



INCORPORATED COUNTY OF LOS ALAMOS
REQUEST FOR PROPOSALS
CAD, Mobile, RMS, JMS (CMRJ) - INTEGRATED PUBLIC SAFETY SYSTEM
RFP No. 24-56

Proposal Release Date – February 2, 2024

Proposal Submittal Due Date – March 19, 2024 2:00 p.m. MST

Any changes/additions from previous RFP23-62 are denoted in red

No Changes have been made to the Functional Specification attachments from the previous RFP 23-62

Addenda Questions/Responses from previous RFP 23-62 cycle have been attached to this document as Exhibit Q.

The non-mandatory pre-proposal conference will be held Tuesday February 12, 2024, at 1:00 pm (MST).

Integrated Public Safety System Pre-Proposal Meeting
Monday, February 12, 2024, 1:00 PM - 2:00 PM (MST)

Please join my meeting from your computer, tablet or smartphone.
<https://meet.google.com/wdi-wphg-uzt>

You can also dial in using your phone.
United States: +1 470-268-2238

Access Code: 470 994 209#

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
<https://meet.google.com/>

Contents

Contents	2
1 General Information	7
1.1 RFP Information	7
1.2 RFP Submission Information.....	7
1.2.1 RFP Submission Procedure Change	7
1.2.2 Electronic Submission	7
1.2.3 Paper Form Submission.....	8
1.3 Submission Instructions	9
1.3.1 Contact Information.....	10
2 Project Information	11
2.1 Needs Statement.....	11
2.2 General Background	11
2.3 Agency Background.....	11
2.3.1 Los Alamos County Emergency Communications Center	11
2.3.2 Los Alamos Police Department	13
2.3.3 Los Alamos County Detention Center.....	14
2.3.4 Los Alamos County Fire Department.....	14
2.3.5 Los Alamos County Information Management Division.....	15
3 Scope of Work.....	17
3.1 Software Modules or Components.....	19
3.2 Licensing.....	22
3.3 Interfaces.....	23
3.3.1 Current Interfaces.....	23
3.3.2 Required Interfaces	24
3.3.3 Other Interfaces.....	25
3.4 Project Management Services.....	25
3.5 Planning	26
3.6 Performance Criteria.....	27
3.6.1 Prosecution of Work	27
3.6.2 Performance Requirements.....	27
3.6.3 Ongoing System Performance	27

3.6.4	System Performance Profile	28
3.6.5	System Response Times	28
3.6.6	Computer System Availability.....	29
3.7	Support and Maintenance Requirements	30
3.7.1	Application Errors.....	30
3.7.2	Error Reporting	30
3.8	Technical Support Center.....	31
3.8.1	Software Malfunction Severity Level Definitions.....	31
3.8.2	Response Time Credits	32
3.9	Legacy Data Conversion.....	33
3.10	Testing.....	35
3.10.1	Functional Acceptance Testing.....	35
3.10.2	Integration Testing	35
3.10.3	Thirty (30) Day Reliability Testing (Final Acceptance).....	36
3.11	Training.....	36
3.11.1	Training Guidelines	37
3.12	Documentation.....	38
3.13	Deployment Plan.....	39
3.14	Pre and Post Cutover Support	40
3.15	Data Requirements at Contract Termination.....	40
4	Proposal Review and Evaluation (Guidelines and Schedule)	40
4.1	Process	40
4.2	Evaluation Criteria	41
4.3	Evaluation Method.....	42
4.3.1	Step 1 – Offeror Scoring.....	42
4.3.2	Step 2 – References, Demonstrations, Site Visits and other elements as may be determined by County at time of issue of Step 2 of the RFP.....	43
4.3.3	Final Recommendation for Award.....	43
4.3.4	Discussions with finalist offeror(s).....	43
4.4	Evaluation Criteria	44
4.4.1	Step 1	44
4.4.2	Stage 2 – (short-listed offerors only)	45

4.5 Award Of Solicitation	46
4.6 Obligations Of Federal Contractors and Subcontractors; Equal Opportunity Clauses	46
4.7 Illegal Acts	46
4.8 Certification Form Regarding Debarment, Suspension, And Other Responsibility Matters	47
4.9 Campaign Contribution Disclosure Form	47
4.10 Verification Of Authorized Offeror	47
5 Proposal Format	47
5.1 Format	47
5.2 Title Page	49
5.3 Letter of Transmittal	49
5.4 Table of Contents	49
5.5 Executive Summary	50
5.6 Company Background and Experience	50
5.7 Project Understanding	51
5.8 Project Staffing and Organization	51
5.9 Project Work Plan and Schedule	52
5.10 System Hardware and Infrastructure Description	54
5.10.1 Hardware Requirements	54
5.10.2 General Requirements	55
5.10.3 Mission Critical Server Hardware Requirements	56
5.11 Software Maintenance, Updates, and Customer Support	56
5.11.1 Warranty Provisions	56
5.11.2 General Maintenance Provisions	58
5.11.3 System Warranty and Ongoing Maintenance Support	59
5.11.4 Help Desk Support	59
5.11.5 File Back-Up/File Recovery	59
5.11.6 Additional Support Information Requirements	59
5.12 Other Documents	60
5.13 Appendices	60
5.13.1 Functional Specification Workbooks (Appendix A)	61
5.13.2 References (Appendix B)	63
5.13.3 Resume of Key Personnel (Appendix C)	64

5.13.4 Notification to Propose (Appendix D).....	64
5.13.5 Addenda Acknowledgement (Appendix E).....	64
5.13.6 Cost (Appendix F)	64
5.13.7 Proposal Forms	66
Exhibit A – Functional Specification Workbooks	67
Exhibit B – Reference Form	68
Exhibit C – Resume Form.....	69
Exhibit D – Notification to Propose Form.....	70
Exhibit E – Addenda Acknowledgement Form	71
Exhibit F – Proposal Cost Summary Sheet and Proposal Cost Sheets	72
Exhibit G – Verification of Authorized Offeror Form.....	80
Exhibit H – Primary Covered Transactions Certification Form	83
Exhibit I – Campaign Contribution Disclosure Form.....	85
Exhibit J – Confidential Information Disclosure Statement	88
Exhibit K – Incorporated County of Los Alamos Technical Questions	90
Exhibit L – Incorporated County of Los Alamos Technical Standards	93
Exhibit M – Sample Services Agreement.....	97
Exhibit N – LiNX Interface Questionnaire	106
Exhibit O – CJIS Security Addendum	108
Exhibit P – Sample Reports	114
Exhibit Q – Addenda Questions from RFP 23-62	115
Exhibit R – E-Signature Policy	119
Exhibit S – Records And Information Management Governance Policy	123
Exhibit T – IT Usage and Security Policy	132

SPECIAL INFORMATION RELATED TO THIS RFP

This is a Multi-Step RFP. This RFP document comprises Step 1. A description of the process for this Multi-Step RFP is as follows:

Step 1 - After Proposals are received in response to Step 1 of the RFP, the evaluation committee will conduct an evaluation of the responses, using the evaluation criteria set forth in this Step 1. During Step 1, County may, at County's sole option, request clarification from any Offerors for the purpose of adjusting initial Step 1 scoring.

Step 2 – Step 2 of the RFP will then be issued, limited to those Offeror(s) whose offers have been determined by the evaluation committee to be qualified under the criteria set forth in the first solicitation (Step 1). County anticipates that Step 2 will include but will not necessarily be limited to a demonstration of the Offeror(s) software via a virtual meeting format. As part of Step 2, discussions may be conducted with responsible offerors who submit proposals determined to be reasonably likely to be selected for award for the purpose of clarification to ensure full understanding and conformation with the solicitation requirements. County reserves the right to request a best and final offer. Following evaluation of Step 2 responses, award shall be made to the responsible offeror whose proposal is determined in writing by the evaluating committee to be the most advantageous to the County, taking into consideration the evaluation factors set forth in the request for proposals. County reserves the right to modify Step 2 evaluation criteria prior to issuance of Step 2.

1 General Information

**INCORPORATED COUNTY OF LOS ALAMOS
PROCUREMENT DIVISION
101 Camino Entrada, Building 3, Los Alamos, New Mexico 87544
(505) 663-3507**

1.1 RFP Information

Advertised: February 1, 2024

Closing Date: March 19, 2024

Non-Mandatory Pre-Proposal Conference: [February 12, 2024](#)

<p style="text-align: center;">Request for Proposals (“RFP”) RFP Number: 24-56 RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM</p>
--

1.2 RFP Submission Information

1.2.1 RFP Submission Procedure Change

Due to the current COVID-19 (coronavirus) pandemic and Public Health Emergency declaration by the New Mexico Governor, until further notice, the following procedure is in effect: Proposals in response to this Requests for Proposals (RFP), may be submitted either in paper form, in a sealed envelope, or electronically by email in PDF format. All other requirements stated in the solicitation document remain unchanged and in effect.

Only one of the following submission methods is required:

1.2.2 Electronic Submission

Emails should be addressed to: lacbid@lacnm.us. Subject line must contain the following information: **RESPONSE – RFP 24-56 CMRJ – Integrated Public Safety System.**

It is strongly recommended that a second, follow up email (without the proposal included or attached) be sent to [Derrill Rodgers, Deputy Chief Purchasing Officer](mailto:derrill.rodgers@lacnm.us) at derrill.rodgers@lacnm.us to confirm the Proposal was received.

RFP No. 24-56
Issued by Procurement Division: [D. Rodgers](#)

The body of the email must contain enough information for the identity of the Proposer to be clear, including company name, name of person sending the email, and contact information including email address and phone number.





Only emails with proposals received in the lacbid@lacnm.us email box prior to **2:00 p.m. Mountain Time, March 19, 2024** will be reviewed.

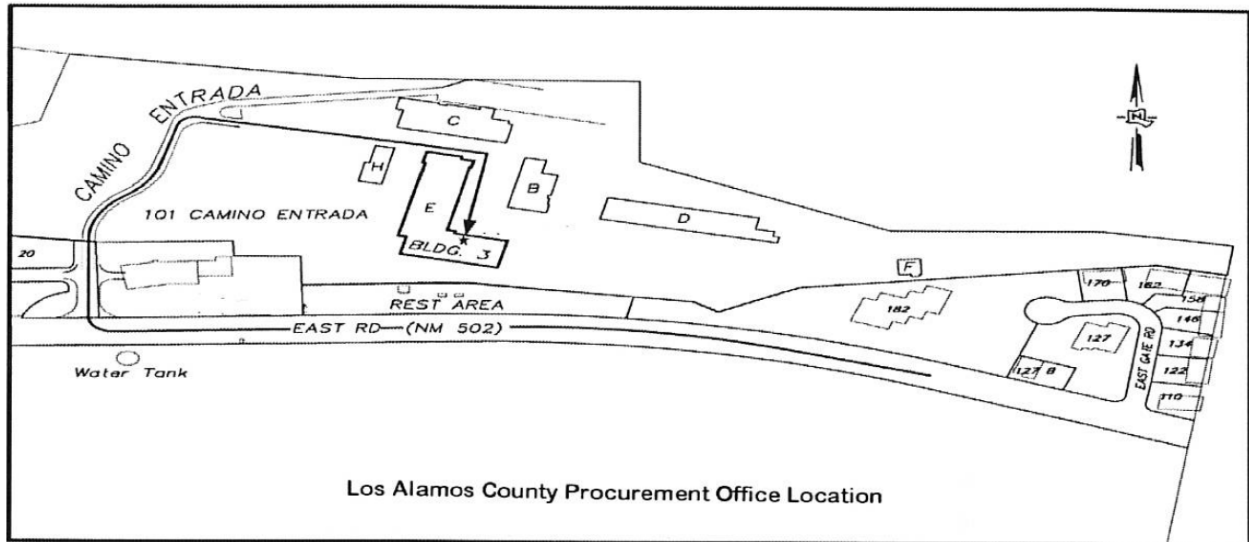
Proposals submitted by email will be opened only after the closing date and time stated in the solicitation document.

1.2.3 Paper Form Submission

Sealed proposals in one (1) clearly labeled unbound original, three (3) bound copies and one (1) USB flash drive or CD, will be accepted at the Office of the Chief Purchasing Officer, Procurement Division - 101 Camino Entrada, Building 3, Los Alamos, NM 87544, until **2:00 p.m. Mountain Time, March 19, 2024** for this solicitation. **Clearly mark the RFP Number and Name and Offeror on the outside of the sealed proposal, including outer envelope and/or shipping label.** The USB flash drive or CD should be clearly identified. It is the responsibility of the Offeror to ensure that the information submitted in both its written response and the electronic version are consistent and accurate. If there is a discrepancy between what is provided on the paper document and the USB flash drive or CD, the written paper response shall govern.

Directions to Procurement office:

-  1. Drive WEST on NM-502 to Los Alamos.
 - Camino Entrada (formerly known as Airport Basin) is 0.4 miles past East Gate Drive, just past East Entrance Park Rest Area.
-  2. Turn RIGHT on Camino Entrada.
 - The road slopes downhill and curves to the right.
-  3. Take the second RIGHT into the driveway through the gated fence (before the stone sign “Pajarito Cliffs Site”).
 - Follow the signs to Building 3, the L-shaped building in the center of the complex.
 - If you pass the Holiday Inn Express and the Airport, you’ve gone too far.
-  4. Enter glass door marked “PROCUREMENT.” *See map below.*



1.3 Submission Instructions

1. The Incorporated County of Los Alamos (“County”) invites Proposals from all qualified respondents. No Proposal may be withdrawn after the scheduled closing time. Proposals will not be accepted after the scheduled closing time. **Please make note of the submittal requirements outlined in this solicitation.** Read and follow the instructions carefully. **Include the required documents provided in this RFP as part of your submittal packet.** Any misinterpretation or failure to comply with the submittal requirements could result in rejection of the proposal. Proposal preparation is at the Offeror’s expense.
2. Any change(s) to the solicitation will be conveyed through the written addenda process. Read carefully and follow all instructions provided on any addendum, as well as the instructions provided in the original solicitation.
3. Any questions must be received in writing by **2:00 p.m. Mountain Time, March 5, 2024.**
4. The County reserves the right, at its sole discretion, to accept or reject any proposals; to waive any and all irregularities in any or all statements or proposals; to request additional information from any or all respondents; and to award a contract to the responsible Offeror whose proposal is most beneficial to County. While County intends to execute a contract for the services listed herein, nothing in this document shall be interpreted as binding County to enter into a contract with any Offeror or Proposer.
5. Bids and Proposals are Public Records. Pursuant to the New Mexico Inspection of Public Records Act, NMSA 1978, Chapter 14, Article 2, all materials submitted under this RFP/IFB shall be presumed and considered public records. Except to the extent any

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

information may be protected by state or federal law, proposals shall be considered public documents and available for review and copying by the public.

6. The County is contemplating a multi-term contract as a result of this RFP. The term of the contract may be for a period of up to 15 years. This is the written determination of the Chief Purchasing Officer which: such a contract will serve the best interests of the County by promoting economies in County procurement.
7. Proposers are notified that they must propose pricing for each potential year of the contract.
8. Proposers/Offerors are informed that State law requires that all foreign corporations (NMSA 1978 §53-17-5) and limited liability corporations (NMSA 1978 §53-19-48) procure a certificate of authority to transact business in the state prior to transacting business in the state of New Mexico.
9. The Chief Purchasing Officer has determined a preference is applicable to this offer. An offeror must submit a written request for preference, with a copy of the state-issued preference certificate, with its proposal to qualify for this preference. Ref. County Code Section. 31-261(b) and Section 13-1-21 NMSA 1978 et al.
10. **Non-mandatory Integrated Public Safety System Pre-Proposal Meeting**
Tues, February 12, 2024, 1:00 PM - 2:00 PM (MST).

1.3.1 Contact Information

1. For project-specific information, contact [Katherine Stoddard](#), at katherine.stoddard@lacnm.us; (505) 661-3435.
2. For procurement process information, contact [Derrill Rogers](#), Deputy Chief Purchasing Officer, at derrill.rodgers@lacnm.us; (505) 663-3507.

