourage you to return any unwanted hardcopy reports to our office to help us save on printing costs. Please mail to: P. O. Box 1088, Austin, Texas 78767-8808.

Alternative formats are available upon request.  
Please call (512) 974-2805 or Relay Texas #711.



*Printed on recycled paper*



# City of Austin



## Office of the City Auditor

301 W. 2<sup>nd</sup> Street, Suite 2130  
P.O. Box 1088  
Austin, Texas 78767-8808  
(512) 974-2805, Fax: (512) 974-2078  
email: [oca\\_auditor@ci.austin.tx.us](mailto:oca_auditor@ci.austin.tx.us)  
website: <http://www.ci.austin.tx.us/auditor>

Date: August 6, 2010

To: Mayor and Council

From: Kenneth J. Mory, City Auditor

Subject: Performance Audit of the Austin Water Utility SCADA System

I am pleased to present this audit report on the Austin Water Utility (AWU) Supervisory Control and Data Acquisition (SCADA) system.

We found that controls over the AWU SCADA system are not adequate to provide reasonable assurance that data is reliable or the system is secure. In addition, our limited testing indicated that data being transmitted to SCADA is not always accurate, which has contributed to dissatisfaction among system users. We also found that AWU does not survey users of the system for customer satisfaction.

Subsequent to the completion of our audit work, AWU and the Communications and Technology Department completed work related to our findings on system security and data reliability. Based on a review of this work, we believe that there is reasonable assurance that the external vulnerability related to system security has been adequately addressed.

Based on our findings, we recommend that AWU document and implement controls over the SCADA system and begin surveying users of the system to provide reasonable assurance that the system is performing as intended. We also recommend that AWU review and monitor maintenance policies and procedures for field instrumentation to determine if procedures are adequate to keep field instruments operating effectively.

We appreciate the cooperation and assistance we received from staff in the Facilities Engineering and Treatment divisions during this audit.

cc: Marc Ott, City Manager  
Rudy Garza, Assistant City Manager  
Greg Meszaros, Austin Water Utility Department Director  
Gopal Guthikonda, Austin Water Utility Assistant Director

[This page intentionally left blank]

## COUNCIL SUMMARY

This report presents the results of our performance audit of the Austin Water Utility Supervisory Control and Data Acquisition (SCADA) system.

The SCADA is a computer-based system that remotely controls processes previously controlled manually. The system allows AWU to collect data from field equipments such as pumps and valves via sensors.

We found that controls over the AWU SCADA systems are not adequate to provide assurance that data is reliable or that the system is secure. Based on a comparison to best practices for information technology management we identified significant control weaknesses requiring improvement in several areas.

In addition, AWU does not compare performance of the SCADA systems against performance goals, and does not survey users on system performance. Our limited testing indicated that, while the SCADA system properly recorded data transmitted to it by field instruments, the data transmitted was not accurate in every case. Finally, SCADA system users were dissatisfied with some aspects of the system.

Subsequent to the completion of our audit work, AWU and the Communications and Technology Management Department (CTM) completed work related to our findings on system security and data reliability. Based on a review of this work, we believe that there is reasonable assurance that the external vulnerability related to system security has been adequately addressed. The actions AWU has taken are discussed in the Management Response in Appendix A of this report.

Based on these results, we recommend that AWU management document and implement controls over the SCADA system, begin surveying users and incorporating the responses into performance measures, and review and monitor maintenance policies and procedures for field instrumentation to determine if procedures are adequate to keep field instruments operating effectively.

[This page intentionally left blank]



## ACTION SUMMARY AWU SCADA SYSTEM AUDIT



<b>Recommendation Text</b>	<b>Management Concurrence</b>	<b>Proposed Implementation Date</b>
01. To provide reasonable assurance that the SCADA system is performing as intended, the Director of the Austin Water Utility should work with the Facilities Engineering Division Manager to document and implement controls over the system, including, but not limited to: <ul style="list-style-type: none"><li>a. Security</li><li>b. Access</li><li>c. Configuration management</li><li>d. Contingency planning</li><li>e. Segregation of duties</li></ul>	Concur	September 2010
02. To provide reasonable assurance that the SCADA system is performing as intended, the Facilities Engineering Division Manager should begin surveying users of the system and incorporate the results into the AWU performance measures.	Concur	October 2010
03. To provide reasonable assurance that field instruments are generating accurate system data, the Instrumentation and Control Maintenance Division Manager should review and monitor maintenance policies and procedures for field instrumentation to determine if procedures are adequate to keep field instruments operating effectively.	Concur	October 2010



**TABLE OF CONTENTS**

**BACKGROUND .....1**

**OBJECTIVES, SCOPE, AND METHODOLOGY .....3**

**AUDIT RESULTS .....4**

**APPENDIX A: Management Response .....11**

**APPENDIX B: SCADA Operator Survey Results.....17**

**EXHIBITS**

Exhibit 1: Diagram of an AWU SCADA System.....2

[This page intentionally left blank]

