



RFQ Summary

Selected vendor(s) were notified

RFQ ID RFQ389902		Reference # FCC-RFQ09000091	
RFQ Title Project Roll Call Software & Support Services			
RFQ Status Open		Delivery Days From Date of Award to Date of Completion	
RFQ Issue Date 08/28/2009 11:11:36 AM EDT		RFQ Close Date 09/04/2009 12:00:00 PM EDT	

Line Items					
Mfr. part No/NSN/Item	Manufacturer	Product/Service Name	Qty	Unit	Ship Address
		Project Roll Call Software	1	LO	1

Description

This specification shall define the complete requirements for the Roll Call software upgrade for the Project Roll Call Systems currently operated by the FCC. This software shall replace the existing "BCAP" (Basic Computer Analyzer Program) software (FCC developed), eliminating the shortcomings of the current system and providing significant enhancement to the previous capabilities.

This software shall provide improvement in the ease of use of the Roll Call System, enhance the productivity and speed of results of the analysis staff, improve the stability and reliability of the software, and bring Project Roll Call into compliance with all applicable Federal directives concerning software. (See Attached Software Requirements and other attachments)

Attached Documents:

- Performance-based Work Statement
- RFQ09000091 - Project Roll Call Instructions.doc
- RFQ09000091 - Project Roll Call Cover Page.doc
- RFQ09000091 - Project Roll Call Past Performance.doc

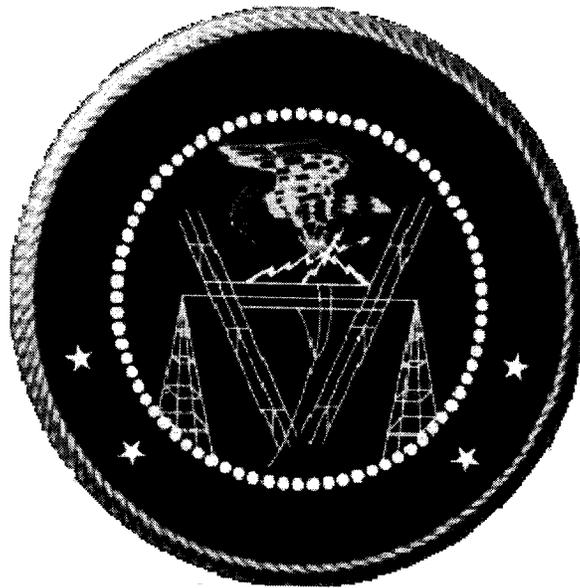
Shipping Address

(1) Arnett Rogiers:

Federal Communications Commission
 CONTRACTS & PURCHASING CENTER
 445 12TH STREET SW, ROOM # 1-A522
 Washington, DC 20554

Individual Receiving Shipment
 ARNETT ROGIERS
 202-418-1973
 ARNETT.ROGIERS@FCC.GOV

PROJECT ROLL CALL
SOFTWARE REQUIREMENTS
FOR THE
FEDERAL COMMUNICATIONS COMMISSION
PUBLIC SAFETY AND HOMELAND SECURITY BUREAU
PUBLIC COMMUNICATIONS OUTREACH AND OPERATIONS DIVISION



March 19, 2009

**Project Roll Call
Software Requirements**

March 19, 2009

Restricted Proprietary Information

This information contained herein is the exclusive property of the FCC HFDF and the FCC Operations Center, Columbia, MD. No part of this document may be disclosed, reproduced or transmitted in any form or by any means including electronic storage, reproduction, execution or transmission without the prior written consent of the FCC HFDF Center. The recipient of this document by its retention and use agrees to respect the proprietary status of the information contained herein.

© Copyright 2009 FCC HFDF Center, Columbia, MD 21046.

TABLE OF CONTENTS

1	Introduction	1
1.1	<i>Project Roll Call</i>	<i>1</i>
1.2	<i>Purpose</i>	<i>1</i>
1.3	<i>Requirements Overview and Scope</i>	<i>2</i>
1.4	<i>Acronyms</i>	<i>4</i>
2	System Overview	6
3	System Level Requirements	7
4	Project Roll Call Software Requirements	8
4.1	<i>Roll Call Graphical User Interface</i>	<i>10</i>
4.2	<i>Local Licensee Extraction</i>	<i>10</i>
4.3	<i>Data Collection Module</i>	<i>11</i>
4.4	<i>Data Analysis Module</i>	<i>11</i>
4.5	<i>Data Report Module</i>	<i>12</i>
4.6	<i>Data Storage and Recall</i>	<i>13</i>
5	Remote Operation Interfacing Requirements	14
6	System Event Logging Requirements	14
7	Report Formats	15
8	Source Code and Documentation Requirements	16
9	Software Security Requirements	16
10	Appendix A – Moderate System Required Controls	17

1 Introduction

This System Requirements Document shall provide the detailed requirements to be implemented as part of the Project Roll Call Software which will be used:

- to collect spectrum usage data with the Project Roll Call equipment, and
- to analyze the collected data and produce reports from that data.

All of the requirements specified in this document are necessary for initial deployment of the Roll Call software. There shall be no optional requirements and none shall be intended to be deferred until a subsequent software update.

1.1 Project Roll Call

Project Roll Call is a joint effort by the Federal Communications Commission (FCC) and Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA). In the wake of a National-level disaster, the effectiveness of first responders and critical infrastructure managers is sometimes hindered by disrupted or destroyed communications systems. Restoring or replacing these systems is a high priority for Federal responders.