2 Project Information

2.1 Needs Statement

Incorporated County of Los Alamos (County) invites proposals from qualified firms that possess the qualifications, experience, and knowledge to provide a fully integrated, **single vendor solution** for Computer Aided Dispatch (CAD) system, Mobile Data System (MDS), Law Enforcement Records Management System (LERMS), Jail Management System (JMS) and associated interfaces including Fire Records Management System (FRMS) and electronic Patient Care Reporting (ePCR).

2.2 General Background

County is located in the north-central part of New Mexico, encompasses 110 square miles, and is situated at the foot of the Jemez Mountains on the Pajarito Plateau, with an elevation ranging from 6,200 feet to 9,200 feet. Two (2) distinct communities, Los Alamos Townsite and White Rock, each with its own visitor center, are home to approximately 19,000 people. The County is mostly known for the historic accomplishments of its largest employer, Los Alamos National Laboratory (LANL), and continues to gain notice for its vast scenic assets and recreational opportunities. Due to the presence of the LANL, the daytime population of the County increases significantly during normal business hours.

Table 1 (Based on 2020 Census)

Cities/towns/villages	Population
Los Alamos	13,179
White Rock	5,852

Visit the Los Alamos County website (www.losalamosnm.us) and the tourism website (www.visit.losalamos.com) for more information.

2.3 Agency Background

The County is served by the Los Alamos County Emergency Communications Center (ECC), the Los Alamos Police Department (LAPD), the Los Alamos County Detention Center (DC), and the Los Alamos Fire Department (LAFD). The Emergency Communications Center and the Detention Center fall under the umbrella of the Los Alamos Police Department.

2.3.1 Los Alamos County Emergency Communications Center

The ECC provides 9-1-1 call-taking and dispatching services for the County. The ECC provides 24 hours a day, 365 days a year connection between the community, the Los Alamos Police

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

Department, and the Los Alamos Fire Department. In addition, it provides service for the Bandelier National Monument Park Rangers and after-hour service to other County Departments, such as the Utilities, Facilities and Parks Divisions. The ECC is an accredited Public Safety Answering Point, having been awarded accreditation by the New Mexico Emergency Communications Professional Standards Council in July 2022.

The ECC is also responsible for compliance with all the rules and regulations concerning the National Crime Information Center (NCIC), radio communications, telephone communications, teletype and automated data communications, alarm monitoring and all other duties, responsibilities and tasks assigned to the ECC. Call for service (CFS) volume statistics for the years 2018-2022 are included in Table 2.

Table 2

Description	2018	2019	2020	2021	2022
Emergency and non-emergency phone calls processed	53,956	51,171	*43,000	47,300	50,585
Calls For Service - LE	14,216	13,439	17,657	14,291	14,831
Calls For Service – Fire/EMS	2,332	2,422	2,012	2,400	2,459
Transferred/Advised	2,332	2,923	2,453	2,503	3,980
Total CAD Entries	18,940	18,784	22,122	19,194	22,037

**Phone software was replaced in April 2020, and data was lost for the first quarter.*

The ECC operates out of two locations, the primary location in Los Alamos, located within the Police Department, and a secondary location in White Rock, located within Fire Station 3. The secondary location is utilized as an alternate or backup Emergency Communications Center and is not manned unless needed as an alternate or backup center, or for special events. The County leverages their current WebCAD product (represented in this RFP as “view only CAD”) significantly, allowing inquiry access to the majority of personnel at both the Fire Department and the Police Department.

Personnel (sworn and civilian): 16

CAD Workstations: 9

CAD inquiry only (web CAD or view only CAD client): 9

Number MDCs/Tablets with full CAD installed: 2

Maximum concurrent users: 50 (including view only CAD)

CPE: Vesta

CPE Vendor: ConvergeOne

The radio system is a trunked digital Harris radio system, with all positions at both ECC locations operating the radio through the Symphony console. The radio system is owned by the Los Alamos National Laboratory.

The current CAD in use by the ECC is the Infor Public Sector EnRoute system, which was implemented in December 2016.

2.3.2 Los Alamos Police Department

The Los Alamos Police Department (LAPD) is a CALEA accredited, full-service law enforcement agency responsible for a wide variety of services to Los Alamos residents and visitors. LAPD includes four Bureaus: The Operations Bureau, the Emergency Management Bureau, the Professional Standards Bureau, and the Staff Services Bureau. LAPD operates the County Detention Center and is also responsible for Animal Control, including the operation of the County Animal Shelter.

The LAPD Records Division reports to the Professional Standards Commander. Records is supervised by the Records Manager, an Officer Manager or Management Analyst, and is responsible for the collection, collation, approval, filing and safekeeping of all Police reports (e.g., incident, crime, accident, citations, etc.) as well as all other documents required by law or ordinance. This Section is also responsible for handling all subpoenas, warrants, Inspection of Public Records Act (IPRA) requests, providing criminal records checks, civil process, and other duties as assigned. The Records Section also prepares reports both internally and externally for purposes of research, mandated crime reporting to the FBI for the Uniform Crime Report using the FBI's National Incident-Based Reporting System (NIBRS), and other reports as directed. The Records Manager, in addition to supervising the Records Section staff, will be responsible for management of the Department's automated and paper records (including the archives at the County warehouse), Department payroll and timesheets, website maintenance and development, ensuring quality service to internal and external customers, providing support to the Office of the Chief of Police and other duties as assigned by the Professional Standards Commander. All personnel within Records will fulfill all the responsibilities encompassed within the job description for each respective position.

CFS and report statistics for 2018 through 2022 are included in Table 3.

Table 3

Description	2018	2019	2020	2021	2022
Calls For Service	14,216	13,439	17,657	14,291	14,831
Reports Taken	873	765	690	723	766
Records Processed	4172	5,266	3,861	4,706	4771

Personnel (sworn and civilian): 83
 LERMS workstations: 65
 Number MDCs/Tablets: 35
 Maximum concurrent users: 40

The current LERMS in use by the Los Alamos Police Department is the Executive Information Services, Inc. system (EIS), which was implemented in January 2017.

2.3.3 Los Alamos County Detention Center

The Los Alamos County Detention Center is responsible for the intake, processing, classification, confinement, and care of individuals lawfully arrested, charged, and placed in his or her care. The facility houses pre-trial detainees and prisoners sentenced to one year or less and does accommodate temporary regional and state holds when circumstances warrant or upon request. The Los Alamos County Detention Center has 32 beds, with separate housing pods for male and female inmates, as well as separate Court Housing and visitation rooms. The facility has a full-service laundry room, multiple showers, an outdoor recreation room, a weight room, and library. The Detention Center offers several programs to provide opportunities for inmates. Statistics for average daily population and number of annual bookings from 2018 through 2022 can be found in Table 4.

Table 4

Description	2018	2019	2020	2021	2022
Average Daily Population	17	8	9	6	3
Number of Bookings per year	376	210	195	123	109

Personnel: 16

Jail workstations: 7

Maximum concurrent users: 5

Number of tablets/handheld devices (current and/or anticipated): 4

The current Jail Management System in use by the Detention Center is EIS, which was implemented in January 2017.

2.3.4 Los Alamos County Fire Department

The Los Alamos County Fire Department serves Los Alamos County and the Los Alamos National Laboratory. They provide fire suppression, emergency medical services, technical rescue, hazardous materials mitigation, aviation rescue, fire prevention, fire investigation, code enforcement, public education, and domestic preparedness planning and response. LAFD provides these services with a career staff of 150 personnel (140 uniformed/10 civilian) and operates out of five stations, with plans to build a sixth station.

Table 5

Calls For Service	2018	2019	2020	2021	2022
Los Alamos County Fire Dept	2,425	1,994	1,732	2,400	2,458
Fire	1,104	601	570	807	1,118
EMS	1,321	1,393	1,162	1,593	1,340

Number of MDCs/tablets: 70
FRMS software offeror: ESO Firehouse*

* Los Alamos County Fire Department is looking into replacing the current FRMS system in the near future which will need to be accounted for once a selection has been made to provide a CAD-to-FRMS interface.

2.3.5 Los Alamos County Information Management Division

The County Information Management Division (IM) ensures networking, voice, and data telecommunications, help desk and enterprise applications are available to support County operations.

COMPUTING AND NETWORKING BACKGROUND

** Network Overview

The County presently has two existing dispatch centers in Los Alamos and White Rock. These house a total of nine fully equipped CAD dispatch workstations running Windows 10 and dedicated connections to the County network, servers, and storage assets.

Presently, CMRJ computing services are provided using computing and storage assets located in a single central County facility. The new CAD computing and storage assets will continue to be housed in this facility. The County is investigating possible future use of a second data center operated by a third party for the County.

In its current operation, the County relies on Infor Enroute software and support services to provide CAD, Mobile CAD, Web CAD, CFS export to FRMS, and CAD database instances, backups of these databases and high availability clustering. Executive Information Systems, EIS, provides, maintains, and upgrades the on-premises police and jail records system applications and databases which are also running on County owned and operated infrastructure.

** Server and Network Operations.

Currently, internal network operations, excluding cellular data services, along with hardware and operating system maintenance are the primary responsibility of County IM personnel. Additionally, contractor personnel partner with County IM staff as necessary to maintain any CMRJ software related interfaces to network infrastructure and to remote users via mobile devices. All network connections linking computing resources, physical sites, end users and

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

mobile devices and their users are maintained by County personnel. The County has no plan to deviate from this structure.

County IM will incorporate new CMRJ servers to its existing backup for disaster recovery purposes, therefore disaster recovery is not within the scope of this RFP.

** Current High Availability Overview

Current CMRJ services and storage are running in a two-node Windows failover cluster using two Dell servers each equipped with Intel Xeon 2.30 GHz dual core processors and 384 GB of memory. The hypervisor for the cluster's virtual machines is Microsoft Hyper-V running on the Windows Server 2012R2 Datacenter operating system with a planned update to Windows Server 2019 Datacenter. The present CMRJ system cluster has an allocated storage capacity of 2.7Tb for each node in the cluster or 5.4Tb in total. It is important to note that the County wishes to move away from use of the Hyper-V hypervisor and now requires all new virtualization solutions to be compatible with the VMWare hypervisor. Databases are presently running on MSSQL Server 2014 with a planned update to MSSQL Server 2019 Enterprise.

The County CAD environment includes a network infrastructure (i.e., switches, routers, firewall, intrusion detection software) which maintains connectivity to external interfaces as well as County-owned workstations running various, limited functionality versions of the CAD software. It is the County's expectation that the CAD Contractor will provide a system design that includes an overview of their production, testing, training, and backup environments, as well as any network hardware and software details needed to allow interconnectivity between their system and internal and external networks identified in this document.

** Mobile Computing

Mobile computer hardware is maintained by the County's Information Management Division. Connectivity between mobile computers and other county computing assets is through either wired, wi-fi, or cellular data connections depending on the physical location of the mobile computer. The fleet of mobile computers presently in use by police officers and fire crews are primarily Getac brand rugged laptops and tablets. These machines have the following minimum specifications: Windows 10, Intel i5 x64 processor, 8 Gb memory, 1 GB wireless networking, 10-14 screen size, 128Gb SSD storage and a dedicated GPS receiver. County personnel ensure each mobile computer has network connectivity and up to date applications as needed. Contractors provide a wireless cellular virtual private network for the current fleet of CMRJ mobile computers to access County networks. No substantive changes to the mobile computer fleet as described here are anticipated at this time.

3 Scope of Work

For award of an agreement, County requires a Not-to-Exceed (“NTE”) amount for total compensation. In order to estimate a total NTE amount of a potential agreement, County requests that Offerors submit proposals with proposed pricing or a proposed pricing mechanism for a **fully integrated, single vendor solution for CAD, MDS, LERMS, JMS, as well as** interfaces to the County Fire Department’s FRMS and ePCR systems, which allow for calculation of a Not-to-Exceed amount. **(As defined in the high level requirements below – 3.c) The** County is seeking implementation of a system that is an on-premise solution that includes environments for production, testing, and training. **Refer to “Computing and Networking Background” on pages 15 and 16 for details regarding the County’s current operating environment, which also includes preferences for configuration of future system deployments.**

County seeks a tier 1 solution, based on key constituent needs (e.g., Los Alamos National Laboratory) and the high Insurance Service Office (ISO) rating maintained by the Los Alamos Fire Department that is of critical importance to the Los Alamos community. The offeror must specify all required hardware, software, and professional services. The solution provided must adhere to applicable aspects of the County’s technology standards located in [Exhibit L](#) and must also include the logical architecture to include how the solution provides High Availability (HA) and any required network routing.

The successful offeror shall be capable of providing a fully integrated operational turnkey system that includes installation, training, testing, user & system documentation, acceptance testing support, and cutover support. Conversion services, system warranty, and software maintenance must be part of the offeror’s response.

County expects to award a maintenance contract for 15 years. The proposal should also include costs for a 15-year maintenance plan that outlines the yearly percentage of increase or decrease.

The following high-level requirements have been identified for this procurement:

- a. Solution has been successfully implemented in at least five (5) sites; two (2) of which are similar in size and requirements to the County’s public safety environment
- b. The ability to operate more efficiently through automated workflow
- c. Fully integrated* across CAD, MDS, LERMS, and JMS

***In the context of a public safety software solution with multiple applications, "fully integrated" refers to the seamless and efficient interoperability of all individual applications within the solution. This integration involves the ability of different software components to work together cohesively, sharing data, functionalities, and workflows without encountering significant compatibility issues or requiring complex manual interventions.**

Key characteristics of a fully integrated public safety software solution include:

1. **Unified Data Management:** The applications within the solution share a common database or data architecture, ensuring consistency and real-time updates across all modules. This enables users to access accurate and up-to-date information from any part of the system.
 2. **Smooth Workflow Automation:** Workflows across various applications are interconnected and automated, eliminating redundant data entry and manual handoffs. This enhances overall operational efficiency and reduces the likelihood of errors.
 3. **Single Sign-On (SSO) Capability:** Users can log in once and gain access to all integrated applications without the need to repeatedly enter credentials. This simplifies the user experience and enhances security by centralizing access control.
 4. **Cross-Application Communication:** The appropriate applications can communicate seamlessly with each other, allowing data and processes to flow smoothly between different modules. This enables comprehensive and real-time reporting and analysis across the entire solution.
 5. **Consistent User Interface (UI):** A fully integrated solution maintains a consistent look and feel across all applications, making it easier for users to navigate and use various modules. This consistency contributes to a more intuitive user experience.
 6. **Scalability and Flexibility:** The solution is designed to accommodate growth and changes in business requirements. New modules or functionalities can be added without disrupting existing integrations, ensuring adaptability to evolving business needs.
 7. **Centralized Administration and Security:** Administration tools are centralized, simplifying the management of user access, security policies, and system configurations across all applications. This centralization enhances control and reduces the risk of security vulnerabilities.
 8. **Vendor Support and Updates:** The software solution is provided by a single vendor and supported by the same single vendor or a tightly coordinated group of vendors (e.g., ESRI support of GIS mapping within CAD), ensuring that updates, patches, and support are consistently applied across all integrated applications.
- d. The ability to meet state and federal reporting requirements
- e. Data analytics and ad-hoc reporting designed to be used by end users

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

- f. Includes system administration and user documentation
- g. System that is able to restrict attachments to records to be only .JPG or .PDF
- h. Available, high quality technical and end user support (call center)
- i. Allows for exporting data to other applications including MS Office products and Adobe PDF
- j. Provides highly customizable agency specific reports.
- k. The system is scalable and can be expanded to include additional modules, functionality, interfaces, and additional participating entities
- l. Has dashboard reporting capabilities
- m. Supports information sharing across departments and agencies
- n. Software is regularly updated and actively maintained
- o. **Must propose a High Availability deployment with the ability to expand High Availability to multiple secondary physical operational location(s)**
- p. **On-premise data conversion with seamless integration into the appropriate applications within the new solution (Provisioning converted data from outside the new solution is not an acceptable option)**

The County prefers the following technical environment:

- a. Browser-based client with multi-task capabilities
- b. Solution that can be deployed via intranet/WAN
- c. Microsoft SQL Server database version 2016 through current
- d. VMware based virtualized windows server environment (OS 2019 or current)
- e. Capability for searching file attachments in common formats
- f. Modern solution built using industry standards and best practices
- g. Supports single sign on capabilities (Active Directory)
- h. Compatibility/integration with Microsoft Office

3.1 Software Modules or Components

The County and the agencies it serves are seeking an integrated public safety system that includes the following software components/modules.