## **BACKGROUND**

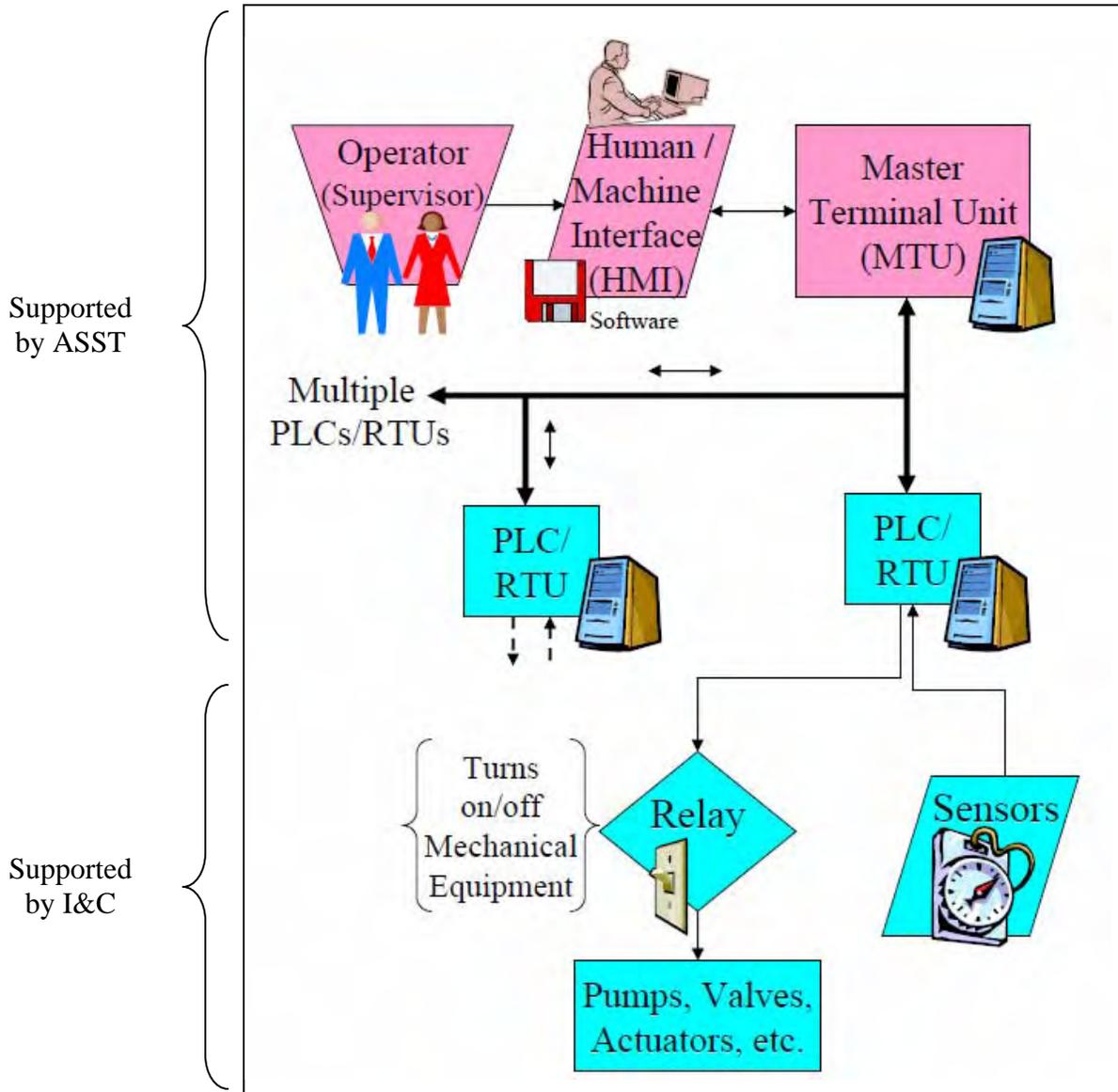
The City Council's Audit and Finance Committee approved an audit of the Austin Water Utility's (AWU) Supervisory Control and Data Acquisition (SCADA) system as part of the Office of the City Auditor's (OCA) FY 2010 Service Plan. AWU's SCADA system was identified and ranked as high risk by AWU's Facility Engineering Division during a risk self-assessment workshop conducted by OCA in FY 2009.

The SCADA is a computer-based system that remotely controls processes previously controlled manually. The SCADA system allows AWU to collect data from field equipment such as pumps and valves via sensors. This data is used to monitor and control the equipment from a central site using multiple networked computers at remote locations. For example, users can open and close valves as needed to increase or decrease water flow using the SCADA system. The SCADA communication system includes public phone lines, radio & microwave communication, and Ethernet cable.

The AWU Facilities Engineering Division is responsible for the networked computer system portion of SCADA. It is supported by the Facilities Engineering Division Automated SCADA Support Team (ASST). The field instruments including the relays, sensors, pumps, and valves are supported by the Maintenance Services Division Instrumentation & Control (I&C) maintenance group.

Exhibit 1 on the next page provides a visual representation of a typical SCADA system.

Exhibit 1:  
Diagram of an AWU SCADA System



SOURCE: Environmental Protection Agency Office of Inspector General

A study by the EPA identified potential vulnerabilities related to SCADA systems in the following areas:

- Physical (e.g., Theft, vandalism)
- Natural (e.g., Tornados, floods)
- Hardware (e.g., Inadequate security features)
- Software (e.g., Programs poorly written.)
- Communications (e.g., Messages changed or blocked.)
- Human (e.g. Human error, intentional damage)

## **OBJECTIVES, SCOPE, AND METHODOLOGY**

### **Objectives**

The audit objective was to determine whether management of the AWU SCADA system is congruent with best practice to ensure:

- The SCADA system facilitates compliance with applicable laws and regulations.
- Information from the SCADA system is reliable (includes accuracy, timeliness, completeness, consistency, and confidentiality) and available.
- SCADA performance information is used to support decision-making.

### **Scope**

The audit focused on AWU's SCADA system and the Facilities Engineering Division that is responsible for maintaining and supporting the networked computer system. Our scope also covers other divisions that interface with the SCADA system.

### **Methodology**

To accomplish our audit objectives, we performed the following steps:

- Conducted interviews of key personnel involved with AWU's SCADA process.
- Administered an internal control questionnaire to gather information about the SCADA system.
- Obtained relevant documentation to confirm controls exist for select internal controls governing the AWU SCADA process,
- Performed limited tests of SCADA data for reliability (validity, accuracy and completeness).
- Surveyed end-users to gauge overall satisfaction with the SCADA system.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## AUDIT RESULTS

**Controls over the AWU SCADA systems are not adequate, and our limited testing indicated that data being transmitted to SCADA is not accurate in every case, which has contributed to dissatisfaction among system users.**

We compared controls over the SCADA systems against best practice criteria for managing information technology systems and noted that controls were not adequate in some areas. We also completed limited testing of SCADA system performance and noted issues with data generated by field instruments. Finally, the results of a survey of SCADA system users indicated that users were dissatisfied with some aspects of the system and would like to see improvement.

**FINDING 1: Controls over the SCADA systems are not adequate to provide reasonable assurance that data is reliable and the system is secure.**

Components of an effective framework for internal control include<sup>1</sup>:

- Control environment - the tone of the organization
- Risk assessment - identifying and analyzing risks to achieving objectives
- Control activities - policies and procedures for carrying out directives
- Communication – flow of operational, financial and compliance information
- Monitoring - assessing the performance of the internal control system

We compared controls on the SCADA systems to information technology system management criteria contained in the 2009 U.S. Government Accountability Office Federal Information Systems Control Audit Manual (FISCAM). Based on the FISCAM criteria we identified significant weaknesses requiring improvement in the areas listed below.

Subsequent to the completion of our audit work, AWU and the Communications and Technology Management Department (CTM) completed work related to our findings on system security and data reliability. Based on a review of this work, we believe that there is reasonable assurance that the external vulnerability related to system security has been adequately addressed. The actions AWU has taken are discussed in the Management Response in Appendix A of this report.

---

<sup>1</sup> The Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control integrated framework

**Security management.** According to FISCAM, major IT systems should include the following security management controls:

- An effective security management plan,
- Security control policies and procedures, and
- Security awareness training.

The SCADA system supervisor indicated that these policies and procedures have not been fully documented and approved. Copies of the draft policies and procedures provided to us lacked senior management sign off or approval.

Without a well-designed security management program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

**Access controls.** According to FISCAM, major IT systems should include the following access controls:

- Protection of information system boundaries that are effective or in place.
- Identification and authentication mechanisms.
- Authorization controls in place.
- Protection of sensitive system resources.
- Audit and monitoring capability, including incident handling.

The SCADA system supervisor indicated that controls over passwords could be improved. For example, he stated no warning banners are displayed before logging onto the system, and tighter controls are needed to prohibit the use of easily guessed passwords and generic or group user IDs and passwords. For example, we observed that in one case a group password was the name of the operating plant, and in another case a group password was “Austin”. Both of these are easily guessed passwords that would allow unauthorized access to critical infrastructure. According to the SCADA system supervisor AWU currently has a project underway to complete and implement password policies.