At FEMA's request, FCC agents deploy to the disaster area and use Project Roll Call equipment to examine the radio spectrum and identify disaster-related communications outages. Outages are identified by studying the radio frequency spectrum before "Pre-disaster" and after the disaster "Post-disaster" and comparing those results to each other and to licensee databases to determine which public safety or critical infrastructure systems are unexpectedly off the air.

The Project Roll Call equipment includes a "typical" Windows Operating system based computer, a spectrum analyzer, and one or two receivers. The receivers are interfaced with the computer using Spectrum SentryNet™ software (<http://www.scanstar.com>). The Roll Call software identified in this Requirements Specification operates only with the spectrum analyzer and not with the receivers. The sole receiver-related requirement is that the software provided under this specification must co-exist and function on the Roll Call computer with the Spectrum SentryNet™ software. The Roll Call software must operate simultaneously with no performance effects to either the SentryNet™ software or the Roll Call software.

1.2 Purpose

This specification shall define the complete requirements for the Roll Call software upgrade for the Project Roll Call Systems currently operated by the FCC. This software

**Project Roll Call
Requirements Specification**

March 19, 2009

shall replace the existing “BCAP” (Basic Computer Analyzer Program) software (FCC developed), eliminating the shortcomings of the current system and providing significant enhancement to the previous capabilities.

This software shall provide improvement in the ease of use of the Roll Call System, enhance the productivity and speed of results of the analysis staff, improve the stability and reliability of the software, and bring Project Roll Call into compliance with all applicable Federal directives concerning software. (See Appendix A)

1.3 Requirements Overview and Scope

The Roll Call software shall involve a “software only” upgrade for the Project Roll Call system. There shall be no new hardware or communications infrastructure requirements needed as part of this upgrade.

Roll Call software shall perform the following four major functions:

- Local Licensee Extraction Function
 - The software shall allow the user to specify a geographic circle region by a latitude and longitude (a GPS location) for the center of the area and a radius in units of miles.
 - The software shall extract licensee information pertaining to the specified region from the FCC licensee database or other databases (if available) into a small “local region licensee” database for use with the Data Analysis Function and Data Report Function described in this software requirement.

- Data Capture Function
 - The software shall allow the user to configure and set up the connection to the spectrum analyzer for the purpose of radio frequency (RF) data collection and provide a system level diagnostics to verify the proper operations of the hardware and software of the Roll Call system.
 - The software shall allow the user to either enter or load (from an existing configuration) the data collection parameters into the Roll Call software and manually start data collection, or specify a time when collection will start automatically.
 - In an unattended manner, the software shall collect information on a particular part of the spectrum for a user-specified time (nominally one minute) and then save the collected data to a file on the Roll Call computer hard drive. The software shall then automatically re-tune the analyzer to the next portion of the spectrum specified in the data collection parameters and collect the next set of data.
 - While data collection is underway, the software shall display the spectrum analyzer sweeps on the Roll Call computer screen so that the operator can observe that the system is functioning.

**Project Roll Call
Requirements Specification**

March 19, 2009

- The software shall allow the user to stop data collection manually, or to specify a time when the collection will stop automatically.
- Data Analysis Function
 - This software function shall use the data file produced by the Data Capture function as its input.
 - The data shall be presented in a graphical manner which shall allow the user to review the collected data on a per-sweep basis or as a composite of the cumulatively collected data.
 - This function shall provide the operator with the ability to perform a graphical review of all collected to validate the quality of the data before producing reports.
- Data Report Function
 - This function will use the data file produced by the Data Capture function and the extracted local region licensee database produced by the Licensee Extraction function as its input.
 - The final product of the Report Function will generate a report formatted like the examples displayed in Section 7.
 - The Report Function will provide two types of reports based on the type of data available/collected.
 - If “Pre-disaster” scan data is available as well as “Post-disaster” data and a FCC database extract is available for the area, the Report Function shall:
 - Compare and correlate “Pre-disaster” collected signals (stored in the collection data files) with the FCC provided database to identify (as shown in Section 7) which licensed emitters were active before the disaster. Then using “post-disaster” data identify which licensed emitters were not heard during the “post-disaster” collection period.
 - If no “Pre-disaster” scan data exists, the Report function shall identify all licensed emitters in the FCC provided database extract, and also correlate and identify “post-disaster” collected signals that were observed during the “Post-disaster” collection period.
 - This function will produce reports in the format shown in the Report Formats section (Section 7) of this Requirements Specification. At present the reports are produced in MS Excel. For this Requirements Specification, reports will be produced in any standard MS Office application format or may be in any data format which can be directly imported into an MS Office application (i.e. CSV, tab delimited text, etc.).

One of the primary goals of this development is to replace the existing BCAP software while achieving significant gains in the time required to process these reports through automation. The Analysis Function and the Report Function must be routinely completed in less than one half hour, from receipt of the data file to production of the finished report.

1.4 Acronyms

The following acronyms are used in this document.