Table 6

Multi-discipline CAD	
Software Module or Component	Required = R Desired = D
A multi-discipline CAD system	R
Leverages integrated ESRI mapping technology, such as ArcGIS, and the ESRI map data managed by the County	R
Leverages AVL to improve unit location and status tracking	R

Provides a User Interface that is highly configurable, supports an intuitive call entry and call management process, and provides a modern look and feel	R
Is tightly integrated with the proposed law mobility solution	R
Is tightly integrated with proposed LERMS and JMS system	R
Interfaces with/to ProQA Paramount EMD, EFD, EPD	R
Interfaces with/to NMLETS/NLETS/NCIC	R
Interfaces with/to Harris radio system	R
Interfaces with/to WestNet	R
Interfaces with/to ePCR	R
Interfaces with/to First Due	R
Interfaces with/to WatchGuard	D
Interfaces with/to Call Logging Recorder	D
Interfaces with/to ASAP to PSAP (incoming Alarm calls)	D

Mobile solution for Law, Fire, and EMS	
Software Module or Component	Required = R Desired = D
CAD to Field-based reporting information transfer	R
CAD to ePCR information transfer	D
CAD to FRMS information transfer	R
Interface to TRACs	R
Field-based Reporting System for Law Enforcement	
Software Module or Component	Required = R Desired = D
TraCS e-Citation/e-Accident application interface	R
Accident reporting with State upload capability	R
Case entry	R
Field contacts/interviews	R

Law Enforcement Records Management System	
Software Module or Component	Required = R Desired = D
Master Name, Master Vehicle, and Master Location shared with CAD, MDS, and LERMS, and JMS	R
Accidents module (integrated with mobile State submission application TraCS)	R
Animal Control module	R
Career Criminal tracking	R

Case Management module	R
Civil Process module	R
Crime and Data Analysis module	R
NIBRS Reporting capability	R
Narcotics module	D
Gang Tracking module	D
Fleet Management module	D
Impounded Vehicle module	D
Photo Imaging/Line-ups module	R
Warrants/Orders of Protection module(s)	R
Personnel Administration and Training module	D
Tickets/Citations module (integrated with State e-Citation application - TraCS)	R
Asset Tracking/Management module	D
Forms tool (preference for native forms tool, will accept tightly interfaced 3 rd party tool if native tool not available)	R
Interfaces with/to LInX	R
Interfaces with/to Property Room bar-coding	R
Interfaces with/to BEAST – Porter Lee Evidence Management System	D
Interfaces with/to Asset Management bar-coding	R
Interfaces with/to Forms Tool (if not provided within base LERMS product)	D
Interfaces with/to TraCS - State Accident/Citation upload	R
Interfaces with/to FullCourt – Records / Judiciary information management	R
Interfaces with/to Prosecuting Attorney via web/browser-based application	D
Jail Management System	
Software Module or Component	Required = R Desired = D
Master Name integration with CAD, MDS, and LERMS	R
Arrest/pre-book form processing from law mobile application	R
Booking module	R
Inmate Property Intake and Tracking module	R
Classification module	R
Housing module	R
Personnel Administration and Training module	D
Personnel Activity Reporting and Scheduling module	D
Personnel and Facility Equipment Tracking module	D

Officer Activity log	R
Inmate Scheduling and Tracking module	R
Inmate Activity Tracking module	R
Inmate Movement module (with handheld integration)	R
Inmate Programs module	R
Inmate Case Management module	R
Inmate Incident and Disciplinary module	D
Inmate Grievance Tracking Module	D
Inmate Contacts module	R
Inmate Financial Management module	D
Jail Commissary module	D
Jail Data Analysis and Reporting module	R
Forms tool <i>*preference for native forms tool, will be accepted tightly interfaced 3rd party tool if native tool not available</i>	R
Monthly reporting capability to include breakdown by felony misdemeanor, sex, and ethnicity/race	R
Interfaces with/to Livescan (Safran MorphoTrak)	R
Interfaces with/to Guard 1 RFID Inmate Movement Tracking	R
Interfaces with/to VINE	R
Interfaces with/to Data sharing with 3 rd party medical records provider(s)	D
Interfaces with/to Inmate Phone System (Securus)	D
Interfaces with/to Forms Tool (if not provided within base JMS product)	D

3.2 Licensing

A site license is preferred but offerors should submit pricing using the license model that best minimizes the cost to the County without being too restrictive related to future growth. The information typically needed for licensing costs is in Table 7 below and is shown by the agency. (See [Exhibit F](#) for the required cost sheet.) If an offeror uses another approach for licensing, please submit this information by the question cutoff date so it can be addressed.

Table 7

Agency	Application	Description	# of devices	# of users	# of concurrent users
LACDC	CAD – Full	Access to Full CAD	15	20	15

LAPD	CAD - View Only	Access to CAD in view-only mode, WebCAD	40	85	40
LAPD	LERMS (full user)	Full RMS user	65	80	40
LAPD	LERMS (view only)	Access to RMS in view-only mode	25	25	25
LAPD	Mobile	Mobile-CAD (laptop) to include mapping and AVL	35	45	20
LAPD	Mobile Field Reporting	Field-based reporting (laptop)	35	45	20
LAFD	CAD - (view only)	Access to CAD in view-only mode, WebCAD	70	150	100
LAFD	Mobile	Mobile-CAD (laptop/tablet) to include mapping and AVL	70	150	70
JMS	JMS (full user)	Full JMS user	7	16	5

3.3 Interfaces

The following interfaces have been identified as part of this project.

3.3.1 Current Interfaces

The interfaces defined in Table 8 below are the interfaces currently in use with the Infor/EIS software. These interfaces are required.

Table 8

Interface	Current Solution Provider
E911	VESTA
Medical and Fire protocols	Paramount Priority Dispatch Fire and Medical Modules
Livescan	Executive Information Services
Automatic Vehicle Location System	EnRoute AVL
Mobile Data Computer	EnRoute CAD
Mobile Field-Based Reporting	EIS Field Reporting
Message Switch (State and Local)	EnRoute CAD
LERMS	Executive Information Services
Fire RMS	ESO Firehouse (likely to be replaced in Q1 or Q2 2024)
EMS RMS	ESO EHR

3.3.2 Required Interfaces

The interfaces defined in Table 9 below are the interfaces required as part of this project. Please indicate if proposed solution can provide the following data transfer/export natively or requires an interface.

Table 9

Interface	Summary
Alphanumeric Paging	Text messaging
Alerting Interface	The system provides an interface with the Harris Symphony radio console to perform tone alert paging
AVL	System provides an Automatic Vehicle Location (AVL) system which displays unit locations to all mobile users and all dispatchers in real time.
CAD to CAD	CAD to CAD interface that supports the NENA EID call transfer
CAD to FRMS	CAD CFS export to LAFD FRMS vendor
CAD to LERMS	CAD and LERMS should share events, hazards, alerts, notifications, and global (master) files
E911	E911 phase I and phase II (ANI/ALI)
External Databases	System is able to export data to other records systems and/or CAD systems.
ESO ePCR (EMS)	CFS export
First Due	System provides the ability to interface via cloud-based API or web service API to First Due and similar applications
Forms	System provides the ability to interface with a Forms Tool that will allow agency to create custom forms the same as or similar to reports currently being used by the agency.
Guard1	Interface between Guard1 and proposed JMS
LInX interface	Data export to Northrop Grumman data sharing solution - RMS
Livescan	Export subject and charge information to fingerprint system
LEADS/NCIC interface	NM supports inquiries over interface.
NG911	CAD interface to Next Gen 911 data input
ProQA Paramount	Interface with Priority Dispatch Fire, Medical, and Police Modules,
Radio System	System provides an interface to Harris Symphony Radio Console solution
Rapid SOS	Rapid SOS has a default browser view but can also integrate with CAD or phone system
Smart911 or Agent 511	Receive information from Smart911 app to CAD
State Accident Import - TraCS	TraCS (Traffic and Criminal Software – TEG, Inc.)
State Ticket Import - TraCS	TraCS (Traffic and Criminal Software – TEG, Inc.)
Station Alerting	WestNet First-In

TDD / TYY	The system attaches the TDD / TTY dialog from the Customer's E9-1-1 answering positions to the CAD event.
VINE	Victim Information and Notification Everyday data export to Appriss
WatchGuard	Interface with Motorola Solutions WatchGuard Body Camera application

3.3.3 Other Interfaces

Other interfaces may be under consideration as part of this project. Please indicate if your proposed solution can provide the following data transfer/export natively or requires an interface:

Table 10

FUNCTION/FEATURE	DETAILS
Arrest to Booking	Send subject and charge information to ECC from MDCs or Law workstations.
ASAP to PSAP (incoming Alarm calls)	Alarms call information via NLETS per ASAP specification
BEAST	Evidence, property Management to RMS, MDS
Call Logging Recorder	Link to CAD CFS
CountyProtect.com	Ability to export incident/event information to a network location or URL
Emergency Notification System	Supports one-way interface from CAD to any Reverse 911 system (CodeRED)
Full Court	Case management link between RMS and Los Alamos Judiciary System.
Pictometry	CAD mapping system integrates seamlessly with current version of Pictometry

3.4 Project Management Services

The awarded contractor shall assign a Project Manager dedicated and available for the entire duration of the project. The County reserves the right to pre-approve the assigned Project Manager. Furthermore, should the awarded contractor need to replace its assigned Project Manager, the County has the right to pre-approve the new Project Manager. A Project Manager that is Project Management Institute (PMI) certified Project Management Professional (PMP) is preferred by the County and as such will have an impact on scoring of submitted proposals. Regardless of whether the assigned Project Manager is a credentialed PMP, the County requires that the project is run based on PMI principles outlined in the Project Management Body of Knowledge (PMBOK). The County project team (including its third-party consulting firm) will work with the awarded contractor's Project Manager to coordinate all project activities. All communications between the County, the offeror, and the third-party consulting firm shall be coordinated through their respective Project Managers.

At a minimum, the awarded contractor's Project Manager shall be responsible for:

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

1. Managing the project as the awarded contractor contact with responsibility for planning, organizing, managing, and controlling all aspects of the project.
2. Developing a project plan, managing the project plan throughout the project, and providing regular updates to that plan as the project proceeds.
3. Providing periodic updates to the project work plan and schedule (as outlined in section 5 of offeror proposal). Minor changes to the plan are subject to approval by the County's project manager. Major changes must be approved as a written change order to the contract.
4. Develop a project staffing plan that addresses awarded contractor and county resources, the level of participation, and when the staff need to be available. The County requires the awarded contractor to staff the project with personnel with relevant public sector experience.
5. Provide consultation and advice to the County on matters related to the project.
6. Submit status reports.
7. Help coordinate and participate in project meetings, including tracking risk items, issues, and providing meeting minutes.
8. Help prepare agendas for project status meetings.
9. Provide minutes for all project meetings to participating parties/stakeholders.
10. Identify personnel, equipment, facilities, and resources of the County that are required by the awarded contractor – at least two (2) weeks in advance of that need.
11. Work with the County's project management team to ensure that the project stays on-track and within budget.
12. Help verify that the project and that the system complies with the specifications and requirements.
13. Identify and provide immediate notice of all issues that may threaten the implementation, operation, or performance of the system.
14. Develop and maintain a risk management plan that includes risk assessment, project and organizational impact and mitigating actions.
15. Help manage and document any project scope changes to include:
 - a. Change request evaluation and documentation
 - b. Assessment of impact of any change to the project
 - c. Integration of the changes into the implementation

3.5 Planning

The awarded contractor shall work with the County's staff and will be responsible for planning and executing all phases of the system's life cycle. This includes, but is not limited to planning, analysis, design, data conversion, training, interface implementation, testing, system documentation, and system implementation (including cutover support for all applications), and post cutover support.

As part of planning, the awarded contractor shall provide a project work plan that includes the implementation strategy, change management plan, and the strategy for transitioning from existing legacy systems to the new public safety system(s) while considering interim interfaces and the impact on the County and constituent agencies' operations, as legacy systems are phased out. The initial draft of that plan is required to be delivered no later than 45 days after the initial project kick off (on-site kickoff meeting).

3.6 Performance Criteria

The following sub-sections outline performance expectations.

3.6.1 Prosecution of Work

After the work has been started, it shall be diligently prosecuted without stoppage until the entire contract is completed. In case the awarded contractor neglects or fails to diligently prosecute the work required under the contract, the County may terminate the contract and use any method deemed necessary to complete the project.

3.6.2 Performance Requirements

This specification section contains general and specific requirements related to the performance of the proposed system, both at the point of system acceptance and throughout the life of any warranty and maintenance contracts between the County and the awarded contractor.

System acceptance will occur in phases as various milestones identified in the implementation plan and agreed to by the County are reached. The awarded contractor must work closely with the County, their agents, and consultants to develop an implementation plan that clearly defines the hardware and software deliverables, tasks or other criteria associated with each milestone. The awarded contractor's phased implementation plan must specify how performance testing for each phase will be done.

3.6.3 Ongoing System Performance

The following specification describes the performance requirements for the successfully awarded contractor's system following formal acceptance of the System by the County and throughout the life of the contract between the County and the awarded contractor.

- a. For any consecutive 30-day period during the life of the contracts and/or warranties, the software components of the System must remain fully operational and available at 99.99 percent availability as calculated in [section 3.6.6](#). Thirty-day performance periods are incremental from system acceptance. If a problem occurs, a new 30-day period will begin once the problem has been corrected. The County will decide and notify the awarded contractor when issues have been satisfactorily resolved.

- b. The initial system hardware and software configuration must be scalable to handle the anticipated increase in work. This expansion must maintain the specified system performance requirements. The System must continue to meet the functional, reliability and performance requirements as expressed in this specification throughout the life of the System. In the event that the System fails to meet any requirement of this RFP after final acceptance and during the initial warranty period, the awarded contractor must take appropriate steps to cure the problem and bring the System back into compliance with the performance and reliability requirements, at no cost to the County. In the event the System fails to meet any requirement of this RFP during the maintenance period, the awarded contractor must take appropriate steps to cure the problem and bring the System back into compliance with the reliability requirements.
- c. The awarded contractor must describe the means and timeframe by which such failure will be resolved, and the County must agree in writing.

3.6.4 System Performance Profile

The following performance criteria are provided as a guide to the awarded contractor in designing the system and form the basis for acceptance testing of the implemented system.

- 1. The System must conform to the requirements specified in this RFP.
- 2. All inquiry and file maintenance functions must be performed without adversely affecting system performance.
- 3. Users must not be required to halt CAD or mobile operations during backups or other system administration tasks.
- 4. The proposed system design must provide for a minimum of 70 active MDCs during the peak busy hour.

The awarded contractor will not be responsible for the processing time of external systems (e.g., NLETS, NCIC, AFIS) when such systems are involved in a transaction. It is understood that outside factors may negatively affect such times and may need to be analyzed as part of the response time determination should an issue with these times occur.

3.6.5 System Response Times

The System response time must not exceed an average of the seconds defined below when operating with a workload up to the number of licensed users or devices.

3.6.5.1 Transaction Maximum Response Time for CAD and Mapping

The System must provide response times of less than one (1) second 95 percent of the time for the following transactions:

- a. Display of blank event entry screen
- b. Assigning a single unit to an event

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

- c. Changing a single unit's status
- d. Clearing a single unit from an event

The System must provide response times of less than two (2) seconds 99 percent of the time for the following transactions:

- a. Verification of a unique address
- b. Return of a list of possible addresses matches when an address cannot be uniquely verified with the information entered
- c. Display unit recommendation based on uniquely verified address

3.6.5.2 Transaction Maximum Response Time for CAD and Mobile Data System

The System must provide response times of less than five (5) seconds 99 percent of the time to complete the following transactions:

- a. Assignment of up to ten (10) units to an event from a single command
- b. MDC (Mobile Data Computer) to CAD or other MDC message (without attachment)
- c. CAD-MDC dispatch message
- d. Display of premises/hazard file data for a given location
- e. Generation and display of "new" report form from a mobile data/field-based reporting workstation or mobile device

The System must meet all the above performance requirements during normal daily activities to include report generation, analytics, and system backups.