Finally, incident handling policy and procedures have been developed, but not approved by senior management.

Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and control sensitive resources and make undetected changes and deletions for malicious purposes and personal gain. Authorized users can intentionally or unintentionally read, add, delete, modify or exfiltrate data or execute changes that are outside their span of authority.

**Configuration management.** According to FISCAM, major IT systems should include the following configuration management controls:

- Policies, plans and procedures at the entity-wide system and application levels
- Identification information procedures that identify and describe the characteristics of a controlled item (e.g. serial number and name)
- Policies for authorizing, testing, approving, tracking and controlling system changes
- Configuration monitoring procedures
- Policies for documentation and approval of emergency changes in the system

However, we determined that AWU has not fully documented and approved configuration management policies, plans or procedures. The SCADA system supervisor stated that configuration changes are performed by personnel authorized to make changes. However, we found that no configuration change policy has been approved or implemented.

Furthermore, the current and comprehensive baseline inventory of hardware, software, and firmware is not fully documented in the utility's maintenance management system. According to the SCADA system supervisor, only seventy percent of the SCADA equipment has been entered into the system, and the data entered does not include the useful life of the equipment to help determine whether it is due for replacement. Finally, configuration change controls are not adequate to authorize, test, approve, track and control all configuration changes.

Without an adequate configuration management plan, unauthorized modifications or changes to the SCADA system resources (e.g. software programs and hardware configurations) can be made, which could significantly affect operation of the system.

**Contingency planning.** According to FISCAM, major IT systems should have the following contingency planning controls:

- A comprehensive contingency plan approved by senior management.
- Periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.
- Steps to prevent and minimize potential damage and interruption.

According to the SCADA system supervisor, a contingency plan has been documented, but it does not include all of the properties of a best practice plan. For example, the plan:

- Has not been updated to reflect current conditions.
- Has not been approved by key affected groups.
- Does not clearly assign responsibilities for recovery.
- Does not identify an alternate processing facility, although it does specify a backup storage facility.
- Does not specify procedures to follow when the facility is unable to receive or transmit data.
- Does not include the necessary contact numbers, although those numbers are available in a separate document.

- Has not been coordinated with related plans and activities.
- Is not reevaluated before changes to the system are made.
- Does not specify facility access.
- Is not periodically reassessed and revised.

According to the SCADA system supervisor, some but not all SCADA system contingency plans and backup systems have been tested. Where there is no testing, the supervisor stated it is because of lack of equipment and resources. Also, there is no method for documenting and communicating test results.

Finally, there is no routine periodic hardware preventive maintenance scheduled and performed in accordance with vendor specifications.

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect AWU's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving the SCADA system or safety, system interruptions could result in injuries, as well as negative environmental impacts.

**Segregation of duties.** According to FISCAM major IT systems should have the following controls:

- Policies for identifying and segregating incompatible duties.
- Formal procedures to guide personnel in performing their duties.
- Active supervision and review for all personnel.

The SCADA system supervisor stated policies and procedures for segregating duties have not been finalized or implemented.

Dividing duties diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

## **FINDING 2: AWU does not compare performance of the SCADA systems against performance goals or survey users on system performance.**

According to FISCAM, user satisfaction should be measured over time to determine if performance is satisfactory. In addition, goals should be established against which to compare performance. According to the SCADA system supervisor, AWU is not surveying end users to measure user satisfaction, and no performance measure for user satisfaction exists. AWU also does not survey customers to measure customer satisfaction for the Automated SCADA Support Team. Because they do not survey end

users, AWU may be missing opportunities to determine where problems exist and to improve the system.

**FINDING 3: Our limited testing indicated that, while the SCADA system properly recorded data transmitted to it by field instruments, the data transmitted was not accurate in every case.**

According to FISCAM, controls are needed to provide reasonable assurance that

- Transactions are properly recorded on a timely basis
- Key data elements (e.g. amount, date) input for transactions are accurate
- Data is processed accurately by applications
- Output is accurate.

There are more than 63,000 control points being monitored or controlled by SCADA systems at the various treatment facilities and throughout the utility's distribution and collection system. We tested data generated from 65 facilities or processes representing 149 control points and found that the SCADA system accurately recorded the data transmitted by field instruments. However, in three instances the data generated by the field instruments and transmitted to the SCADA system was not accurate.

Some field instruments are exposed to potentially damaging elements such as heat, humidity, and corrosive gases. This can sometimes result in the malfunction of this equipment. Preventative maintenance procedures for field instrumentation are the main control to provide assurance that field instruments communicate accurately with the SCADA system

Inaccurate information on the SCADA system can result in system operators making wrong decisions that could significantly affect department operations and customer safety and satisfaction.

**FINDING 4: SCADA system users were dissatisfied with some aspects of the system.**

We surveyed 43 out of 142 SCADA system operators and learned they were dissatisfied with some aspects of the system. For example,

- Only 66% believe the system is always available when needed
- About 45% believe the system is not reliable
- About 42% believe the SCADA system does not respond quickly
- Only 40% agreed that SCADA does everything needed to fulfill their tasks
- Overall, about 40% were dissatisfied with the SCADA system

Operators also stated other issues, including:

- "Nuisance" alarms at multiple treatment facilities that result from out of service equipment that is still being monitored by the system
- The SCADA touch screens for the lift stations at one treatment plant are not working properly, preventing local control of the lift stations.

- The historical trending data reports module is slow and not always accurate.

SCADA system operators were also dissatisfied with some aspects of the performance of the Automated SCADA Support Team (ASST):

- Only 50% of respondents indicated the ASST responded to or resolved their issues in a timely manner.
- Only 51% of respondents rated the ASST as either good or excellent, while 42% of respondents rated ASST as average or poor.
- Only 52% agreed or strongly agreed that they were satisfied with the quality of service received from the ASST.

Operators were satisfied with some aspects of the system and performance of the ASST:

- 72% agreed that the ASST members were courteous and professional.
- 73% believe the SCADA system is easy to understand
- 68% believe the system is easy to use.

For more on the survey results, see Appendix B to this report.

## **Recommendations:**

01. To provide reasonable assurance that the SCADA system is performing as intended, the Director of the Austin Water Utility should work with the Facilities Engineering Division Manager to document and implement controls over the system, including, but not limited to:
  - a. Security
  - b. Access
  - c. Configuration management
  - d. Contingency planning
  - e. Segregation of duties

---

**MANAGEMENT RESPONSE:** Concur

AWU will take immediate steps to address the more pressing concerns raised by the audit. In addition, AWU will conduct a Risk Assessment based on the FISCAM methodology to develop industry specific Policies and Procedures to meet these requirements. A Mitigation Plan will also be developed to prioritize improvements needed to address the deficiencies identified in the audit findings.

---

02. To provide reasonable assurance that the SCADA system is performing as intended, the Facilities Engineering Division Manager should begin surveying users of the system and incorporate the results into the AWU performance measures.