BCAP – Basic Computer Analyzer Program

CSV – Comma Separate Values

DAM – Data Analysis Module

DCM – Data Collection Module

DHS – United States Department of Homeland Security

DOS – Detected Operative Signals

DRM – Data Report Module

FCC – Federal Communications Commission

FEMA – Federal Emergency Management Agency

GPIB – General Purpose Interface Bus

HFDF – High Frequency Direction Finding Center

HTTPS – Hypertext Transfer Protocol over Secure Socket Layer

ID – Identification

LAN – Local Area Network

LLE – Local Licensee Extraction

LRL – Local Region Licensee

MS - Microsoft

PSHSB – Public Safety and Homeland Security Bureau

PCOOD – Public Communications Outreach and Operations Division

PKI – Public Key Infrastructure

**Project Roll Call
Requirements Specification**

March 19, 2009

PNG – Portable Network Graphics

RCGUI – Project Roll Call Graphical User Interface

TCP/IP – Transmission Control Protocol / Internet Protocol

TLS – Transport Layer Security

TLS-PSK – Transport Layer Security pre-shared key

USB – Universal Serial Bus

WAN – Wide Area Network

2 System Overview

The primary subsystems that comprise the Project Roll Call data collection unit are a Spectrum Analyzer, a GPIB-to-USB interface or LAN interface, and a “typical” Windows based computer.

Spectrum Analyzer: The Project Roll Call front line spectrum analyzer is the Rohde & Schwarz Model FSL-3. However, this Requirements Specification also requires that the software work with a number of legacy spectrum analyzers. Makes and models of these analyzers are listed in the System Level requirements.

GPIB-to-USB Interface: The Project Roll Call standard GPIB-to-USB interface is an ICS Electronics Model 488-USB2.

LAN interface: TCP/IP local area network interface of RJ-45 connector type or WiFi connector type.

Computer: The front line Project Roll Call data collection computer is a Stealth Computer Corporation SR-2500. (Intel Pentium 4 CPU, 3.20 GHz, 1 GB RAM, 80 GB HD, Windows XP Professional Service Pack 2) However, several legacy computers are still in use.

The primary computers that will be used for the Analysis Function and the Report Function will be standard FCC office computers operating on the internal FCC “FOCUS” network. These computers are typically HP xw4600 workstation (equipped with Intel Core 2 Duo 2.20GHz CPU with 2GB of RAM). They operate MS Windows XP Professional. In addition, field agents will need to run the Analysis Function and the Report Function on their laptops in the field. These laptops typically use 1.86 GHz Processors and 512 MB of RAM. The laptops operate MS Windows XP Professional. Project Roll Call computers and FCC “FOCUS” computers currently run MS Windows XP Professional, however the Project Roll Call software should be written to accommodate current and future MS Windows patches and a possible change in operating systems to Windows Vista (or similar MS Windows architecture) if necessary.

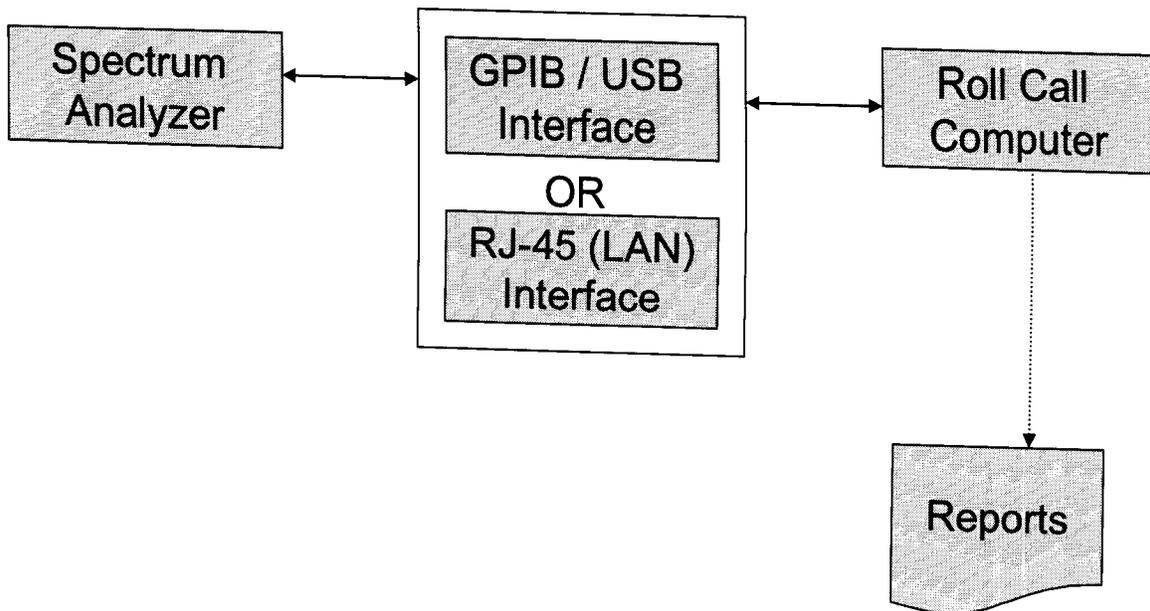


Figure 1: The Roll Call system overview.