3.6.6 Computer System Availability

The following specification defines both System availability and the method by which it is calculated, as it is used in other sections of this RFP.

The System will be considered available for use only when all the following conditions are met:

- a. All features, functions, and interfaces are installed and are operating correctly.
- b. System can process calls for service and dispatch resources.
- c. Mobile and mobility units with AVL display on map, automatically update their location, and can use that location for other application features.

System availability will be expressed as a percentage of the maximum expected availability over a given period. The System must be available 24-hours a day, 7-days a week (24/7). Scheduled down time (e.g., maintenance), as defined by the awarded contractor and accepted by the County, will not be considered as unavailable time.

The percentage availability for any period will be calculated as follows:

RFP No. 24-56
Issued by Procurement Division: [D. Rodgers](#)

(Total Hours in Period - Hours System Unavailable) ÷ Total Hours in Period

For example: In a 30-day period, maximum availability is 24 hours x 30 days = 720 hours. If the system is unavailable for 7.2 hours during that period, then the availability of the system during the period is (720-7.2) ÷ 720 which equals 99 percent.

3.7 Support and Maintenance Requirements

Subject to the terms and conditions set forth in the contract, the awarded contractor shall provide the following support for the covered applications (“Basic Support”). The awarded contractor shall maintain the Software and each component thereof so that such Software and components operate in conformity with the Documentation and with all specifications, performance standards and functional requirements in this Agreement. The awarded contractor shall promptly transmit, by the most expeditious means available, corrective material and related instructions for correcting malfunctions.

Software updates for all applications, enhancements, and refinements to purchased capabilities must be provided by the offeror as part of the price for maintenance for those years in which the County has purchased maintenance from the awarded contractor.

The selected contractor must warrant that all software supplied under the contract will be operational and available 99.99 percent of the time during the maintenance period or the maintenance period will be extended on a day-for-day basis for each day the System performance falls below this level.

There must be minimal system downtime for routine maintenance or system backups. The awarded contractor must provide a detailed explanation of any required (scheduled) system processes that may require downtime.

3.7.1 Application Errors

Upon notification, the awarded contractor will promptly correct malfunctions in any of the covered applications discovered by the County during the term of this Agreement, provided (a) the County provides all information regarding such malfunction that may be requested by the awarded contractor and (b) the County has provided the awarded contractor with remote access to the System as required by the contract.

3.7.2 Error Reporting

County personnel making such a report will describe to support service staff the malfunction in reasonable detail and the circumstances under which the malfunction occurred or is occurring and will, with the assistance of support service staff members, classify the malfunction as a severity level 1, 2, or 3. The County shall provide all information requested by the awarded contractor and reasonably available to the County, necessary to fulfil its request for technical

services. Upon detection of any malfunctions in any of the covered applications, the County shall provide the awarded contractor a listing of command input, resulting output and any other data, including databases and back-up systems, that the awarded contractor may reasonably request and is reasonably available in order to reproduce operating conditions similar to those present when the malfunction occurred.

3.8 Technical Support Center

The awarded contractor will provide toll-free telephone and email support for operational and technical assistance. Support for Severity 1 and Severity 2 calls relating to the awarded contractor's proposed solution shall be available twenty-four hours a day, seven days a week (24x7). Support for all other calls and any awarded contractor-provided third-party software will be available during normal support hours of 0900 to 1700 mountain time (not including weekends and awarded contractor-defined holidays).

3.8.1 Software Malfunction Severity Level Definitions

“Severity Level 1 Malfunction” – For CAD, Mobile, and Message Switch

A call requesting technical support for a malfunction in any Covered Application or a failure of the System server on which such Covered Application is installed that affects functions or results in system related failures, as follows:

1. The users are unable to enter new requests for service via the application UI.
2. The users are unable to change status or raise priority of a call.
3. The users are unable to close an incident.
4. The users are unable to view incident information needed to dispatch an incident.
5. The users are unable to clear assigned units from the call and/or close the call.
6. The users are unable to view premise history related to the location of the call.
7. The users are unable to update unit status or location related to a call.
8. The users are unable to change the call type or the priority of the call.
9. The users are unable to assign or exchange units or apparatus on the call.
10. The users are unable to log units on or off.
11. Major issues that prevent continued use or operation of the system endanger the integrity of any database or impacts 25% or more of the operators using the system.
12. The user's inability to view the current status of all units.
13. CAD side of any interface is down (but other side is active)
14. The user's inability to perform address verification because of an application problem.
15. The map cannot be displayed or cannot display any valid location.
16. Units do not display on map and/or unit location does not automatically update map.

“Severity Level 2 Malfunction”

Shall mean a problem which causes the Software to be inoperative, disrupted or malfunctioning and which materially interferes with the County's use of the Software.

“Severity Level 3 Malfunction”

Shall mean any problem in the Software which causes the Software not to function in accordance with applicable specifications, including the Documentation, but which causes only a minor impact on County's use of the Software and for which an acceptable “workaround” is available.

“Workaround”

Shall mean a temporary procedure, routine, solution or fix that restores operational capability without substantially compromising the performance of the Software or integrity of the operating system or data. A workaround will not require recurring system or workstation downtime. A workaround gives the County the ability to achieve substantially the same functionality as would be obtained without the programming error. Workarounds may include changes to configuration parameters or operational processes. To be acceptable, it must be an action, or series of actions, that can reasonably be accomplished by an average user without excessive impact to other capabilities and/or impeding work or process flow.

3.8.2 Response Time Credits

All Technical Service Requests (TSR) that the awarded contractor and the County classify as a Severity Level 1 must be resolved within 24 hours from the time the Severity Level 1 call is reported to the awarded contractor. If a TSR is not resolved within 24 hours, the County may reduce any subscription or maintenance costs for the time exceeding 24 hours to resolution on a prorated basis.

All Technical Service Requests (TSR) that the vendor and County classify as a Severity Level 1 must be resolved within 24 hours from the time the Severity Level 1 call is reported to the vendor, otherwise the County shall receive a one-thousand dollar (\$1,000) credit for each day thereafter until the vendor has notified and delivered to the County a fix or patch that restores required functionality to the system as set forth in the As-Built Specifications and any documented subsequent change orders. Upon notification by the County, the credits may resume if after the County tests the fix or patch and determines the fix or patch fails to restore the required functionality to the system as set forth in the As-Built Specifications and any documented subsequent change orders. If a reliable and suitable CAD Workaround, which does not impact CAD's intended Work or Process Flow, is delivered to the County in order to temporarily fix or patch a Severity 1 Malfunction, the Service Request shall be downgraded to a Severity Level 2. If the parties, in good faith, fail to agree that a CAD Workaround is reliable and suitable for purposes of downgrading the TSR, then the County shall have authority to decide whether the Severity Level 1 Malfunction Service Request may be downgraded to a Severity Level 2. Under no circumstances can a Severity Level 1 ever be downgraded to

anything other than a Severity Level 2 TSR. A fix shall mean restoring functionality in accordance with the As-Built Specifications and any documented change orders.

Severity Level 2 Service Requests: All TSRs that the vendor and the County classifies as a Severity Level 2 Malfunction must be resolved within forty (40) business days from the time the Severity Level 2 Call is reported to the vendor. Otherwise, the County shall receive a five-hundred-dollar (\$500) credit, followed by a one-hundred-dollar additional credit (\$100) for each day (24 hour) increment thereafter until the Severity Level 2 TSR is resolved and submitted to the client for testing. Once a fix is delivered to the Client no further credits for the corrected TSR will be assessed. All confirmed credits will be applied to the quarterly maintenance fee in the second quarter following the credit occurrence. In order to receive the Response Time Credits described above, the County must be in conformance with the most current version of the software that is in general release, and providing that all new releases are scheduled in advance with the County to minimize any operational impacts and the County is current with the support fee payment terms set forth in the contract. Such charges shall be itemized monthly and formally submitted to and approved by the County.

3.9 Legacy Data Conversion

As part of this procurement and the associated implementation, **the County will require a full, on-premise data conversion which will reside in the new system's active database and is accessible with no additional login/navigation. The data conversion will not require translation or transfer to alternate storage or application.** The data conversion includes, but may not be limited to, the following files/data components:

1. CAD
 - Calls For Service
 - Hazards and Alerts
2. LERMS
 - Incidents
 - Cases
 - Subjects
 - Arrests
 - Warrants
 - Orders of Protection
 - Evidence/Property
 - Tickets
 - Accidents
 - Master Name Index
 - Master Vehicle Index
 - Master Location Index

- Civil Process
 - Field Interviews (FIs)
 - Subpoenas
3. JMS
- Inmates
 - Bookings
 - Classification
 - Housing
 - Inmate Movement
 - Inmate Property
 - Inmate Disciplinary Incidents
 - Master Name Index

County has the need to convert existing records from the above-mentioned modules into the new system. County requires the selected offeror to perform review, analysis, data extraction, data mapping, and conversion. County expects the offeror to also perform the following actions as part of the conversion effort:

- a. Review with each participating agency what is required to collect, prepare, and translate their current data into the offeror's product(s).
- b. Develop conversion matrix for the files to be converted that provides a from to map of the data elements to be converted.
- c. Create a list of fields in each agency's current system that have no match in the offeror's system, with available options related to the translation of those fields (e.g., written to narrative, file attachment, etc.)
- d. Create list of required/mandatory fields within the offeror's system that have no corresponding field in their current systems from which to populate, and options available to populate those fields.

The proposal shall describe:

- a. The scope of data conversion services, approach, and cost to meet county's needs mentioned above.
- b. The roles and responsibilities between the Offeror and the County for conversion tasks, such as data extraction, data cleansing, data mapping, data verification and validation, etc.

3.10 Testing

The awarded contractor shall, as one of the early milestones, submit test plans for County's review and approval. These test plans must document how the functional specifications are to be validated. The plan must also include integration testing of all inter-related functional elements that are outside of the procured System, including other procured applications, and how that testing will be accomplished. A performance test plan must also be submitted for review and approval by the County, which includes the performance criteria specified in this section of this RFP. In these plans, the awarded contractor must include reasonable remedies for the County to exercise if failures are not corrected in a timely manner.

The test plans must include scenarios to demonstrate to County personnel that the System will operate as a fully integrated system (hardware/software/interfaces), under operational conditions.

The performance requirements specified in this RFP as part of the 30-day Reliability Test must be met before the System is accepted and final payment is made by the County to the awarded contractor.

3.10.1 Functional Acceptance Testing

The following specifications apply to the requirements for functional testing of the System at the completion of each phase (defined as CAD, MDS, LERMS, and JMS) of the overall implementation plan.

Beginning with the first day after the completion of each phase (phases will be specified in the implementation plan as defined above), the system phase is operational and available for testing. Acceptance testing will be conducted for up to 15 consecutive calendar days (the acceptance period).

During the testing period, the proposed Integrated Public Safety System will undergo a "use" test of the functions and applications defined in the Functional Specification Matrix for the given phase.

During functional acceptance testing (FAT), the awarded contractor will exercise the System to demonstrate that the selected functions have been delivered and are operational prior to going "live" on the System. The awarded contractor must demonstrate that each function included as part of the system deliverable, operates as defined in the contract, awarded contractor's proposal, the RFP, or the system documentation and/or users manuals (in that order of precedence).

3.10.2 Integration Testing

During integration testing, which will be completed for each phase of the project, the awarded contractor must demonstrate that each system interface operates in concert with the system to provide information and details required by the interface.

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

3.10.3 Thirty (30) Day Reliability Testing (Final Acceptance)

The reliability test will be conducted at the completion of all awarded contractor tasks associated with each phase to demonstrate the operational capability and reliability of that module or modules. In order to successfully complete this test, the awarded contractor must demonstrate in live operations that all software supplied under the contract will be operational and available 99.99 percent of the time during the warranty period or the warranty period will be extended on a day-for-day basis for each day the System performance falls below this level.

Offerors are advised the County may elect to review and modify the acceptance criteria for the reliability test during contract negotiations based upon specifics of Offerors' proposals. Once the awarded contractor has certified to the County the System is ready for live operational use, the System will undergo a 30-day reliability test. The purpose of this test is to demonstrate the System, as delivered, can perform under live operational conditions without the occurrence of critical priority software errors, as defined in this RFP. If the System experiences a critical priority software error during the first 15 days of the reliability test, a new 30-day period will begin once the problem has been corrected. If a critical priority software error is detected on or after day 16 of the initial 30-day test period, once corrected, the test will continue from day 16 and go for the remaining 14-day period.

Upon notification from the County of a critical priority software error, the awarded contractor must work continuously to resolve the problem. If the awarded contractor determines that a resolution or workaround cannot reasonably be provided within 24-hours of notification, the awarded contractor must, within the 24-hour period, provide the County with a resolution plan that includes status updates and estimated time of resolution. Upon successful completion of the reliability test for each given phase, the parties will jointly acknowledge system acceptance in writing.

3.11 Training

The awarded contractor shall provide the necessary training for system administrators, train-the-trainer staff, and staff end users. This training must ensure that the users will be capable of continued operation of the System and that the systems' support staff will be capable of maintaining the System and handling the diagnosis of software problems. The response to the RFP shall include related costs for training materials, e.g., Reference Guides, Tutorials and Related CDs/DVDs, etc.

The following on-site training is required:

- a. System Administrator Training
- b. Call Taker Training
- c. Dispatcher Training
- d. Supervisor Training

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

- e. Mobile Training
- f. Field Reporting Training
- g. LERMS Training
- h. JMS Training
- i. Interface Training

3.11.1 Training Guidelines

The general training approach desired is as follows:

- a. Targeted training for specialized functions, i.e., system administrators and technical support personnel for general systems administration and operations, and select staff for application operations, data entry and data maintenance.
- b. User training for all County ECC call takers / dispatchers. Minimum training time for call takers / dispatchers is 24 hours of classroom training.
- c. User training for core LERMS user staff.
- d. User training for core JMS user staff.
- e. Train-the-trainer staff as determined between the awarded contractor and the County.

The awarded contractor must provide classroom instruction for all call takers/dispatchers, supervisors; various support staff and management to ensure their complete understanding of the functional and operational use of the CAD system, mapping, LERMS, JMS, and other elements of the system(s) (including interfaces). At the completion of the training, staff must be capable of operating the System at a level of proficiency that will allow them to operate the proposed systems effectively.

Hourly or per course rates quoted must remain firm for one (1) year following the completion of all proposed training. Rates for subsequent years of refresher training must be included in Offerors response. County will consider, but is under no obligation to accept future year unit prices based on a specified dollar amount, a percentage, or some other formula (e.g., a specific Consumer Price Index.)

The County prefers training to be conducted on-site in their facilities. A copy of all training materials planned to be used by the awarded contractor must be delivered to the County PM fifteen (15) business days prior to the commencement of training. The training plan must identify any training requirements applicable after implementation and acceptance of the System. Awarded contractor must include an optional follow up training program that provisions 80 hours of training per year to be used as determined between the County and the awarded contractor, and the cost for such a program must be provided in the Proposal Pricing Forms.

With the implementation plan, awarded contractor must submit a schedule of all proposed training modules in Microsoft Project or other County-approved scheduling tool media with the following information:

1. Course summary/outline
2. Duration of training for each module
3. Audience
4. Class size maximum 10 to 30 students
5. Location of training
6. Student prerequisites

Training Simulator

The proposed System must include a training module that allows users to access all system applications, and associated databases, including the Geofile/mapping system.

Users logged on to the training module must utilize the same commands, forms and system features as users logged on to the live system. Data entered and commands invoked while logged in to the training module must not corrupt the live system or noticeably impede the performance of the live system.