---

**MANAGEMENT RESPONSE:** Concur

AWU will develop and implement a survey for their SCADA users to establish a baseline from which key performance indicators will be developed and tracked on a periodic basis.

---

03. To provide reasonable assurance that field instruments are generating accurate system data, the Instrumentation and Control Maintenance Division Manager should review and monitor maintenance policies and procedures for field instrumentation to determine if procedures are adequate to keep field instruments operating effectively.

---

**MANAGEMENT RESPONSE:** Concur

Maintenance policies and procedures for field instruments will be reviewed quarterly. Additionally, a select number of random field instruments will be reviewed each quarter to ensure that procedures are adequate to keep the instruments operating properly.

---

**APPENDIX A**  
**MANAGEMENT RESPONSE**

[This page intentionally left blank]



## MEMORANDUM

**TO:** Kenneth Mory, City Auditor

**FROM:** Greg Meszaros, Director, Austin Water Utility

**DATE:** August 3, 2010

**SUBJECT:** Response to Austin Water Utility SCADA System Audit

---

Enclosed please find our response to the Austin Water Utility SCADA System Audit. We concur with all the findings and as such, have provided our strategy and implementation plan to address each of the audit recommendations.

Austin Water has also taken immediate actions to mitigate the identified risks, and to further secure the SCADA system. Changes have been made to the SCADA computers and user accounts to make them more secure, and stricter procedures to enforce stronger passwords and inactivity time-outs have been implemented. In addition, Communication and Technology Management (CTM) security personnel performed a vulnerability assessment of SCADA System internal and external networks to test the validity of the recent improvements.

Austin Water Utility is committed to making all necessary improvements to ensure the SCADA system is both reliable and appropriately secure. The current and proposed projects will help to identify, mitigate and remediate deficiencies in the SCADA System as identified in your findings.

We trust that our response will be satisfactory and allow your office to complete the next steps of the process. Please feel free to contact me if you have any questions.



Greg Meszaros, Director  
Austin Water Utility

cc: Marc A. Ott, City Manager  
Rudy Garza, Assistant City Manager

**ACTION PLAN**  
**Austin Water Utility SCADA System Audit**

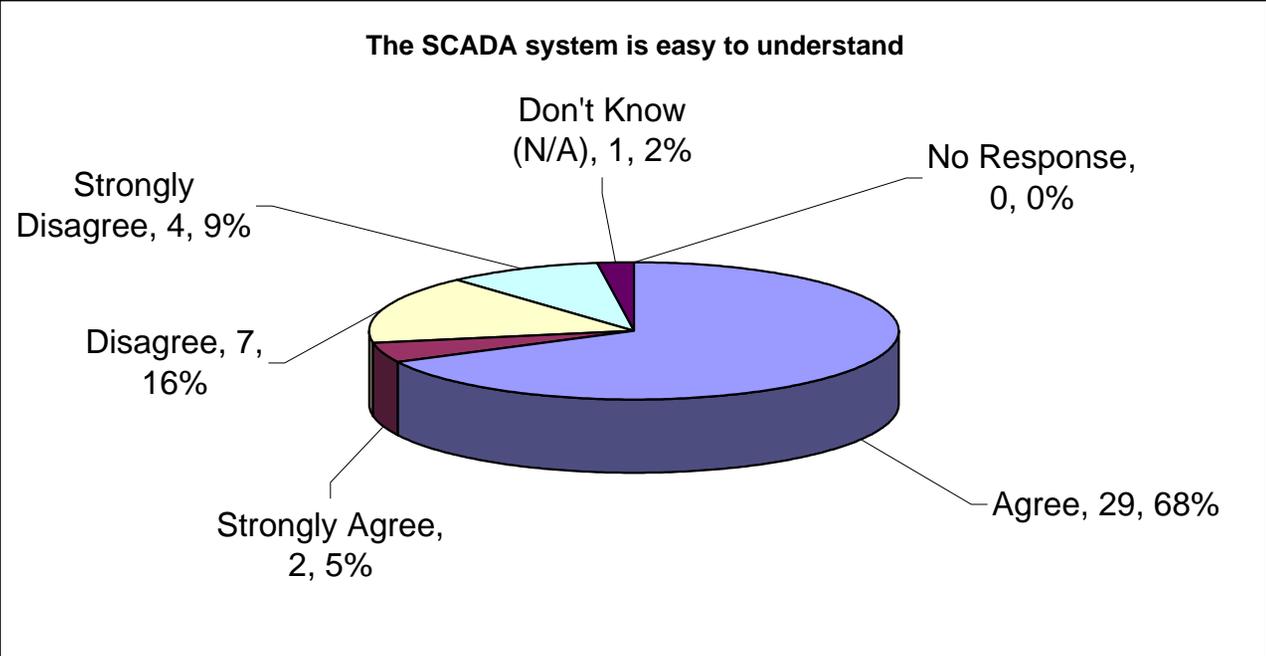
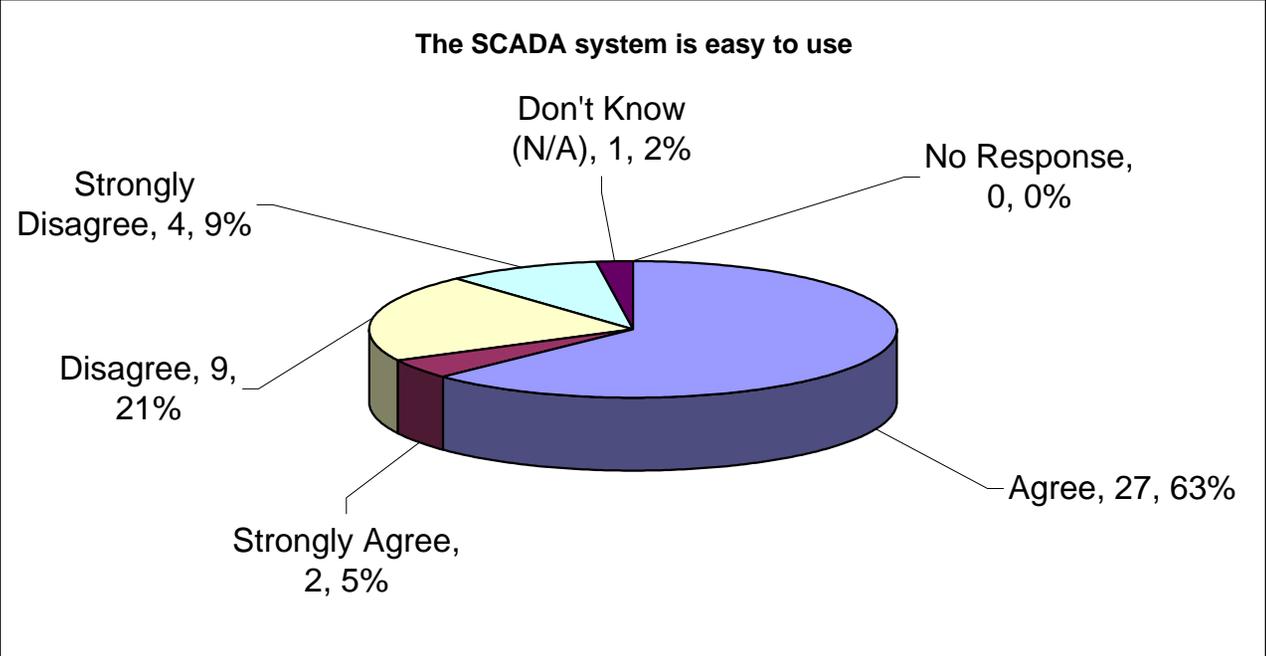
<b>Rec #</b>	<b>Recommendation Text</b>	<b>Concurrence</b>	<b>Proposed Strategies for Implementation</b>	<b>Status of Strategies</b>	<b>Responsible Person/ Phone Number</b>	<b>Proposed Implementation Date</b>
01	To provide reasonable assurance that the SCADA system is performing as intended, the Director of the Austin Water Utility should work with the Facilities Engineering Division Manager to document and implement controls over the system, including, but not limited to: <ul style="list-style-type: none"> <li>a. Security</li> <li>b. Access</li> <li>c. Configuration management</li> <li>d. Contingency planning</li> <li>e. Segregation of duties</li> </ul>	Concur with the recommendation.	AWU will take immediate steps to address the more pressing concerns raised by the audit. In addition, AWU will conduct a Risk Assessment based on the FISCAM methodology to develop industry specific Policies and Procedures to meet these requirements. A Mitigation Plan will also be developed to prioritize improvements needed to address the deficiencies identified in the audit findings.	Underway. AWU has already started implementing measures to address the more pressing concerns raised by the audit. It has also started performing analysis and testing of its systems to further identify additional improvements. AWU has also hired a Cyber Security consultant to start working on the Risk Assessment task as well as to develop the applicable Policies and Procedures and Mitigation Plan.	Gary Quick P.E. 972-0248	The more pressing system improvements are expected to be complete by July 28, 2010. The Risk Assessment and Policies and Procedures will be complete before the end of August, 2010. The Mitigation Plan will be complete before the end of September, 2010.