3 System Level Requirements

- 3.1 The software shall be designed to operate 24/7 with no planned down time.
- 3.2 The software shall utilize the existing hardware and communication infrastructure (including RF communication, GPIB, LAN, and WAN) of the Roll Call system.
- 3.3 The software shall utilize the TCP/IP protocol for computer network communications.
- 3.4 The software shall provide graphical user interface using standard secure web browsers (such as Microsoft Internet Explorer, Mozilla FireFox, or ...).
- 3.5 The software shall support multi-user access through the software graphical user interface.
- 3.6 The software shall implement timeout and gracefully disconnect remote access users for no request activity exceeding a certain timeout period.
- 3.7 The software shall provide users access to the functional services of software modules via menu icon styles and sub-menu icon styles.
- 3.8 The software shall support real-time graph displays of collected data for direct and remote access users.
- 3.9 The software shall be designed to perform real-time graph displays of collected data on a per-sweep basis.
- 3.10 The software shall progressively log all activities related to user access, user request, software operation error, and software operation terminations.
- 3.11 The software shall provide a hardcopy and electronic copy of software documentation which shall contain user manual, software module manual, and installation instruction manual.

4 Project Roll Call Software Requirements

The Project Roll Call shall provide a graphical user interface (GUI) and software modules to allow users directly or remotely (through networking or dial-up) access and perform all Roll Call services. These services include, but are not limited to, configuring connected spectrum analyzers, providing a system diagnosis of the Roll Call system, collecting Roll Call information, viewing collected information, performing data analysis, generating Roll Call reports, archiving and recalling captured information. Figure 2 depicts an overview of the Roll Call software.

Roll Call Block Diagram

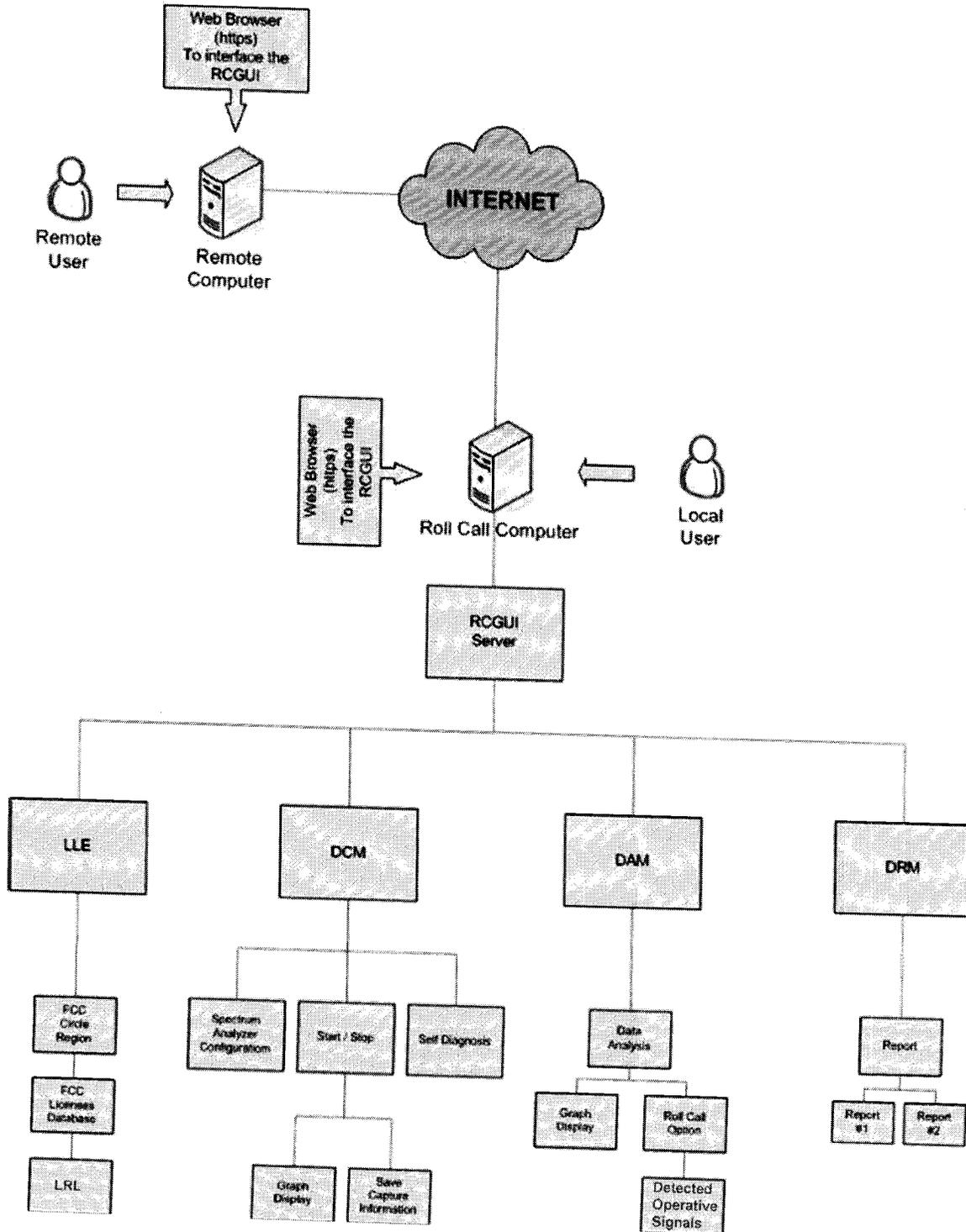


Figure 2: The Roll Call Software Overview.