3.12 Documentation

County requires the awarded contractor to provide documentation, bound or in binders, during the implementation for each functional sub-component that is provided by the awarded contractor as part of the System configuration. The awarded contractor must also provide documentation for all software applications (system administrator, system maintenance and user guides), interfaces, and training. The awarded contractor must provide at least three (3) hard copies and one (1) digital copy (i.e., e-mail, CD, DVD) of all documentation provided by equipment manufacturers and other suppliers providing equipment or software not procured by the County. The documentation must be contained in one (1) or more binders or otherwise bound to prevent their loss or destruction. The digital copy must be in a format that the County can reproduce for distribution to staff, trainees, and authorized stakeholder agencies.

Examples of Documentation include, but are not limited to:

- Operating System Software
- Server Manual(s) (if procured by the awarded contractor for the County)
- Mapping/GIS Software
- Application Software Reference
- Application Software Tutorial

- Hardware Operations
- Hardware Manual(s) (if procured by the awarded contractor for the County)
- User Manual(s)
- System Administrator(s) Manual(s)
- Functional System Description
- As-Built drawings for hardware and network engineering (if procured by the awarded contractor for the County)
- File (Database) Set up and Maintenance (File Maintenance Manual)
- Hardware and System Configuration (System Configuration Manual)
- Data Dictionary used in query-building or other reporting/data extraction functions

County requires the awarded contractor to provide documentation (paper and electronic) for any software the awarded contractor supplies as part of the System configuration.

The System documentation must be consistent with the instructions supplied by the on-line help systems for the application. The System must include no less than three (3) original copies of documentation describing the use of the system and its administration.

County has a strong preference for on-line support that is granular enough to provide help for specific items without having to scroll through a file to find a specific description.

The awarded contractor must provide a printed database schematic and data dictionaries to assist the County with the addition of site-specific fields and support for the System. The System must be fully documented prior to final acceptance of the System by the County. County shall maintain the right to make a sufficient number of copies of all documentation for its own internal use. Documentation must include:

- System Overview
- Hardware and System Software Documentation (if procured by the awarded contractor for the County)
- System Functional Specifications
- System Interface Specifications
- System Administrators Documentation
- End User Documentation (CAD, Mobile, FBS, LERMS, JMS) including abbreviated quick reference guides for each system.

3.13 Deployment Plan

The awarded contractor shall be responsible for deployment of the Public Safety solution in the County's environment. The Deployment Plan shall include a description of the awarded contractor's methodology including site preparation, roll-out strategy, legacy system transition, system phasing and other related system deployment requirements.

3.14 Pre and Post Cutover Support

The awarded contractor will be responsible for assisting County in such tasks as planning, preparation, pre-cutover issue resolution, conversion, post cutover issue resolution, communications, etc. during the weeks leading up to and weeks / months shortly after cutover. The awarded contractor should describe the resources, approach, and plans that will be used to assist the County during this critical time in the project.

Please note that the requested information regarding the awarded contractor's long-term Support and Maintenance plans are addressed elsewhere in this RFP. This section should focus specifically on the pre-cutover, conversion, and post cutover support offered by the awarded contractor.

3.15 Data Requirements at Contract Termination

The awarded contractor will be responsible for providing the County with a copy of all data stored within the System in a non-encrypted, readable format (CSV or similar readable/transferrable data format) upon termination of the contract and/or maintenance services agreement. The data must be provisioned within three (3) months of said termination.

4 Proposal Review and Evaluation (Guidelines and Schedule)

4.1 Process

After the RFP has closed, Procurement Division staff prepares a register of proposals containing the name of each Offeror, the number of modifications received, if any, and a description sufficient to identify the item offered. The register of proposals is open to public inspection only after the contract award. Procurement Division staff delivers the RFP submittals to the Evaluation Committee Chairperson. The Evaluation Committee reviews and evaluates the submittals. Interviews are only for the purpose of clarification and may be used for adjusting the final score. Discussions may be conducted with responsible offerors who submit proposals determined to be reasonably likely to be selected for award for the purpose of clarification to ensure full understanding and conformation with solicitation requirements for the purpose of obtaining best and final offers.

The total evaluation score with or without the cost factor of each proposal received from a qualifying offeror shall be multiplied by 1.05. After application of the factor, the contract shall be awarded to the highest score. If one or more scores are equal, the same procedure shall be followed with respect to the next category of offerors listed, and the next, until an offer qualifies for award. The priority of categories of offers is as follows:(1) Local business; (2) Resident business.

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

The Evaluation Committee Chairperson forwards the final evaluation results to the Procurement Division. Award shall be made to the responsible Offeror whose proposal is determined in writing by the Evaluation Committee to be the most advantageous to the County, taking into consideration the evaluation criteria set forth in the solicitation.

4.2 Evaluation Criteria

As described and/or demonstrated in the RFP response.

STEP 1 - RELATIVE WEIGHT OF EVALUATION FACTORS FOR PROPOSALS:

Table 11

ID	Criteria	Weighted Points
1.	Conformance to RFP	Pass/Fail
2.	Functional Specifications	30
3.	Customer Service and Support	10
4.	Company Background and Experience	10
5.	Project Workplan and Schedule	10
6.	Hardware and Infrastructure	25
7.	Cost	15
	Total Score	100

STEP 2 of the RFP - FOR “SHORT-LISTED” OFFERORS (See Part 2)

“Short listed” means those offerors whose offers have been determined by the evaluation committee to be qualified under the criteria set forth in the first solicitation (Step 1 of the RFP). The County’s Evaluation Committee will evaluate proposals according to the criteria described in Part 2 and set forth in Table 12 below.

Proposers are informed that the software demonstration element of Step 2 will be conducted before the evaluation committee. County may amend or alter the Step 2 evaluation criteria prior to the issuance of Step 2 RFP.

Table 12

ID	Criteria	Weighted Points
----	----------	-----------------

1.	On-site Demonstrations	60
2.	Vendor Rating by References	20
3.	Reference sites w/same or similar software	20
	Total Score	100

4.3 Evaluation Method

The following RFP scoring categories will be used:

Step 1

As described in Table 11

Step 2

As stated in Table 12, or as determined by County at time of issue of Step 2 of the RFP

4.3.1 Step 1 – Offeror Scoring

The County will score offeror proposals based on the criteria outlined above, including responses to the functional specifications, company background and experience, customer service and support, project work plan and schedule, pricing, and hardware and infrastructure profile. It will also include the requirement of proposing offerors to provide a qualifying web demonstration of the following items:

As part of that evaluation process, offerors submitting a proposal will be requested to give a short on-line demonstration of the following features and functions:

- a. Product Integration – show product integration by showing a call created in CAD, sent to MDS, completing a field-based reporting (FBR) summary including an arrest, sending arrest information to JMS for booking, booking, and housing the arrestee, completing the case in LERMS, and show how incident-based reporting (IBR) submission is created.
- b. Master Name File in all major applications – show the same subject Master name file (jacket) record in CAD, MDS/FBR, LERMS, and JMS.
- c. Discuss Conversion processes.

4.3.2 Step 2 – References, Demonstrations, Site Visits and other elements as may be determined by County at time of issue of Step 2 of the RFP

The County will further evaluate Step 2 offeror's solutions by utilizing demonstrations which may include scripted scenarios. Each short-listed offeror will be provided any scripted scenarios that they are to use to prepare for an on-site solution demonstration. The short-listed offerors will be further evaluated based on the results of reference checks, and, at the option of the County, organized site visits to offeror's customer sites. Offerors will provide County with a list of all of offeror's New Mexico clients and a list of five potential customer sites as defined in the reference section, [Exhibit B](#); and unless other arrangements are made, County may select any number of sites to visit or otherwise make contact with. County reserves the right to visit any offeror customer site that it finds beneficial or that can otherwise provide valuable offeror insight. Customer sites provided by the offeror should be using the same major version of the software being proposed to the County, similar in scope and complexity, and geographically like the County if possible.

Specific days and times for each short-listed offeror will be determined as part of Step 2 of the RFP; offerors should be prepared to conduct on-site demonstrations as an element of Step 2.

4.3.3 Final Recommendation for Award

Award shall be made to the responsible offeror whose proposal is determined in writing by the evaluating committee to be the most advantageous to the County, taking into consideration the evaluation factors set forth in the RFP. County reserves the right, at its sole discretion, to accept or reject any proposals; to waive any and all irregularities in any or all statements or proposals; to request additional information from any or all respondents; and to award a contract to the responsible Offeror whose proposal is most beneficial to County. While County intends to execute a contract for the services listed herein, nothing in this document shall be interpreted as binding County to enter into a contract with any Offeror or Proposer.

4.3.4 Discussions with finalist offeror(s)

Upon selection of a finalist(s), County may request the finalist(s) to conduct a solution confirmation workshop. This workshop is intended to confirm all requirements and representations in order to complete the best and final offer. This workshop may include additional demonstrations, confirmation of the Requirements worksheets, or any additional items that either party requires to be confirmed. The offeror may then be requested to submit their best and final offer.

4.4 Evaluation Criteria

4.4.1 Step 1

4.4.1.1 Conformance to RFP

Offerors must meet the requirements in the subsections below. (Pass/Fail basis).

a. Conforms with RFP Guidelines and Submittal Requirements

The offeror must follow all RFP guidelines and submittal requirements, including the completion of required forms and templates.

b. Offeror's Ability/Willingness to Accept the County's Terms and Conditions

The offeror's ability to accept the contract terms and conditions as outlined in the Services Agreement, a sample of which is attached as [Exhibit M](#), acknowledge responsibility for ensuring that the proposed solution is in line with the offeror's proposal and responses, and their willingness to incorporate their responses as part of the contract.

c. Certified Platinum Partner for Priority Dispatch's ProQA® Paramount

Offerors must be [Paramount-Platinum Certified](#) in interfacing with Priority Dispatch's ProQA® dispatch protocol software and include verification of the certification as part of the proposal submission package.

d. Proposal Completeness

Proposals must include all software and hardware being requested by the RFP. This includes required software and interfaces and required hardware. Should an offeror not supply all the required elements, the offeror will propose strategic partnerships with other offerors or contractors to provide a complete and tightly integrated public safety solution.

4.4.1.2 Product Functionality

The functionality being provided by the proposed system, based on the completed functional specification workbooks.

4.4.1.3 Customer Service and Product Support

Including, but not limited to, the offeror's acceptance of RFP warranty terms, guaranteed response time requirements, support hours and staffing, and the completeness and granularity of product help features.

4.4.1.4 Cost

The template provided must be used to outline the cost of the proposed solution. Failure to use the provided worksheet may characterize the proposal as non-responsive and preclude the offeror from further consideration in this procurement. Please provide the level of detail as defined in the pricing worksheet. Clarification may be sought for incomplete responses. If clarifications are not received by the specified due date, they will be considered non-responsive and precluded from evaluation. All items not defined in Scope must be shown separately as optional modules or tasks and priced separately. Offerors should submit pricing on their standard forms as supplemental information related to the pricing submitted on the required worksheet.

4.4.1.5 System Architecture and Infrastructure

Information related to the system hardware, software, and networking requirements should be included in this section. This information should be supplemented by a network diagram that shows the framework of the System as the offeror anticipates it will be configured. Information should also outline how the proposed System meets County technology standards, **integrates effectively with the current operating environment**, and will serve as a suitable replacement for the existing CMRJ system.

4.4.1.6 Project Work Plan and Schedule

Including the offeror's demonstrated understanding of the overall scope of work for this project, the proposed project approach and methodology, as well as the thoroughness and completeness of the implementation, integration, training, testing, and cut-over plans. This will also include the offeror's proposed ability to meet the anticipated schedule and scheduling requirements, and acceptance of requirements associated with staffing and resource substitutions projected by the County in this RFP.

4.4.1.7 Company Background and Experience

Including the offeror's financial and organizational stability, as well as the firm's experience performing work of a similar nature to that solicited in this RFP. This segment also includes the evaluation of the experience level and competence of the project team and organizational staff outlined in the proposal.

4.4.2 Stage 2 – (short-listed offerors only)

4.4.2.1 Demonstrations and Offeror References

Short-listed offerors will be invited to the County to provide demonstrations of the proposed solution. Project Manager attendance at demonstrations may be considered as part of scoring demonstrations. Reference scoring may include the quality and timeliness of work performed by the offeror for previous clients and the comparability of such work to the requirements of this

RFP. County will conduct reference calls and/or site visits to other organizations it deems as similar in size and composition or that can provide otherwise valuable insight to offeror performance and quality.

4.4.2.2 Site Visits (finalist offeror(s) only)

County may conduct site visits of relevant customer sites recommended by the offeror or based on direct contact with any client of a proposing offeror it deems may provide valuable insight to offeror performance and quality.

Proposals shall be handled so as to prevent disclosure of the identity of any Offeror or the contents of any proposal to competing Offerors during the process of negotiation.

4.5 Award Of Solicitation

Following award of the solicitation by County Council, the successful Offeror will be required to execute a contract with County in accordance with the terms and conditions set forth in the Services Agreement, a sample of which is attached as [Exhibit M](#). Offeror may identify any exception or other requirements to the terms and provisions in the Services Agreement, along with proposed alternative language addressing the exception; County may, but is not required to, negotiate changes in contract terms and provisions. The Services Agreement as finally agreed upon must be in form and content acceptable to the County.

4.6 Obligations Of Federal Contractors and Subcontractors; Equal Opportunity Clauses

Contractors and Subcontractor shall abide by the requirements of 41 CFR §§ 60-1.4, 60- 300.5 and 60-741. These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability.

Contractors and subcontractors agree to comply with all the provisions set forth in 29 CFR Part 471, Appendix A to Subpart A.

4.7 Illegal Acts

Incorporated County of Los Alamos Procurement Code, Article 9, imposes remedies and penalties for its violation. In addition, New Mexico criminal statutes impose felony penalties for illegal bribes, gratuities, and kickbacks.

4.8 Certification Form Regarding Debarment, Suspension, And Other Responsibility Matters

An Offeror shall complete the Certification Regarding Debarment, Suspension, and Other Responsibility Matters Form, attached as [Exhibit H](#) and submit with the proposal. This Form serves as a warrant of the offeror's responsibility and may not necessarily preclude the offeror from consideration for award.

4.9 Campaign Contribution Disclosure Form

A Campaign Contribution Disclosure Form is attached as [Exhibit I](#). The Offeror is requested to complete and submit with the proposal. If Form is not submitted with the proposal, upon award, Contractor must submit this form, in accordance with Chapter 81 of the laws of 2006 of the State of New Mexico.

4.10 Verification Of Authorized Offeror

A Verification of Authorized Offeror Form is attached as [Exhibit G](#). The Offeror is requested to complete and submit with the proposal. This Form provides County with the name and information of the authorized Officer who can obligate the selected firm in providing the services to Incorporated County of Los Alamos.

5 Proposal Format

5.1 Format

Offerors must include the following information in their proposal and must use the following format when compiling their responses. Sections should be tabbed and labeled; pages should be sequentially numbered at the bottom of the page. The following sections shall be followed to structure an RFP response. Responses should include each section detailed below in the order presented. The detail represents the items that are to be covered in each section of the response. Failure to address all items will impact the evaluation and may classify the proposal as non-responsive and preclude it from further consideration. Please refer to [Section 3](#) – Scope of Work for additional information.