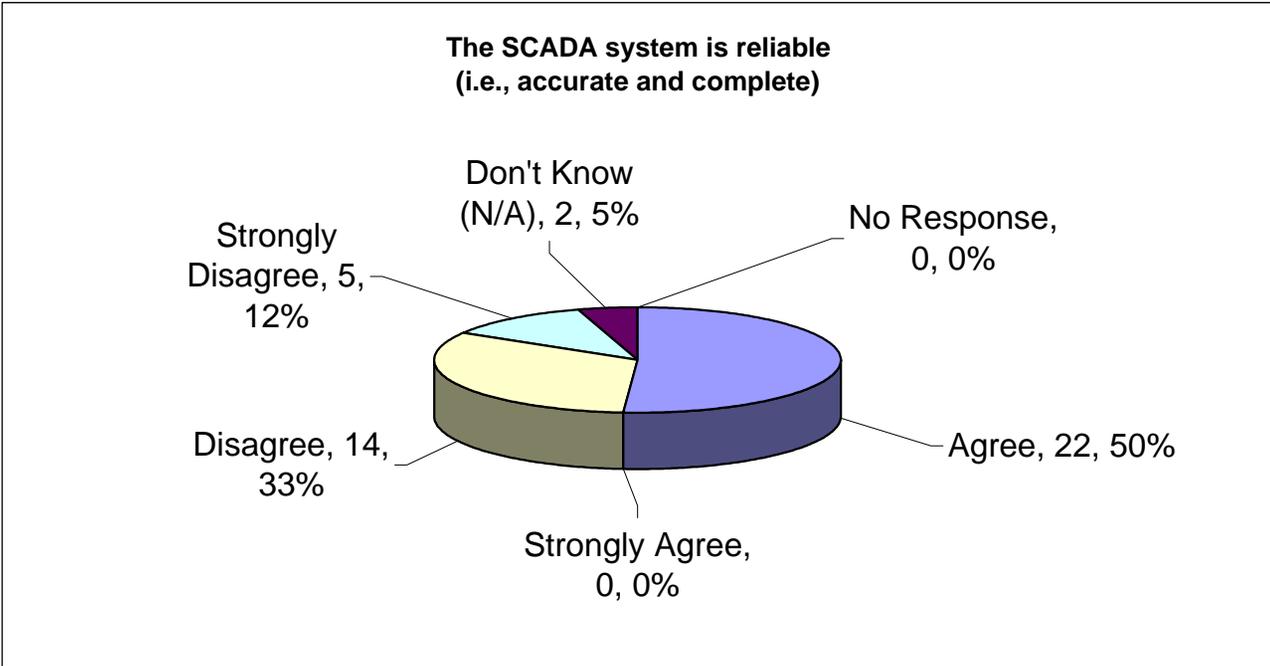
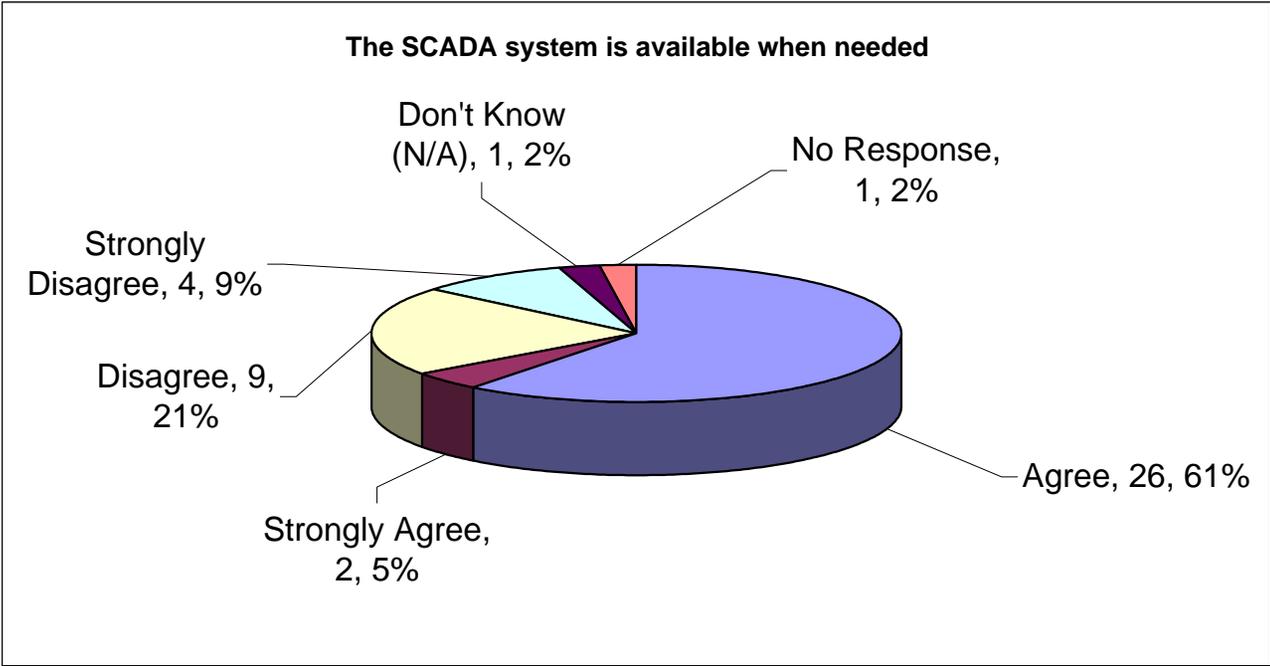
<b>Rec #</b>	<b>Recommendation Text</b>	<b>Concurrence</b>	<b>Proposed Strategies for Implementation</b>	<b>Status of Strategies</b>	<b>Responsible Person/ Phone Number</b>	<b>Proposed Implementation Date</b>
02	To provide reasonable assurance that the SCADA system is performing as intended, the Facilities Engineering Division Manager should begin surveying users of the system and incorporate the results into the AWU performance measures.	Concur with the recommendation	AWU will develop and implement a survey for their SCADA users to establish a baseline from which key performance indicators will be developed and tracked on a periodic basis.	Underway. AWU is currently working with a Consultant to develop the survey.	Gary Quick P.E. 972-0248	The survey will be complete by end of August. Key Performance Indicators will be established and tracked starting with the new fiscal year on October 1, 2010.
03	To provide reasonable assurance that field instruments are generating accurate system data, the Instrumentation and Control Maintenance Division Manager should review and monitor maintenance policies and procedures for field instrumentation to determine if procedures are adequate to keep field instruments operating effectively.	Concur with the recommendation.	Maintenance policies and procedures for field instruments will be reviewed quarterly. Additionally, a select number of random field instruments will be reviewed each quarter to ensure that procedures are adequate to keep the instruments operating properly.	Planned	Marilyn Haywood 972-0550	October 1, 2010