4.1 Roll Call Graphical User Interface

- 4.1.1 The Roll Call graphical user interface (RCGUI) shall be capable of utilizing the latest graphic high resolution display formats at both 4:3 and 16:9 display ratios.
- 4.1.2 The RCGUI shall be interfaced via secure web services such as Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) using Transport Layer Security (TLS). The mutual authentication for HTTPS shall use Public Key Infrastructure (PKI) or Transport Layer Security Pre-Shared Key (TLS-PSK) if PKI is unavailable.
- 4.1.3 The RCGUI shall require an operator ID to sign on when first access RCGUI and provide a means for the operator to gracefully exit from the RCGUI.
- 4.1.4 The RCGUI shall allow access to operators who directly operate from the console of the Roll Call system or who remotely operate via TCP/IP network and a secure web browser.
- 4.1.5 The RCGUI shall exit the access of an operator if there are no activities for a pre-defined time-out period. The RCGUI shall provide a means to change the pre-defined time-out period.
- 4.1.6 The access to RCGUI or exit from RCGUI (log-on or log off) of any operators shall not affect the operations of Roll Call services such as data collection, data analysis, or report generation.
- 4.1.7 Upon accessing the RCGUI of an operator, the RCGUI shall display a system status of current activities or operations of Roll Call services.
- 4.1.8 Upon accessing the RCGUI of an operator, the RCGUI shall provide a menu to access Roll Call services.
- 4.1.9 The RCGUI main display shall, at all times, depict the current date and time, current GPS (Global Positioning System) location of the Roll Call system if provided by a connected GPS device, current operator ID, and system status of current activities or operation of Roll Call services including the file size of ongoing data collection. The current performing services shall have annotations of the initiating operator ID.
- 4.1.10 The RCGUI shall provide means to securely upload computer files (using https services) to connected clients.

4.2 Local Licensee Extraction

- 4.2.1 The Project Roll Call software shall provide a software module, called LLE, to extract licensee information of a geographical circle region in the United States from the FCC licensee database or other databases (if available).
- 4.2.2 The RCGUI shall provide an expandable sub-menu for the Roll Call local licensee extraction service to access and perform all functions of the LLE.
- 4.3.3 The LLE shall be developed for and operated under the environment described in Section 2, System Overview.
- 4.2.3 The LLE shall allow users to specify a geographic circle region in the United States by indicating a latitude and longitude (GPS location) of a center and a radius in units of miles (by default) and also in units of kilometers. The LLE shall allow the default value of the radius to be 30 miles.

4.2.4 The LLE shall use the information of the specified geographic circle region to extract licensee information pertaining to this region from the FCC licensee database or other databases (if available) and save the extracted information into a file, called LRL, which shall be accessible and usable for other services of the Project Roll Call software.

4.3 Data Collection Module

4.3.1 The Project Roll Call software shall provide a Roll Call data collection service as a separate software module, called Data Collection Module (DCM), which shall be interfaced via the menu of RCGUI.

4.3.2 The RCGUI shall provide an expandable sub-menu for the Roll Call data collection service to access and perform all functions of the DCM.

4.3.3 The DCM shall be developed for and operated under the environment described in Section 2, System Overview.

4.3.4 The DCM shall provide a self diagnosis of the Roll Call system to determine proper connectivity and operation of the hardware and software of the Roll Call system.

4.3.5 The DCM shall provide the means to configure and change the connected spectrum analyzer.

4.3.6 The DCM shall provide the means to load a given pre-defined configuration file or a default configuration file and configure the connected spectrum analyzer as specified by the pre-defined file.

4.3.7 The DCM shall provide means to configure the connected spectrum analyzer to capture radio frequency information for predefined bands or given input bands and basic RF measurement specifications.

4.3.8 The DCM shall provide means to start and stop data collection of the connected spectrum analyzer at the input of a user request or automatically at a preset time by a user request.

4.3.9 While capturing data, the DCM shall provide a capability to graphically display on the display screen of the Roll Call system the captured information from the connected spectrum analyzer. The graphical information shall have proper labels, annotation, unit, scaling factors, captured date and time, GPS information, and other necessary, meaningful information pertaining to the collected information.

4.3.10 The DCM shall record the captured information from the connected spectrum analyzer and save the captured information into computer files and embed or annotate the date, time, GPS information, and other information as input by users into computer files.

4.3.11 The DCM shall not initiate more than one data collection session at a time.

4.3.12 The DCM shall support the AM and FM broadcast collections, masking features currently supported by the BCAP software.

4.4 Data Analysis Module

4.4.1 The Project Roll Call software shall provide a Roll Call data analysis service as a separate software module, called Data Analysis Module (DAM), which shall be interfaced via the menu of RCGUI.