Table 13

Section	Title
	Title Page
	Letter of Transmittal
	<ul style="list-style-type: none">Acknowledgements and Exceptions to RFP

	Table of Contents
1.0	Executive Summary
2.0	Company Background and Experience
3.0	Project Understanding
4.0	Project Staffing and Organization
5.0	Project Work Plan and Schedule
6.0	System and Technical Description
	<ul style="list-style-type: none"> • High Level System/Network Diagram
7.0	Software Maintenance, Updates, and Customer Support
8.0	Other Documents:
	Offeror's Standard Software License Agreement
	Offeror's Standard Support / Maintenance Agreement
	Professional Services Agreement
	Offeror Supplemental Agreements
9.0	Proposal Submission Forms
	<ul style="list-style-type: none"> • Verification of Authorized Offeror
	<ul style="list-style-type: none"> • Primary Covered Transaction Form
	<ul style="list-style-type: none"> • Campaign Contribution Disclosure Form
	<ul style="list-style-type: none"> • Confidential Information Disclosure Statement
10.0	Appendices:
	A. Completed Functional Specifications
	<ul style="list-style-type: none"> • Exceptions documentation
	B. References
	C. Resumes of Key Personnel
	D. Notification to Propose
	E. Addenda Acknowledgement
	F. Proposal Cost Sheet(s)

5.2 Title Page

The title page should include, at minimum, the following:

- Name of Project – Incorporated County of Los Alamos CMRJ – Integrated Public Safety System
- Submitted by - Company's Name
- Date of Submittal

5.3 Letter of Transmittal

The transmittal letter will:

- a. Indicate the intention of the offeror to adhere to the provisions described in the RFP without modification; offeror should include a signature line for contract compliance.
- b. Identify the submitting organization.
- c. Identify the person, by name and title, authorized to contractually obligate the organization.
- d. Identify the contact person(s) responsible for this response, specifying name, title, mailing address, phone, and email address.
- e. Explicitly indicate review and acceptance of the County's Terms and Conditions as listed in the Sample Services Agreement (see [Exhibit M](#)), and provide acknowledgement that the proposal submitted, including responses to the Functional Specification worksheets, will be included as part of the contract.
- f. Identify understanding and compliance with RFP requirements, define where the offeror complies with clarification, or otherwise takes exception to RFP requirements and/or content (excluding the functional specifications, which must be contained in [Exhibit A](#) as defined below).
- g. Acknowledge the proposal is considered firm for 180 days after the due date for receipt of proposals or receipt of the last Best and Final Offer submitted.
- h. Acknowledge completion of the pricing worksheets.
- i. Provide the original signature of the person authorized to contractually obligate the organization.
- j. Be signed by a company representative who is authorized to negotiate on behalf of the company.

5.4 Table of Contents

The table of contents should include the sections shown in the above table under the FORMAT heading.

5.5 Executive Summary

The offeror will provide an Executive Summary that presents a brief and concise summary description of the contents of the proposal response. The Executive Summary should be a maximum of one (1) to three (3) pages of single-spaced information providing a high-level description of the offeror's ability to meet the requirements of the RFP.

5.6 Company Background and Experience

This section of the proposal should establish the ability of the offeror to satisfactorily perform the required work by reasons of experience in performing work of a similar nature, demonstrated competence in the services to be performed, strength and stability of the firm, staffing capability, and record of meeting expectations on similar projects. the County, at its option, may require an offeror to provide additional support and/or clarify requested information.

The offeror should provide:

- a. A brief profile of the company.
- b. Any previous names used by any acquired, merged, or traded companies of the submitting organization.
- c. A brief description of the organization structure and primary products and services provided.
- d. Other major products or services offered.
- e. Company's strategic direction in software design and support.
- f. Company's commitment and track record serving public sector clients.
- g. Number of employees.
- h. Number and location of corporate offices.
- i. A general description of the company's financial condition.
- j. Provide three years of financial statements.
- k. Provide information regarding any pending litigation, contract defaults, planned office closures, impending mergers, bankruptcies, or other conditions related to the financial health of the company.
- l. Company's experience in performing work of a similar nature to that solicited in this RFP. Highlight participation in such work by the key personnel proposed for assignment to this project.

If the respondent will not be performing the requirements of this RFP as a single entity, the details of any proposed partnership, joint venture, etc. shall be described, including the organizational structure of the team.

5.7 Project Understanding

This part of the proposal shall contain a description of how the offeror intends to organize its approach to the project. The offeror will: (a) Discuss how its software solution meets County's requirement for an integrated system, as requested in this RFP; (b) Relate how it perceives its role in carrying out the responsibilities required by this implementation; (c) Provide examples of challenges encountered on similar engagements; and (d) Discuss its approach in handling some of the specific challenges and opportunities it foresees for this project.

5.8 Project Staffing and Organization

This section shall identify key personnel who will be assigned to the project, assuming a September 1, 2024, start date. An organization chart for the project shall be provided. The chart shall indicate how the offeror intends to structure the project effort, and identify the Project Director/Engagement Manager, Project Manager, Technical Team Members, Trainers, and all other key personnel.

Offeror implementation staff must be fully trained and certified by the manufacturer(s) of the system(s) proposed; training must be current. In addition, all key implementation staff must be experienced in similar installations. Resumes must be provided for all implementation staff.

Additional requirements include maintaining the involvement of offeror personnel essential to the project, timely replacing of any staff deemed unqualified by the County and directing staff to comply with any of the County-specified rules and regulations.

The Project Manager designated by the awarded contractor shall have the overall responsibility to the County or its representative. The Project Manager shall have the responsibility for the day-to-day communications with the County, to coordinate the activities of the installation and implementation team, and to accomplish the scope of work within the contract budget and project schedule. The Project Manager must have at least three (3) years of experience in administering project management services of the proposed software for a Public Safety institution. A resume of the Project Manager must be provided detailing the work history for the last five (5) years.

Each team member included in the project organization chart shall be identified by name, and a resume or profile shall be provided for each key person. Each resume or profile shall be complete and concise, featuring experience that is most relevant to the task responsibility the individual will be assigned. If an individual is assigned to more than one position, relevant experience shall be indicated for each task assigned. Each proposed team member must have a minimum of two (2) years of experience with the installation of the current (or one previous) version of the proposed software for Public Safety.

For all proposed project team members, please also indicate other projects these individuals will most likely be engaged in at the time this project commences, as well as anticipated completion dates for those other projects, and how that may impact the amount of time the individuals will be spending on the County's implementation. Please also indicate the anticipated percentage of time each team member will be dedicated to the implementation throughout the course of the project.

The specific staff identified in the proposal may not be changed prior to commencement of work or during the project without the specific approval of the County and a two-week notice. Replacement candidates must have the same or higher level of similar experience as the original project team member they replace. Resumes of replacements shall be submitted with all applicable information.

5.9 Project Work Plan and Schedule

In this section, the offeror is requested to provide details of its methodology, implementation strategy and schedule for the performance of the tasks identified in [Section 3](#), Scope of Work, of this RFP. The work plan shall provide a narrative description of the plan for implementing the work tasks as well as any substantive or procedural innovations used by the offeror on similar projects that are applicable to the services described in this RFP. The work plan should address the number of resources expected from the County to successfully carry out all the implementation activities.

The work plan and schedule shall address the components identified in a detailed implementation schedule, assuming a September 1, 2023, project start date, which should include:

- a. Project Management Services
- b. Planning
- c. Implementation
- d. System Integration Plan
- e. Data Conversion Plan
- f. Data / System Interface Plan
- g. Functional Test Plan
- h. Training Plan
- i. Documentation
- j. System Deployment
- k. Pre and Post Cutover Support

The work plan and schedule should be of enough detail to provide the County with the necessary task, resource, and sequence information to allow for logistics and staff allocation planning. The

offeror's Work Plan must state any facilities, data, and other requirements that the County will be expected to provide.

County understands that each offeror will have their own implementation methodology derived from their industry experience and software requirements. It is the desire of the County to have consistency of detail within the work plan and schedule across respondents to allow for an objective determination by staff as to the quality and feasibility of each respondent's submission.

The work plan should be created in Microsoft Word and the schedule must be created in Gantt chart format using Microsoft Project or other similar program that produces Gantt formatted output. At a minimum, this chart must show phases, tasks, sub-tasks, and staff utilization. County may request task expansion or contraction, additional task details, and/or scheduling modifications within the work plan or schedule prior to award of the contract. County may require offeror to perform Project Management activities on a web-based Project Management tool or portal to enhance review and collaboration.

The work plan must specify the recommended time period for each phase. The work plan must include the proposed responsibilities of the Project Manager. The work plan must describe the offeror's program control methods for demonstrating offeror's performance, adherence to and control of the project schedule and budget.

The work plan must describe the offeror's commitment of resources for technical and functional-area team members. This team should consist of the experts in the various modules of the proposed software for the County. The work plan and schedule must display the amount and timing of the proposed effort within the project milestones. The work plan must list any specialized system personnel that would be required in the County to maintain and operate the proposed system.

The work plan must include time and activities set aside to revise the County's existing practices to best utilize the proposed software's functionality. The County recognizes that improvements in structure and processes can be as beneficial as improvements in technology. Accordingly, the offeror's experience with similar organizations and "Industry Best Practices" is important to the County and should be reflected in the work plan and schedule.

The project work plan and schedule must include the time and resource commitment for testing and accepting the system components and configuration within the County's simulated production environment.

The work plan must include the offeror's recommended training plan for end users of the selected software and for IT staff responsible for ongoing system maintenance and support. The work plan must also include detailed listings of training programs for technical staff, configuration staff/core users, senior management, and information/end users. Additionally, the work plan must state the method of training (instructor-led hands-on classroom training, train-the-trainer,

offsite public classroom training, web-based training, etc.), the number of training hours to be provided, the recommended number of participants in each training program, and the infrastructure and systems required. The work plan schedule must show the type of training provided and the hours of commitment for each implementation phase.

The work plan and schedule must include the offeror's recommended deployment plan for converting from the testing environment to the "live mode" of operation. This effort must describe the final steps of the process and the resources required to successfully complete this task. The procedure must include offeror's site preparation, roll-out, migration, turnover to production and organizational transition strategies. It must also include contingency plans for falling back to the old system should there be an unexpected problem with the new system.

The work plan must include a description of the offeror's post-implementation technical support programs. This must include the types of programs available, the hours and days of operation and information on response time for urgent and non-urgent assistance requests. Full details of the Service Level Agreements offered should be provided, including penalties for non-compliance.

Although the County is requesting a work plan as part of the RFP response, it recognizes that the offerors may need to refine the work plan to use it as a management tool during implementation. The County expects the selected offeror to develop a detailed work plan as part of their Scope of Work and to be submitted no later than 45 days after execution of the contract.

5.10 System Hardware and Infrastructure Description

5.10.1 Hardware Requirements

The Technical Standards for Incorporated County of Los Alamos are located in [Exhibit L](#) for review and reference. Offeror should include responses to the County's technical questions outlined in [Exhibit K](#) in response to the section of the proposal.

Offerors shall propose a hardware configuration with adequate storage capacity to accommodate data converted from the County's previous systems from 2005 up through "go live" with the awarded vendor's system. It is also expected to have a capacity for the system for the projected 15-year anticipated contract duration. Specifically, a minimum of 15 years of incident data for CAD, 15 years of associated reporting data for the LERMS and Mobile/Field Reporting modules, and 15 years of inmate and jail management data for the JMS modules. The system shall be configured such that the system can operate with the defined anticipated maximum concurrent user count without any system degradation.

The County reserves the right to purchase the hardware proposed by offerors independent of the successful offeror's proposal. Regardless of the method determined by the County to purchase

the hardware proposed, offerors must certify that the hardware proposed meets or exceeds the requirements stipulated above related to system performance and storage capacity.

Offerors shall describe in detail what hardware/software components are included in the cost of its proposal.

Offerors providing a solution where there are multiple platform options must provide information on each.

Offerors must provide an overall design using a system diagram and an overview explanation (no more than four (4) pages) describing the proposed hardware. The installed system must be scalable and capable of expansion in a modular and incremental fashion. CAD workstations are included as part of this project. Offerors must specify minimum and/or optimal requirements for all call taker/dispatcher positions, including what is required to allow multiple monitors from the same workstation.

The system architecture must provide a high availability solution. The system shall be designed to provide automatic fail-over, and other technologies that enable continued operation, to provide the ability to withstand single or multiple component failure.

The selected system shall be sized appropriately to meet performance criteria, accommodate any future workload increases and store enough data history.

The offeror shall provide the recommended hardware with capacity requirements for the proposed system solution. In addition, the offeror shall itemize all required and recommended system software to make the proposed system software operate in the most efficient manner.

Offerors shall provide proposed hardware and system software configuration(s) as part of Proposal Outline.

5.10.2 General Requirements

Offeror must provide all services and supplies necessary to install, operate and maintain the software and equipment specified in the RFP and functional specifications. County's preference for this project is to leverage hardware already in use or defined to be included in this project. Therefore, it is required offeror's provide detailed information for all hardware and software requirements. County may elect to increase or decrease quantities or acquire the hardware separately based upon the successful offeror's provided specifications. Regardless of method of procurement, the successful offeror must be responsible for the hardware configuration proposed. These solutions must support all defined software requirements outlined in [Exhibit A](#) – Functional Specification workbooks.

5.10.3 Mission Critical Server Hardware Requirements

All server hardware proposed must meet a system uptime requirement of 99.99 percent. Integration and use of VMware and virtual front-end platform design is a preference. All application systems must operate concurrently. If several applications utilize the same data server, the System must be configured to assure priority workstation response for the CAD system.

County anticipates purchasing any required and/or specified operating system and third-party applications the selected contractor requires for the proposed system. Any operating system and third-party licenses not acquired by the selected contractor must be in the name of and property of the County. The selected contractor must provide all licenses (software, support, etc.) purchased in the name of the County prior to payment for the software.

All servers proposed must be configured to support the application software requirements, volumes, and processing performance characteristics defined. The equipment proposed must be configured with enough direct access storage to support timely file query and update for all applications, and retention of data, including conversion, if required.

The equipment must be configured with sufficient main memory, disk capacity, and processing capability to facilitate installation of the application programs and peripheral devices for processing information related to the successful offeror-defined systems and must possess sufficient expansion capacity to support future requirements (a minimum 15 years of projected future growth).

5.11 Software Maintenance, Updates, and Customer Support

5.11.1 Warranty Provisions

The following requirements are applicable to all maintenance and repair services supplied by the offeror or respective subcontractors, both under and outside of warranty.

The offeror must warrant that all hardware and software supplied by the offeror and the integration thereof will be free from defects in material, design, and workmanship for the warranty and maintenance period purchased.

The offeror must provide a minimum one-year warranty period from the date of final system acceptance. The offeror must warrant that all hardware and software supplied will be free from defects in material, design, and workmanship for the warranty period and any extended warranty or maintenance period purchased. This warranty shall cover all parts, labor, and travel related to all the hardware and software supplied under the contract.

The offeror must provide a detailed description of the warranty offered and any available extended warranty. This description must include a description of hardware and software support services and system upgrades to be provided. During the warranty period, the offeror must provide support services 24 hours a day, 7-days a week (24/7) for critical software systems. This service must be available any hour of the day via a toll-free dial-up number. The offeror or its subcontractors must have the ability to access the System remotely for troubleshooting and to perform system diagnostics. Any hardware warranty must include 24-hours a day, 7-days a week (24/7) service to be provided by the hardware offeror. Coordination of warranty and service activities will be the responsibility of the primary offeror.

For all critical system problems, major system failures, or for severity level 1 software errors reported, the offeror must provide an immediate response to the incident and must initiate corrective action no longer than 60 minutes from time of notification. Within two (2) hours of any critical system problem, major system failure or critical priority software error, offeror personnel must be either on-site or logged into the System to analyze the cause of the problem and to effect corrective action. Equipment or components required on-site for emergency maintenance must be specified and provided.

In all instances of a critical system problem, major system failure or critical priority software error, whether hardware or software related, the offeror, and/or the provided hardware/network support partner, must affect corrective action within four (4) hours of problem reporting or escalate the problem to their senior support staff for their immediate resolution at no added cost to the County.

The offeror must provide documentation of repair escalation policies and procedures to be followed if either a hardware or software problem is not responded to or resolved within the timeframes referenced above. The offeror must provide the names and contact information for managers and senior level managers listed in the escalation procedure.

The offeror must warrant that all hardware and software supplied under the Public Safety Technology contract will be operational and available 99.99 percent of the time during the warranty period or the warranty period will be extended on a day-for-day basis for each day the System performance falls below this level. The offeror must provide a detailed statement of warranty exclusions. The County reserves the right to reject any proposal based upon stated exclusion of warranties.

The County reserves the right to accept or reject any and all proposed services, offerors, or providers, and/or the use of any proposed service facilities, at the sole discretion of the County.