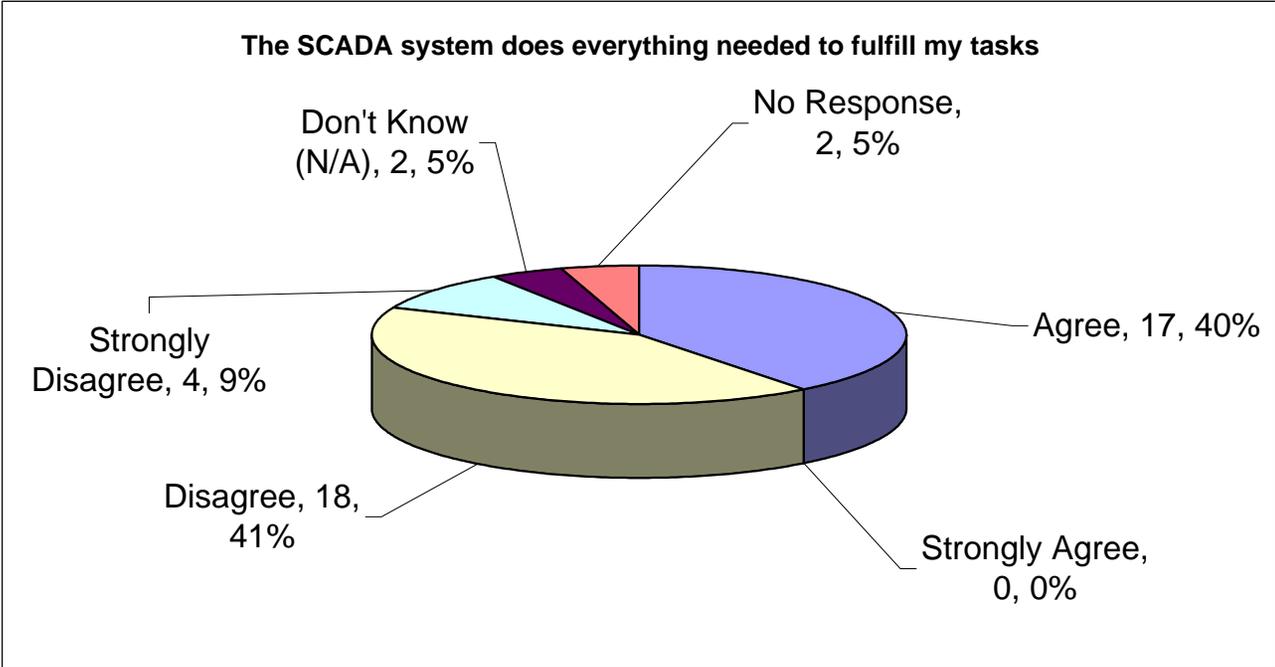
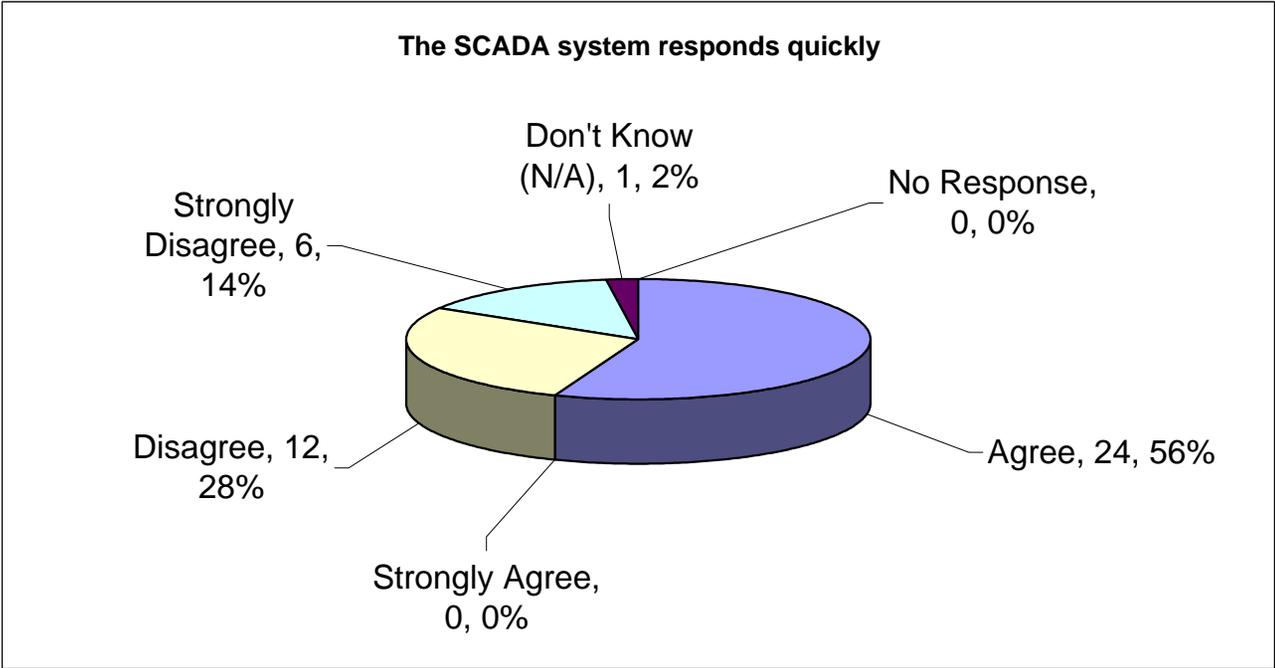
[This page intentionally left blank]