**Project Roll Call
Requirements Specification**

March 19, 2009

- 4.4.2 The RCGUI shall provide an expandable sub-menu for the Roll Call data analysis service to access and perform all functions of the DAM.
- 4.4.3 The DAM shall be developed for and operated under the environment described in Section 2, System Overview.
- 4.4.4 The DAM and all its functions and services shall have access to the local region licensee file, LRL, produced by the LLE (specified in 4.2). If the LRL is not available, the DAM shall prompt users to execute the LLE to have the LRL be generated.
- 4.4.5 The DAM shall use the information of the last captured incident as a default data input to any data analysis services.
- 4.4.6 The DAM shall provide a function icon, called "Data Analysis", which is accessible from the sub-menu of DAM. The "Data Analysis" function shall provide a comprehensive analysis view of captured information from the DCM. The comprehensive analysis shall be comparable to analysis features of the FCC BCAP (Basic Computer Analyzer Program).
- 4.4.7 The "Data Analysis" function shall include, but are not limited to, graphically displaying the collected data on a per-sweep basis or a composite of cumulatively collected data specified by maximum values, minimum values, average values, specific frequency values, or specific frequency bands. The graph display of the "Data Analysis" function shall provide interactively tracing features of point values in signal graphs.
- 4.4.8 The DAM shall provide a function icon, called "Roll Call", which is accessible from the sub-menu of DAM. The "Roll Call" function shall determine from the captured information any present RF signals based on maximum values, average values, or minimum values of RSSI (Received Signal Strength Indicator) and identify the detected operative signals by using the LRL (specified in 4.2). The identification of detected operative signals shall be graphically indicated by a color (easily seen) on the display graph and by a list containing licensee information.
- 4.4.9 The "Roll Call" function of DAM shall provide an option save the lists (containing licensee information of detected operative signals) into files, called DOS (detected operative signals), which shall be accessible and useable by the DRM as specified by 4.5.
- 4.4.10 The DAM shall present the graphical information with proper labels of title, unit, calibration scale, legend, and other meaningful information pertained to the captured incident such as date, time, time zone, GPS location, sweeping time, center frequency...
- 4.4.11 The DAM shall use the RSSI unit to be in dBm format by default.
- 4.4.12 The DAM shall provide a print option to print analysis graphs into hardcopy, an electronic image PNG (Portable Network Graphics) format, and an Adobe PDF (Portable Document Format) electronic format.

4.5 Data Report Module

- 4.5.1 The Project Roll Call software shall provide a Roll Call data report service as a separate software module, called Data Report Module (DRM), which shall be interfaced via the menu of RCGUI.
- 4.5.2 The RCGUI shall provide an expandable sub-menu for the Roll Call data report service to access and perform all functions of the DRM.

- 4.5.3 The DRM shall be developed for and operated under the environment described in Section 2, System Overview.
- 4.5.4 The DRM and all its functions and services shall have access to the local region licensee file, LRL, produced by the LLE (specified in 4.2). If the LRL is not available, the DRM shall prompt users to execute the LLE to have the LRL be generated.
- 4.5.4 The DRM shall provide a function icon, called "Report", which is accessible from the sub-menu of DRM. The "Report" function shall have the options of (1) read the analysis results in the DOS (detected operative signals) files saved in the DAM "Roll Call", or (2) go through each sweep of collected information and perform the same functionality of the "Roll Call" function of DAM and produce analysis results in DOS (detected operative signals) files. Then the "Report" function shall generate a report as specified in section 7 depending on if there are pre-incidence, post-incidence, or both. The "Report" function shall not generate any graphs on the computer display.
- 4.5.5 The "Report" function of DRM shall prompt for the selection of captured information or analysis results, DOS files, performed in the DAM "Roll Call". The selection shall contain pre-incidence, post-incidence, or both for either captured information or analysis results.
- 4.5.6 The "Report" function of DRM shall provide two types of reports based on the type of information available or collected.
- 4.5.6.1 If the pre-incidence captured information is available as well as post-incidence captured information, the "Report" function shall compare, correlate, and identify the same and different detected operative signals between pre-incidence and post-incidence and generated a report format as specified in Table 1 of section 7.
- 4.5.6.2 If the pre-incidence captured information is not available (does not exist), the "Report" function shall identify detected operative signals and generate a report format as specified in Table 2 of section 7.
- 4.5.7 The DRM shall develop and provide options to save reports in Microsoft Excel, Microsoft Office, and Adobe PDF electronic format.

4.6 Data Storage and Recall

- 4.6.1 The Project Roll Call software shall have a data naming convention and data architecture for storing and recalling collected information of the Roll Call system. The data naming convention and data architecture shall work seamlessly with all modules of the Project Roll Call software and the environment of Roll Call system.
- 4.6.2 The data naming convention and data architecture for the Roll Call system shall be capable of storing and recalling collected information on the disk storage of the Roll Call system and differentiating collected information from different events, GPS locations, dates, times, and collecting roll call units.
- 4.6.3 The data architecture of data storage and recall of the Roll Call system shall be fundamentally structured into computer files.

5 Remote Operation Interfacing Requirements

One of the required objectives of the Roll Call software is to remotely access the RCGUI and perform the full functionality of the software.

5.1 The RCGUI shall provide users remote access via TCP/IP network, a secure web browser as well as dial-up connectivity.

5.2 The RCGUI shall provide remote access users full functionality of the Roll Call software.

5.3 The RCGUI shall provide remote users the means to retrieve the collected data and place it in a desired location as needed.

5.4 For data collection, the RCGUI shall provide remote users the status of data collection as necessary in term of file size.

6 System Event Logging Requirements

6.1 The Roll Call software shall provide and progressively maintain a system event log of any access and operation requests to the RCGUI.

6.2 Each entry in the system event log shall include, at a minimum, the date, time, event type, user ID, and any other pertinent information in a textual format.

6.3 The RCGUI shall provide the capability to view entries in the event log based on user specified filter and selection criteria, including time, date range, and the event type(s).

6.4 The Roll Call software shall recycle the system event log and save a backup when the current system event log reaches the maximum file size specified by the operating system of the Roll Call system.