The warranty requirements for the software and hardware are critical components of this project and must be specified by proposing offerors. Should offeror wish to provide warranty which exceeds the stated provision, such warranty may be proposed.

5.11.2 General Maintenance Provisions

The following requirements are applicable to all maintenance and repair services supplied by the offeror or respective subcontractors, both under and outside of warranty.

The offeror must provide a 15-year system maintenance plan to commence at the expiration of the warranty or, if purchased, after the extended warranty period. This maintenance plan must cover all labor and travel related to all the software supplied under the contract to the County if the terms of the Maintenance Agreement are not met.

The offeror must provide a detailed description of the offered maintenance plan. This description must include a description of software support services and software upgrades to be provided. The equipment or components required on-site for emergency maintenance must be specified.

During the maintenance plan period, the offeror must provide support services 24-hours a day, 7-days a week (24/7) for critical systems. Critical systems are defined as CAD and associated interfaces. This service must be available any hour of the day via a toll-free dial-up number. The offeror must have the ability to remotely access the system via an online access methodology to troubleshoot and perform system diagnostics.

For all critical system problems reported, the offeror must provide an immediate response, and must initiate corrective action no longer than 30 minutes from time of notification. Within two (2) hours of any major failure reported, if the problem has not been corrected, offeror personnel must be on-site or logged into the system to analyze the cause of the problem and to take corrective action.

In all instances of a major system failure, the offeror must take corrective action within four (4) hours of problem reporting or escalate the problem to the next higher tier of support for immediate resolution at no added cost to the County.

Critical system or major failures are defined by the County in [section 3.8.1](#) of this RFP, and include (but are not limited to) the following:

- a. The inability of call takers/dispatchers to take calls, monitor units, change status, or dispatch emergency responders to any reported event.
- b. The inability of the CAD system to recommend or select the correct units for dispatch.
- c. The inability to validate call locations during call entry (mapping or address validation error(s)).

The cost of the maintenance plan must be itemized on the cost sheets. The County may purchase one (1) or more additional years of support and maintenance, and other specified ongoing services, on a year-by-year basis, or purchase a multi-year support agreement.

The County reserves the right to accept or reject any and all proposed services, offerors or providers, and/or the use of any proposed service facilities, at the sole discretion of the County.

5.11.3 System Warranty and Ongoing Maintenance Support

The first year of maintenance will be deemed “System Warranty” and shall be provided at no charge to the County. System Warranty will begin upon completion of the 30-day reliability test period of live operations for the CAD system.

The offeror shall provide a fixed cost for maintenance fees for years two (2) through five (5). Offerors must provide costs for forward years, up to a total of fifteen (15) years, County will consider, but is under no obligation to accept future year unit prices based on a specified dollar amount, a percentage, or some other formula (e.g., a specific Consumer Price Index.) The ability to provide costs for maintenance up to fifteen (15) years will be a scored evaluation criteria.

Any selected offeror must maintain compliance with all State and Federal mandates, updates, and modifications related to the system as part of the support they provide.

5.11.4 Help Desk Support

The offeror shall provide 24/7/365 system support (help desk operations) for CAD and Mobile, with dedicated staffing during normal business hours and must be available for emergencies, off hours and at all times.

5.11.5 File Back-Up/File Recovery

The offeror shall provide processes that assure, to a reasonable degree, that upon system failure, disk failure, or other system component failure, that system databases are restored to their pre-failure status and that data integrity is maintained. Recovery from failure must be provided such that operation may be continued immediately following replacement of the failing component.

5.11.6 Additional Support Information Requirements

The offeror is also requested to provide details of its software maintenance and update methodology, including how software updates are distributed, frequency of updates and recommended approaches for the County to test and install software updates prior to rolling them into production. This information must include how updates to mobile data computers (MDCs) are distributed and installed.

The offeror should provide information regarding the types of offeror and County skill sets required to implement incremental and major updates to the County’s production environment as well as how the offeror recommends ensuring that custom configuration and custom code (should there be any) is addressed during the upgrade to ensure that none of the County-specific changes are lost.

The offeror should also describe the Quality Assurance measures in place to ensure the code is thoroughly tested prior to releasing it to the County.

The offeror should discuss if there is a forum where users can report and address software issues. Additionally, the offeror should discuss how much influence customers have in product direction, including technology used, enhancements, and new features, including the process used to provide input, feedback, and software roadmap reviews.

The offeror should disclose if national and regional user groups exist for users to meet and discuss the different ways in which the software can be implemented.

Offerors should also provide details on their Technical Support and Help Desk infrastructure, staffing levels, organizational structure, and abilities, including hours of operation, issue management and tracking tools, service level agreements, and a general description on how the County would interact with Technical Support and Help Desk staff.

5.12 Other Documents

Under this section, offerors shall provide the following:

- a. Standard Software Licensing Agreement
- b. Standard Support/Maintenance Agreement
- c. Professional Services Agreements
- d. Offeror Supplemental Documents

Additionally, offerors shall carefully examine the RFP for required documentation not specifically covered in sections 5.1 through 5.11 and shall also place such documentation in this section. Information considered by the offeror to be pertinent to this project, but not specifically requested in this RFP, may also be placed in the offeror supplemental documents subsection. The offeror is reminded that this is not an invitation to submit voluminous amounts of extraneous material. Examples of documents to be included in this section include:

- a. Sample Training Manuals
- b. Sample Standard Reports
- c. Sample Implementation Plan

5.13 Appendices

Offerors shall complete and submit Exhibits A, B, C, D, E, F, G, and H as appendices to the proposal.

All proposals should have the following appendices (labeled as defined below):

- a. Appendix A – Functional Specifications
- b. Appendix B – References
- c. Appendix C – Resume Form
- d. Appendix D – Notification to Propose
- e. Appendix E – Addenda Acknowledgement
- f. Appendix F – Proposal Cost Summary and Proposal Cost Sheets
- g. Appendix G – Appendix G - Verification of Authorized Offeror
- h. Appendix H - Primary Covered Transactions Certification Form
- i. Appendix I - Campaign Contribution Disclosure Form
- j. Appendix J - Confidential Information Disclosure Statement
- k. Appendix K - Answers to Incorporated County of Los Alamos Technical Questions
- l. Appendix L – Verification of Acceptance of Incorporated County of Los Alamos Technical Standards (or included exceptions)
- m. Appendix M – Acceptance, notes and/or exceptions to Los Alamos Sample Services Agreement
- n. Appendix N - LiNX Interface Questionnaire responses
- o. Appendix O – CJIS Security Addendum
- p. Appendix P – Sample Reports response
- q. Appendix Q – Addenda Questions from RFP 23-62
- r. Appendix R – E-Signature Policy
- s. Appendix S – Records And Information Management Governance Policy
- t. Appendix T - IT Usage and Security Policy
- u. Copies of all applicable licenses, certificates and permits Offeror possesses to carry out the Services required in the State of New Mexico

Appendix D should be submitted by February 21, 2024, in order to register as a potential offeror for this procurement.

Instructions for Appendices A - F are defined below.

5.13.1 Functional Specification Workbooks (Appendix A)

The County has prepared functional requirement worksheets to be completed by the offeror. These worksheets will form part of the basis for scoring the offeror’s overall response. The worksheets are meant to determine how much of the required functionality each offeror’s product can provide. The requirements are weighted and will be scored based on the offeror’s response.

The entire set of requirement worksheets are subject to verification at any time during the procurement and contracting process. If such verification determines that an offeror misrepresented product functionality, they may be disqualified. Also, all functionality responded

to as “available” and that is part of the software package procured by the County will be verified during functional acceptance testing. It is therefore very important that offerors complete the worksheets accurately as it will affect their opportunity to be considered further in this procurement. The awarded contractor will be expected to provide all the functionality it has specified as “available” and that is procured as outlined in any final contract.

Offerors must include a completed electronic copy of the Functional Specifications (Excel Workbooks), with the proposal document package. The functional specifications included in this RFP have the following properties associated with them:

Specifications may appear to be conflicting, where a requirement may request a specific function be provided in one way and be followed by a requirement that requests that same function be provisioned for in a different (or potentially conflicting) fashion. Example:

- LMNI-2 = All master name activity for a subject for all jurisdictions can be accessed via one record.
- LMNI-3 = Master name records for the same subject are separated by jurisdiction.

The intent of specifications like those above is to provide a better understanding of each offeror’s method of provisioning the given functional feature.

The specifications are labeled with the following importance categories:

- N/A (items marked N/A are not applicable to this project, are locked from access)
- Minimal
- Important
- Crucial

Table 14 below outlines the definitions of the availability categories used in the Functional Specification Workbooks.

Table 14

INSTRUCTIONS	RATING LEGEND
Complete the worksheet by opening the drop-down box and selecting the appropriate descriptor for each criterion. The response must represent the current state of the specific requirement.	Functional available – Feature/Function is available and operational in the current release of offeror’s product and is in use in a live client environment.
	Function not available – Feature/Function is currently not available in a live operational client environment. This would include functions and features that may be on an offeror’s development roadmap.

	Exception – Could meet the requirement with modification or is provisioned in a different manner than specified.
--	--

The higher the category of importance, the greater weight in scoring those specifications will carry.

The functional specifications outlined in the SYSTEM and COMMON tabs (included as part of the CAD MAIN Functional Specification Spreadsheet) represent system requirements, and common functional requirements that apply to all packages and modules being proposed.

Each Functional Specification Spreadsheet has an “unlocked” column entitled “Review Comments” that can be used internally by offerors to assist them in scoring and tracking input on each specification. However, all content must be deleted from those fields in the version submitted by each offeror as the final specifications. Should any information be left in those fields, it will have no bearing on the score, the interpretation of the offeror response, or otherwise carry any weight or consideration.

5.14.1.1 Explanations of Exceptions

Following the completed functional specification workbooks should be a document that clarifies any exceptions taken to specific functional requirements. Each exception must be documented to include the specification number (e.g., SYS-4), the specification description (e.g., “The system automatically and correctly adjusts for Daylight Savings Time”), and the details associated with the exception. The response must contain an explanation of any "exceptions" taken to functions that appear in the Functional Specification Workbooks. Any "clarifications" provided for any numbered requirement that has been asserted to be an available function in the Functional Specification Workbooks will generally negate a "Function Available" statement; this will cause an offeror to be judged non-compliant for the specific requirement. For the purposes of this RFP, items not answered or marked as an exception on the Functional Specification Workbooks will be interpreted as Function Not Available and will be factored accordingly for scoring purposes. Once a short list of qualified offerors is determined, based on initial RFP review and scoring, consideration may be given to exceptions to allow for a more complete analysis and offeror comparison.

5.13.2 References (Appendix B)

Offeror references must be submitted in two (2) forms. The first form should be an offeror client list for the State of New Mexico. The County reserves the right to contact any client on that list that it feels may provide valuable offeror insight.

Second, offerors must provide at least five (5) client references. At least two (2) references must be from cities/counties where a Public Safety System was implemented that closely reflect the scope of work for the County as described in this RFP. These references shall be sites at which the software has been fully implemented (“live”) within the past three (3) years.

The County prefers references for previous implementations of the same base version that will be proposed for the County. Please use the Client Reference form provided as Appendix B in this RFP or downloaded from the BidNet site. For each reference listed, offeror must disclose if it has offered or provided any benefits, products, discounts, or other in-kind services/products to the reference in exchange for fulfilling the role of providing a customer reference.

5.13.3 Resume of Key Personnel (Appendix C)

Under this section, provide a brief resume of key persons, specialists, and individual consultants assigned to the project that includes the information as outlined in RFP and [Exhibit C](#).

5.13.4 Notification to Propose (Appendix D)

Use the form provided in [Exhibit D](#) to register as a potential Offeror for this procurement. Only registered offerors will be mailed courtesy notices of changes or addenda to these procurement documents. Failure to complete and return this form may result in the rejection of your Proposal.

5.13.5 Addenda Acknowledgement (Appendix E)

Each Offeror shall acknowledge receipt of Addenda, using the form provided in [Exhibit E](#), in relation to the “CMRJ - Integrated Public Safety System” RFP No. 24-56 by their signature on this form. If the County does not issue any addenda, Offerors do not need to submit this form.

5.13.6 Cost (Appendix F)

Pricing is an important aspect of the overall evaluation of the offeror’s response. Included in [Exhibit F](#) of this RFP is the pricing template ([PROPOSAL COST SHEETS](#)) that must be used to provide the cost of the proposed solution. Failure to use the provided pricing template may characterize the response as non-responsive and preclude the offeror from further consideration in this procurement. Please price the solution as accurately as possible as it may become the basis for the solution price. Please provide the level of detail as defined in the pricing template. Clarification may be requested for incomplete responses.

5.13.6.1 Proposal Cost Summary Form

The offeror shall summarize the key cost categories on the provided Cost Summary Form. This should be based on the pricing included in the Proposal Cost Sheets.

5.13.6.2 Proposal Cost Sheets

The offeror shall use the worksheet provided in [Exhibit F](#) for all software and maintenance related costs. Price should reflect the County's desire to maintain production, test, and training environments.

The software license and costs must allow the County to utilize the software via direct and remote access by the required number of users and departments of the County affiliates and any other person or entity which the County needs to allow access in order to provide the services required of the system.

Additionally, the offeror should use their own format to include a brief description of the software pricing methodology (license cost per seat, per named user, per module, per server, per site/organization, etc.).

The offeror shall also include a brief description of the strategy for maintenance agreement pricing after the initial term of the maintenance agreement has ended or after additional software has been licensed.

The specific categories of software cost are provided in the pages of the Proposal Cost Sheets:

- a. Required software (CAD, LERMS, Mobile, FBR, and JMS) and services
- b. Required interfaces software and services
- c. Optional software, modules, interfaces, and services
- d. Hardware for required software, interfaces, and required peripherals
- e. Conversion support
- f. System maintenance cost – required software and interfaces
- g. Hardware maintenance cost (if applicable) – required hardware

The offeror shall include all costs associated with the implementation of the software solution and provide a “not-to-exceed” amount to perform implementation, integration, roll-out, and other work identified in this RFP.

Service Costs cover all the types of labor for each functional area that will be directly charged to the contract. The hourly rate associated with Conversion Assessment shall represent the offeror's fully loaded rate, including overhead and profit.

Travel shall be based on the number of trips, the number of people traveling, the estimated cost of the transportation, the meal and lodging cost of each traveler, and other miscellaneous travel expenses. Actual travel expenses shall not exceed reasonable amounts as determined by the County based on the contract.

In addition to using the Proposal Cost Sheets to provide the specific information requested, the offeror is expected to use their own document format to discuss any additional information or

supporting schedules that would clarify any ambiguities and assist the County in obtaining a better understanding of the offeror's cost philosophy. Please note that the Proposal Cost Sheets must be completed and must not be altered by the offeror.

5.13.7 Proposal Forms

All offerors must complete and submit the following forms with their proposal package; failure to include these completed forms with the proposal package may result in offeror disqualification. These documents should be submitted in the proposal as Appendices as noted:

1. Appendix G - Verification of Authorized Offeror, use [Exhibit G](#)
2. Appendix H - Primary Covered Transactions Certification Form use [Exhibit H](#)
3. Appendix I - Campaign Contribution Disclosure Form, use [Exhibit I](#)
4. Appendix J - Confidential Information Disclosure Statement, use [Exhibit J](#)
5. Appendix K - Answers to Incorporated County of Los Alamos Technical Questions, use [Exhibit K](#) - – Must Acknowledge with any Exceptions
6. Appendix L – Verification of Acceptance of Incorporated County of Los Alamos Technical Standards (or included exceptions), use [Exhibit L](#) – Must Acknowledge with any Exceptions
7. Appendix M – Acceptance, notes and/or exceptions to Los Alamos Sample Services Agreement, reference/use [Exhibit M](#)
8. Appendix N - LiNX Interface Questionnaire responses, use [Exhibit N](#)
9. Appendix O – Acknowledgement of compliance with CJIS Security Addendum and signature of offeror representative, use [Exhibit O](#)
10. Appendix P – Sample Reports response, reference/use [Exhibit P](#)
11. Appendix Q – Addenda Questions from RFP 23-62 [Exhibit Q](#)
12. Appendix R – E-Signature Policy [Exhibit R](#) – Must Acknowledge with any Exceptions
13. Appendix S – Records And Information Management Governance Policy [Exhibit S](#)
14. Appendix T - IT Usage and Security Policy [Exhibit T](#) – Must Acknowledge with any Exceptions
15. Copies of all applicable licenses, certificates and permits Offeror possesses to carry out the Services required in the State of New Mexico

Exhibit A – Functional Specification Workbooks

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

67

Version: 04212022

Exhibit B – Reference Form

Please copy Table 15 below to list five (5) references, at least two (2) of which must be from cities/counties where the scope of the implementation is similar to the scope of work as described in this RFP. These references should be sites at which the software has been fully implemented within the past five (5) years.