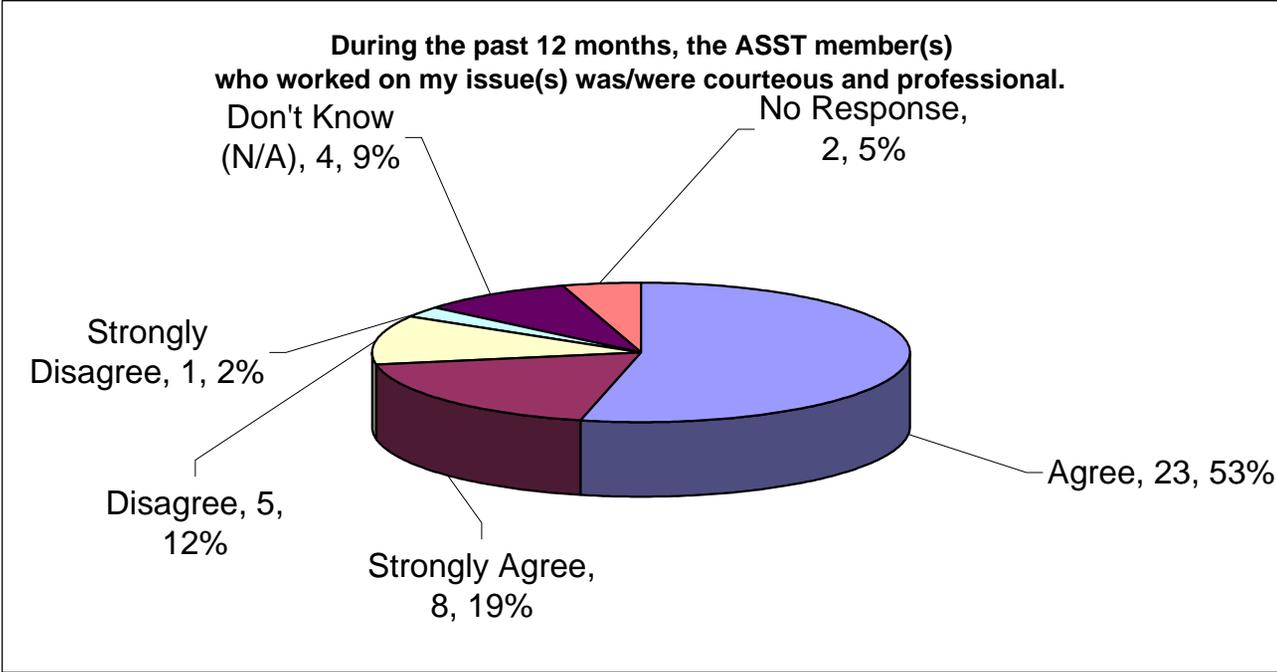
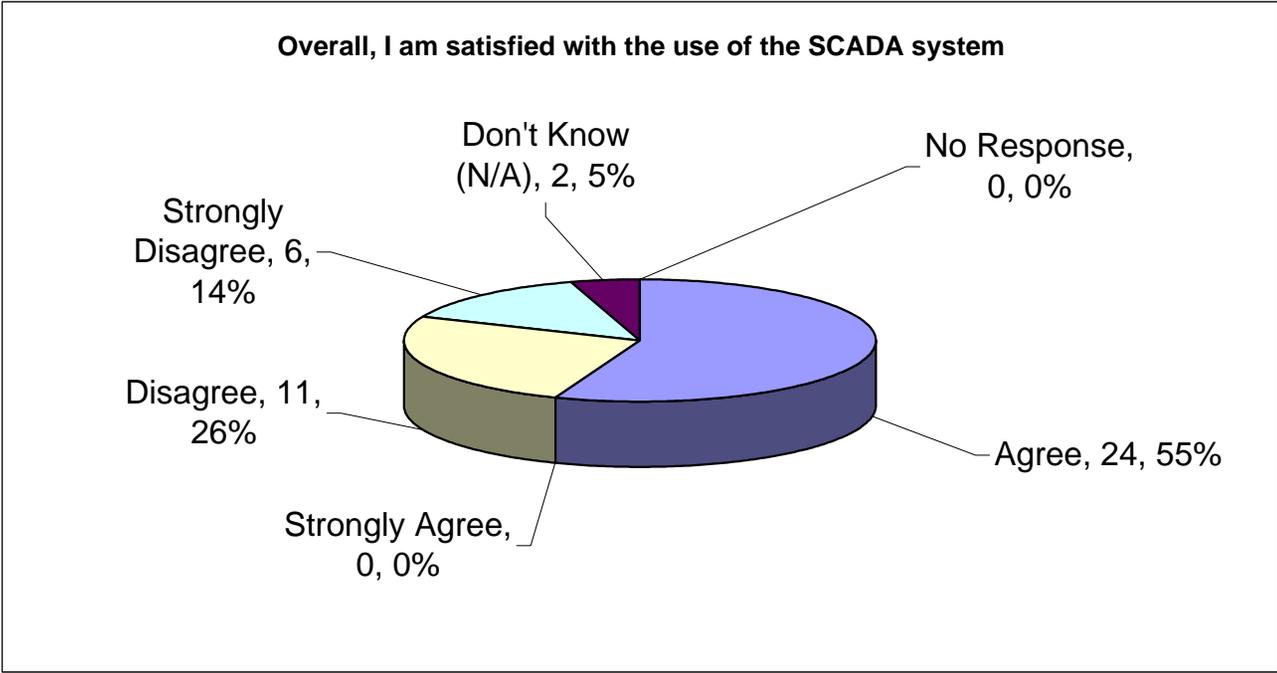
**APPENDIX B**  
**SCADA SYSTEM USER SURVEY**

[This page intentionally left blank]