6.5 The system event log shall log all accessing activities of logging users.

7 Report Formats

Table 1 - Project Roll Call Report Format When Pre-Scan Data is Available

Service	Frequency	Call Sign	Spectrum User	Operational Pre Storm	Operational Post Storm	Comments (language of broadcast, usage of frequency, etc.)	Latitude Longitude
AM, FM, TV, Pub Safety LMR, USGov, etc.			(name)	(date and time observed)	(date and time observed. If not observed, highlight this in RED.)	e.g. Spanish Broadcaster, Fire ground comms, Police tactical, etc.	

Table 2 - Project Roll Call Report Format When Pre-Scan Data is Not Available

Service	Frequency	Call Sign	Spectrum User	Distance from the Base or Repeater Station to the Roll Call Measurement Point	Operating Power	Operational Post Storm	Comments (language of broadcast, usage of frequency, etc.)	Latitude Longitude
AM, FM, TV, Pub Safety LMR, USGov, etc.			(name)	(miles)	(watts)	(date and time observed. If not observed, highlight this in RED.)		

8 Source Code and Documentation Requirements

- 8.1 The delivery of Roll Call software shall include the source code, executable code, and software documentation all of which shall be US Government owned and US Government proprietary.
- 8.2 The Roll Call software shall contain a hardcopy and an electronic copy of software documentation.
- 8.3 The electronic software documentation of the Roll Call software shall be in Adobe PDF electronic format.
- 8.4 The Roll Call software documentation shall be accessible and be viewed through the RCGUI.
- 8.5 The Roll Call software documentation shall consist of user manual, software module manual, and installation instruction manual.
- 8.6 The user manual of the Roll Call software documentation shall describe how to use all the functional features of the software from a stand point of a novice user.
- 8.7 The software module manual of the Roll Call software documentation shall describe in details algorithms developed and used in modules, module operation requirements, and module operations.
- 8.8 The installation instruction manual shall provide enough information to compile the source code to produce executable code (provided the required compiler is available), to install the executable code on a fresh new Roll Call system, and to demonstrate the workability of the installed Roll Call software on the fresh installed Roll Call system.

9 Software Security Requirements

- 9.1 The Project Roll Call software shall be written to conform to as many of the recommendation pertaining to security as outlined in NIST publication FIPS 199 as deemed practical without conflicting with the overall goals and operation of the Roll Call software. (<http://csrc.nist.gov/publications/PubsFIPS.html>)
- 9.2 The Project Roll Call software shall be written to comply with as many of the requirements outlined in NIST Special Publication 800-53 as deemed possible without conflicting with the overall goals and operation of the Roll Call software. (<http://csrc.nist.gov/publications/PubsSPs.html>)
- 9.3 These requirements are outlined in Appendix A of this document.

10 Appendix A – Moderate System Required Controls

AC-2 ACCOUNT MANAGEMENT

The information system staff regularly manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews all information system accounts at least annually. The information system automatically terminates temporary and inactive accounts after 90 days of inactivity.

AC-3 ACCESS ENFORCEMENT

The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy and restricts access to privileged functions and security-relevant information to explicitly authorized personnel.

AC-5 SEPARATION OF DUTIES

The information system enforces separation of duties through assigned access authorizations.

AC-6 LEAST PRIVILEGE

The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

The information system enforces a limit of three (3) consecutive invalid access attempts by a user during a time period. The information system automatically locks the account/node for a period of ten (10) minutes when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

The information system displays an approved, system use notification message before granting system access informing potential users that they are accessing a government system and may be subject to monitoring. The system use notification message provides appropriate privacy and security notices and remains on the screen until the user take explicit actions to log on to the information system.

AC-11 SESSION LOCK (Note: Not applicable to web applications)

The information system prevents further access to the system by initiating a session lock after 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

The information system staff supervises and reviews user activities. The information system employs automated mechanisms (such as system logging functions) to facilitate the review of user activities.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

AC-17 REMOTE ACCESS

The organization authorizes, monitors, and controls all methods of remote access to the information system. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods, uses cryptography to protect the confidentiality and integrity of remote access sessions, controls all remote accesses through a limited number of managed access control points, and permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system (untrusted sources); and (ii) process, store, and/or transmit organization-controlled information using an external information system.

AU-2 AUDITABLE EVENTS

The information system generates audit records for appropriate events to protect the system from misuse, corruption and abuse. The information system provides the ability to compile all auditable events into a combined manageable log. The audit functionality of the system is periodically reviewed and updated to ensure its ability to detect current threats.

AU-3 CONTENT OF AUDIT RECORDS

The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

The information system staff regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or

suspected violations, reports findings to appropriate officials, and takes necessary actions. The information system automatically informs system personnel of inappropriate or unusual activities.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

The information system provides an audit reduction and report generation capability.

AU-8 TIME STAMPS

The information system provides time stamps for use in audit record generation and ensures accuracy by synchronizing system time with reliable clock.

AU-9 PROTECTION OF AUDIT INFORMATION

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

CA-3 INFORMATION SYSTEM CONNECTIONS

The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CM-2 BASELINE CONFIGURATION

The organization develops, documents, and maintains a current baseline configuration of the information system and updates the baseline configuration of the information system as an integral part of information system component installations.

CM-3 CONFIGURATION CHANGE CONTROL

The organization authorizes, documents, and controls changes to the information system.

CM-4 MONITORING CONFIGURATION CHANGES

The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

The organization: (i) approves individual access privileges and only allows authorized personnel to make changes to the information system's hardware or software; and (ii) generates, retains, and reviews records reflecting all such changes.