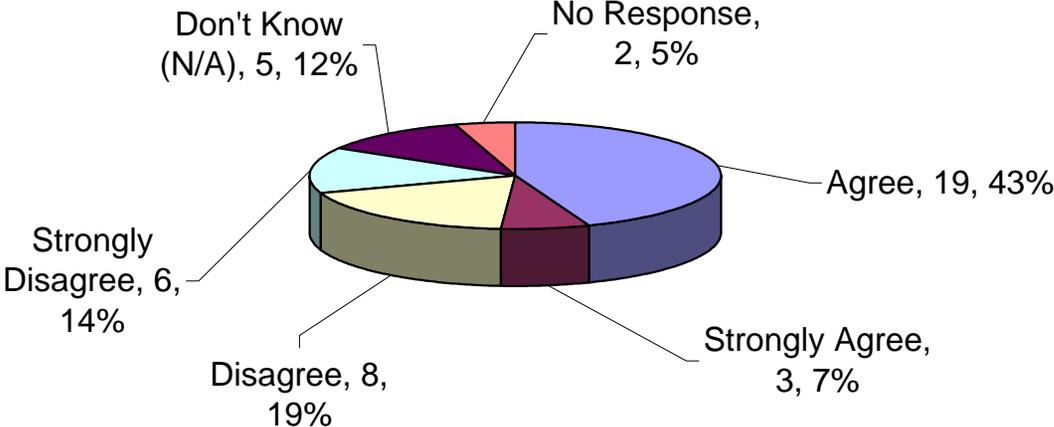




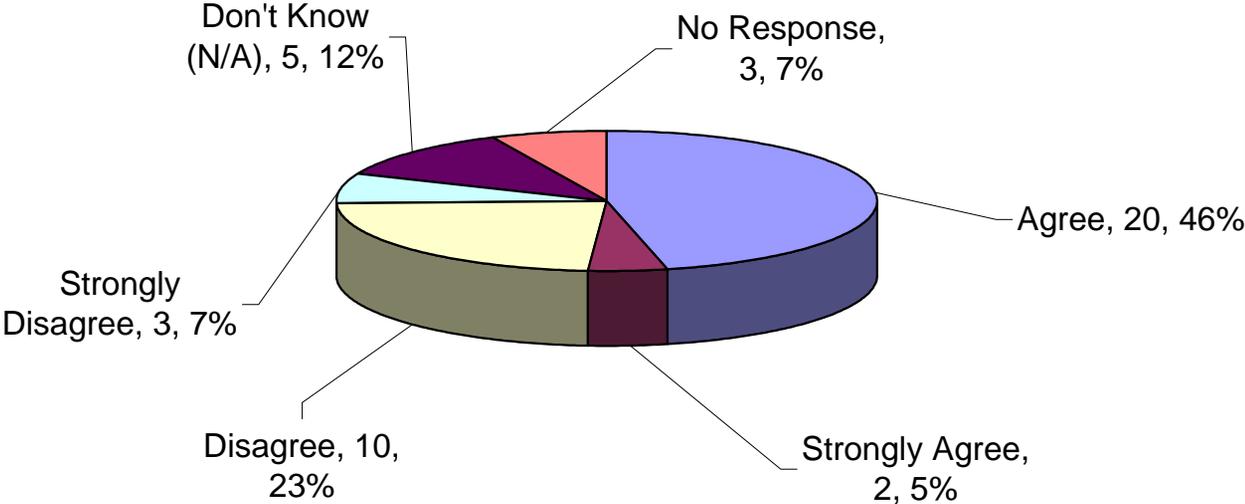




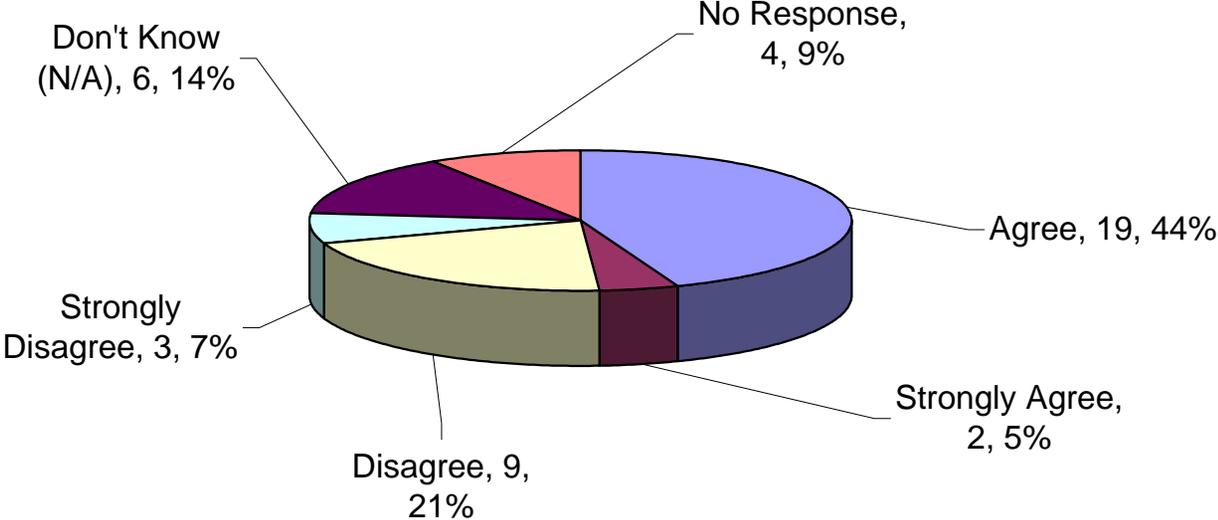
During the past 12 months, the ASST responded to my issue(s) in a timely manner.



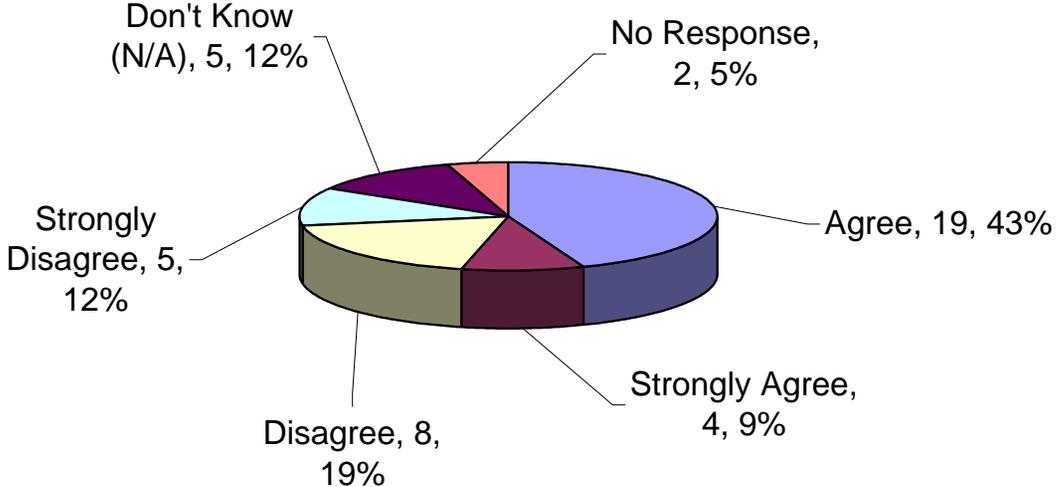
During the past 12 months, the ASST resolved my issue(s) in a timely manner.



**During the past 12 months, the ASST kept me updated on the status of my service request(s).**



**I am satisfied with the quality of service that I received from the ASST during the past 12 months.**



Overall, how would you rate the support/service you received from the ASST during the past 12 months?