CM-6 CONFIGURATION SETTINGS

The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

**Project Roll Call
Requirements Specification**

March 19, 2009

The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

IA-2 USER IDENTIFICATION AND AUTHENTICATION

The information system uniquely identifies and authenticates users (or processes acting on behalf of users). The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 Level 1 compliant.

IA-4 IDENTIFIER MANAGEMENT

The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after 90 days of inactivity; and (vi) archiving user identifiers.

IA-5 AUTHENTICATOR MANAGEMENT

The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. (Authenticators in the case of the FCC will generally be defined as username and password authentication.)

IA-6 AUTHENTICATOR FEEDBACK

The information system obscures feedback (such as using asterisks in place of passwords) of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module, such as FIPS 140.

PL-2 SYSTEM SECURITY PLAN

The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

PL-5 PRIVACY IMPACT ASSESSMENT

A privacy impact assessment has been performed on the information system in accordance with OMB policy.

RA-2 SECURITY CATEGORIZATION

The information system and the information processed, stored, or transmitted by the system has been properly categorized in accordance with NIST FIPS 199 guidance. Designated senior-level officials within the organization review and approve the security categorizations.

SC-2 APPLICATION PARTITIONING

The information system separates user functionality (including user interface services) from information system management functionality.

SC-3 SECURITY FUNCTION ISOLATION

The information system isolates security functions from non-security functions.

SC-8 TRANSMISSION INTEGRITY

The information system protects the integrity of transmitted information.

SC-9 TRANSMISSION CONFIDENTIALITY

The information system protects the confidentiality of transmitted information.

SC-10 NETWORK DISCONNECT

The information system terminates a network connection at the end of a session or after 30 minutes of inactivity.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

SC-13 USE OF CRYPTOGRAPHY

For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with all applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. (ex. FIPS 140)

SC-14 PUBLIC ACCESS PROTECTIONS

The information system protects the integrity and availability of publicly available information and applications.

SC-15 COLLABORATIVE COMPUTING

The information system prohibits remote activation of collaborative computing mechanisms for example, video and audio conferencing capabilities and provides an explicit indication of use to the local users.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

SC-18 MOBILE CODE

The information system follows organization established usage restrictions and implementation guidance for mobile code technologies which include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

SC-23 SESSION AUTHENTICITY

The information system provides mechanisms to protect the authenticity of communications sessions.

SI-2 FLAW REMEDIATION

The organization identifies, reports, and corrects information system flaws.

SI-9 INFORMATION INPUT RESTRICTIONS

The organization restricts the capability to input information to the information system to authorized personnel.

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

The information system checks information for accuracy, completeness, validity, and authenticity.

SI-11 ERROR HANDLING

The information system identifies and handles error conditions in an expeditious manner without providing information to end users with insufficient need to know (ex. error messages displayed to normal end users detailing code or system specifications).

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

QUOTATION INSTRUCTIONS FOR POTENTIAL QUOTERS
RFQ09000091/ PROJECT ROLL CALL

A.) Price Quote Instructions:

1. Provide a price quote based on the work described in the requirement specification. Your prices shall be firm-fixed price and all costs necessary to perform the services identified in the requirement specification including labor, supplies, equipment, materials, travel/transportation, and all other direct costs. Provide any favorable incentives that you may be willing to offer (such as discounted pricing, special expertise, etc.).
2. Complete and return the attached Quotation Cover Page.
3. Complete and return the attached Past Performance Contract Information Sheet for all contracts of similar or the same type of services as described in the PWS, within the past four (4) years (i.e., January 2005 through August 2009).

B.) Basis for Award:

Total contract Price and Past Performance are significantly equal evaluation factors for contract award. **The successful offeror will be awarded** a single award to the offeror that provides the best value and is most advantageous to the Government.

**Federal Communications Commission (“FCC”)
Proposal Cover Page for RFQ09000091
Return via FAX - (202) 418-0237**

Company Name:
Company Representative for GSA Orders:
Contact Phone:
Contact E-mail:
Payment Terms:
GSA Schedule Number and expiration date:
Please check business size: () Large () Small () Minority () Women-owned
TIN or SSN:
DUNS #:
NAICs Code:
Complete Mailing Address:
Other Pertinent Information:
Offer Acceptance Period (no less than 90 days from due date of quote):
Name and Title of Person Authorized to Sign Offer:
Signature:
Date:

PROJECT ROLL CALL SOFTWARE - FEDERAL COMMUNICATIONS COMMISSION
PUBLIC SAFETY AND HOMELAND SECURITY BUREAU
PUBLIC COMMUNICATIONS OUTREACH AND OPERATIONS DIVISION

PAST PERFORMANCE CONTACT INFORMATION SHEET

Offeror Information:

Name of Offeror Providing Services: _____

Address: _____

Past Performance Reference Information:

Name of Company/Organization Receiving Services: _____

Address: _____

Telephone: _____ FAX: _____

Contract Information:

Contract Number: _____ Dollar Value (Annual): _____

Performance Period: _____ Performance Location: _____

Type of Contract (Check all that apply):

Fixed Price _____ Cost Reimbursement _____ Other (specify) _____

Negotiated _____ Sealed Bid _____ Competitive _____ Non-Competitive _____

Basis of Payment:

Labor/Equipment Hours _____ Other (specify) _____

Type & Extent of Subcontracting: _____

Description of Services Provided: _____