For each reference listed, offeror must disclose if it has offered or provided any benefits, products, discounts or other in-kind services/products to the reference in exchange for fulfilling the role of providing a customer reference.

Table 15

REFERENCE #	
Project Name & Location	
Completion Date (Actual or Estimated)	
Project Owners Name & Address	
Project Owner’s Contact Person, Title, Telephone number, and email address	
Estimated Cost for Entire Project	
Estimated Cost for Work Which Firm was/is Responsible	
Scope of Entire Project (Please give quantitative measurements if possible)	

Exhibit C – Resume Form

RESUME OF KEY PERSONNEL

Provide a brief resume of key persons, specialists, and individual third-party offerors that would be representative of the persons assigned to this project. Copy Table 16 below and complete it for each staff member as needed.

Table 16

Name and Role on Project	
Previous Project Assignments	
Name of 3rd Party Offeror with which associated	
Years of Experience	
Education Degree(s)/Year/Specialization	
Other Experience & Qualifications relevant to the proposed project	

Exhibit D – Notification to Propose Form

NOTIFICATION TO PROPOSE

Use this form to inform interest as a potential proposer for this procurement. Only registered offerors will be emailed courtesy notices of changes or addenda to these procurement documents. Complete this form and email to Derrill.rodgers@lacnm.us and Katherine.stoddard@lacnm.us.

Failure to complete and return this form may result in the rejection of your Proposal:

Title: **Incorporated County of Los Alamos NM RFP No. 24-56**

Company Name: _____
Contact Person: _____
Mailing Address: _____
City: _____
State/ZIP: _____
Email: _____
Phone: _____

Exhibit E – Addenda Acknowledgement Form

ADDENDA ACKNOWLEDGEMENT

Each proposer is requested to acknowledge receipt of Addenda in relation to the “CMRJ - Integrated Public Safety Software System” RFP No. 24-56 by their signature affixed hereto and shall attach this appendix to the original proposal.

We have received the following Addenda in relation to the Integrated Public Safety Software System RFP No. 24-56

NOTIFICATION BY PROPOSER

NAME: _____

SIGNATURE: _____

TITLE: _____

COMPANY: _____

DATE: _____

Exhibit F – Proposal Cost Summary Sheet and Proposal Cost Sheets

Software-CAD	
Item	Cost
CAD Base Application Software	
CAD Base Mapping Software	
CAD Modules (in addition to Base)	
CAD Implementation Services	
Subtotal	
Software-LERMS	
Item	Cost
Law RMS Base Application Software	
Law RMS Application OPTIONAL Software	
Law Implementation Services	
Subtotal	
Software-JMS	
Item	Cost
Jail Management Base Application Software	
Jail Management Base OPTIONAL Modules	
Jail Management Implementation Services	
Subtotal	
Software-Mobile	
Item	Cost
Base LE Mobile Applications Software	
Base LE Mobile Mapping Software	
Base Fire/EMS Application Software	
Base Mobile Mapping Software	
Mobility for IOS tablets	
Field Reporting Application Software-Law Enforcement	
Mobile/Field Reporting Implementation Services	
Subtotal	
Software-Required Interfaces	
Item	Cost
CAD Interfaces - REQUIRED	
CAD/Mobile Interfaces - OPTIONAL	
LAW Interfaces - REQUIRED	
LAW Interfaces - OPTIONAL	
Jail Interfaces - REQUIRED	
Jail Interfaces - OPTIONAL	
Interface Implementation Services	
Subtotal	
Hardware-Needed for the System Software	
Item	Cost
Hardware Needed for the System Software	
Subtotal	
Hardware-Conversion Support	
Item	Cost
Data Conversion and Conversion Support	
Subtotal	

System Maintenance Cost	
Item	Cost
System Maintenance Cost	
Subtotal	

SOFTWARE - CAD		
Item	Quantity	Price
CAD Base Application Software*	Lot	
Call Entry		
Call List/Grid Control Panel		
Unit List/Grid Status Control Panel		
Unit Recommendations		
Run Cards/Response Plans		
Call Stacking		
CAD Messaging		
Call Scheduling		
Fire Equipment and Apparatus Search/Move/Assign		
GIS/Geo File Verification		
CAD Base Mapping Software		
CAD AVL		
Proximity Dispatch		
CAD Modules (in addition to base)		
Hazmat Search		
Hydrant Search		
Shift Notes		
BOL/BOLOs		
CAD Analytics and Ad-hoc Reporting		
Wrecker Rotation/Service Vehicle Rotation		
Web CAD (CAD access via browser)		
Integration to Mobile		
CAD Workstation Client	10	
CAD Workstation Mapping	10	
CAD Administrator/Maintenance Positions	6	
WebCAD (browser based view of CAD information)	150	
System Administrator/File Maintenance Training		
Call Taker/Dispatcher Training		
CAD Software System Integration Services**	Lot	
Additional Costs (Must Provide Details)		
Subtotal		

[*] If an individual module listed in the pricing sheet is not included in the base price, include the cost for that module; if the cost is included in the base package then indicate "included".

**** System integration services includes vendor project management, installation, travel, expenses, etc.

SOFTWARE - LERMS		
Item	Quantity	Price
Law RMS Base Application Software*	Lot	
Animal Control		
Incident/Event Tracking		
Accident/Crash Reporting		
Business/Building Entry		
Arrest Processing		
Pre-Booking		
Career Criminal Tracking		
Case Entry		
Case Management		
Investigations		
Field Contacts/Field Interview		
Civil Process		
Analytics and Ad-hoc Reporting		
Crime Reporting (NIBRS)		
Line-up/Mug Shots		
Master Location Index		
Master Name Index		
Master Vehicle Index		
Personnel and Training		
Property & Evidence Processing		
Tickets and Citations		
Wants and Warrants		
Law RMS Application OPTIONAL Software*	Lot	
Fleet Maintenance		
Law Asset Tracking		
Animal Control		
Gang Tracking		
Narcotics		
Personnel and Training		
Impounded Vehicles		
Law Workstation Clients	70	
Law Concurrent Users	45	
System Administrator/File Maintenance Training		
LERMS User Training		
LERMS Software System Integration Services**	Lot	
Additional Costs (Must Provide Details)		
Subtotal		

[*] If an individual module listed in the pricing sheet is not included in the base price, include the cost for that module; if the cost is included in the base package then indicate "included".

[**] System integration services includes vendor project management, installation, travel, expenses, etc.

SOFTWARE – JMS		
Item	Quantity	Price
Jail Management Base Application Software [*]	Lot	
JM Booking and Intake		
JM Inmate Classification		
JM Inmate Housing		
JM Officer Activity Log		
JM Master Name Index		
JM Inmate Scheduling and Tracking		
JM Inmate Property Tracking		
JM Inmate Programs		
JM Inmate Movement Tracking		
JM Inmate Contacts/Visitation		
JM Case Management		
JM Inmate Activity Log		
JM Workstation Clients	8	
JM Concurrent Users	6	
Jail Management OPTIONAL Modules [*]	Lot	
Personnel Administration and Training		
Personnel Activity Reporting and Scheduling		
Personnel and Facility Equipment Tracking/Asset Management		
JM Inmate Incident and Disciplinary Tracking		
JM Inmate Grievance Tracking		
JM Inmate Financial Management		
JM Inmate Commissary		
JM System Administrator/File Maintenance Training		
JM User Training		
JMS Software System Integration Services[**]	Lot	
Additional Costs (Must Provide Details)		
Subtotal		

[*] If an individual module listed in the pricing sheet is not included in the base price, include the cost for that module; if the cost is included in the base package then indicate "included".

[**] System Integration Services includes Vendor project management, installation, travel, expenses, etc.

SOFTWARE - MOBILE		
Item	Quantity	Price
Base LE Mobile Application Software*	Lot	
Dispatch/Messaging		
Unit Status Changes		
State/NCIC/NLETS		
LE Demographic (Racial) Profiling		
Base LE Mobile Mapping Software		
In-Car Mapping/AVL		
In-Car Routing (driving directions)		
In-Car Mapping/Geofencing		
Base Fire/EMS Mobile Application Software		
Dispatch/Messaging		
Unit/Apparatus Status Changes		
Base Fire Mobile Mapping Software		
In-Car Mapping/AVL		
In-Car Routing (driving directions)		
Mobility for iOS tablets		
Fire & EMS Dispatch (unit status monitor, map, call list, dispatch, and AVL)		
Field Reporting Application Software – Law Enforcement		
LE Field Reporting (Incident, Case, Arrest, Field Contact)		
LE Field Reporting - New Mexico Accident submission		
LE Field Reporting - Etix - New Mexico Uniform Traffic Citation		
Law Mobile Licenses	40	
Law Field Reporting Licenses	40	
Fire/EMS Mobile Licenses	75	
Mobile System Administrator Training		
Mobile User Training (Train-the-Trainer)		
Field Reporting System Administrator Training		
Field Reporting User Training (Train-the-Trainer Law Enforcement)		
Mandatory Software System Integration Services**		
Additional Costs (Must Provide Details)		
Subtotal		

¹⁾ If an individual module listed in the pricing sheet is not included in the base price, include the cost for that module; if the cost is included in the base package then indicate "included".

*** System integration services includes vendor project management, installation, travel, expenses, etc.

SOFTWARE – Interfaces		
Item	Quantity	Price
CAD Interfaces - Required		
ASAP (incoming Alarm calls)	Lot	
Alphanumeric Paging	Lot	
Smart 911	Lot	
CAD to Fire Mobile/FRMS - ESO Firehouse	Lot	
E911	Lot	
Logging Recorder (Revcord)	Lot	
WebEOC	Lot	
Pro QA Paramount - EMD, EFD	Lot	
Pictometry	Lot	
CAD to EMS Mobile/ePCR - ESO Medical	Lot	
Fire Station Alerting (WestNet)	Lot	
Tone Encoding (Radio Console or Encoder Device) Harris Radio System	Lot	
State/NCIC Interface (NMLETS/NCIC) for CAD and Mobile	Lot	
CAD/Mobile Interfaces - OPTIONAL		
CAD ASAP to PSAP - commercial alarm interface	Lot	
Mobile to ePCR	Lot	
Mandatory Software System Integration Services **		
Additional Costs (Must Provide Details)		
Law Interfaces - Required		
Property Room Bar Coding	Lot	
Asset Management Bar Coding - LERMS	Lot	
State Accident Import - TraCS	Lot	
State Ticket Import - TraCS	Lot	
Community Crime Mapping - incident information transfer	Lot	
State Ticket Export - FullCourt	Lot	
State/NCIC Interface (NMLETS/NCIC) for LERMS	Lot	
Livescan/AFIS	Lot	
LiNX Interface	Lot	
Law Interfaces - OPTIONAL		
Interface to BEAST - Porter Lee Evidence Management System	Lot	
Interface to Forms Tool - if not native to vendor solution	Lot	
Interfaces with/to Prosecuting Attorney via web/browser-based application	Lot	
Mandatory Software System Integration Services **		
Additional Costs (Must Provide Details)		

CONVERSION SUPPORT		
Item	Quantity	Price
Conversion Analysis and Assessment	Lot	
Hourly Rate for Conversion Engineering Support		
Initial Data Conversion Estimate	Lot	
Additional Maintenance Costs (Must Provide Details)		
Subtotal		

SYSTEM MAINTENANCE – System Software		
Item	Quantity	Price
1st Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
2nd Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
3rd Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
4th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
5th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
6th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
7th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
8th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
9th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
10th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
11th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
12th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
13th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
14th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
15th Year Maintenance 24x7 Maximum 4 Hour Response	Lot	
Additional Maintenance Costs (Must Provide Details)		
Subtotal		

Exhibit G – Verification of Authorized Offeror Form

VERIFICATION OF AUTHORIZED OFFEROR

RFP NO: 24-56

RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM

This document should be returned with RFP submittal.

Sec. 31-261. - State and local preferences.

- (a) *Definitions.* For the purposes of this section:
- (1) The terms "resident business" and "resident veteran business" shall be defined as set out in NMSA 1978, § 13-1-21;
 - (2) The term "local" as applied to a business shall mean that it meets the requirements of the above definition, maintains its principal office and place of business in Los Alamos County, and has a required Los Alamos County business license.
- (b) *Requirements for preference qualification.* The chief purchasing officer shall determine if a preference is applicable to a particular bid or offer on a case-by-case basis. An offeror must submit a written request for preference, with a copy of the state-issued preference certificate, with its bid or proposal to qualify for this preference.
- (1) If a corporation, it shall be incorporated in New Mexico and maintain its principal office and place of business in the state;
 - (2) A person shall have qualified with the state chief purchasing officer as a resident business or resident veteran business and obtained a certification number as provided in NMSA 1978, § 13-1-22.
- (c) Preference factor.
- (1) The preference factor for qualifying resident and local businesses applied to bids and proposals shall be five percent.
 - (2) The preference factor for qualifying resident veteran businesses shall be in accordance with the requirements set forth in NMSA 1978, § 13-1-21.
- (d) *Invitations for bids.* When bids are received, the price quoted by the qualifying offeror shall be multiplied by 0.95. After application of the preference factor, the contract shall be awarded to the lowest offeror. If one or more low prices are equal, the bid shall be awarded with respect to the next category of offerors listed below, and the next, until an offer qualifies for award. The priority of categories of offers is as follows:
- (1) Local business;
 - (2) Resident business.
- (e) *Requests for proposals.* When proposals are received, the total evaluation score with or without the cost factor of each proposal received from a qualifying offeror shall be multiplied by 1.05. After application of the factor, the contract shall be awarded to the highest score. If one or more scores are equal, the same procedure shall be followed with respect to the next category of offerors listed, and the next, until an offer qualifies for award. The priority of categories of offerors is the same as listed in subsection (d) of this section.

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

- (f) *Exemptions from preferences.* The resident and local preference specified in this article shall not be applied:
- (1) To requests for qualifications;
 - (2) To any purchase of goods or services in excess of \$500,000.00;
 - (3) When the expenditure of federal funds designated in whole or in part for a specific purchase is involved; or
 - (4) When the expenditure of grant funds, a condition of which prohibits a local preference, is involved.

(Ord. No. 02-098, § 2, 12-2-2008; Ord. No. 02-305, § 8, 2-25-2020)

Are you requesting Preference?

YES NO

By answering “yes,” the offeror is submitting a written request for preference.

An Offeror must submit a copy of the state-issued preference certificate with its bid or proposal to qualify for this preference.

Having read the proposal conditions and examined the scope of services and deliverables for this RFP, this Proposal is hereby submitted by:

/			
Signature and Printed Name of Authorized Offeror	Title		
Organization’s Legal Name	State of Incorporation		
Email Address			
Mailing Address	City	State	Zip Code
Physical Address	City	State	Zip Code
Telephone No.			
Federal Tax I.D. #	NM CRS # (if located in-state)		

Contract Manager Printed Name, Title and Email Address

If your firm meets the definition of one or more of the types of business described below as defined by the Small Business Administration, please check the appropriate box:

- Small Business**
- Woman-owned Business**
- Minority-owned Business**

Exhibit H – Primary Covered Transactions Certification Form

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS – PRIMARY COVERED TRANSACTIONS

RFP NO: 24-56

RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM

This document should be returned with RFP submittal.

(1) I or We, _____ (the “Offeror/Bidder”) hereby certify to the best of our knowledge and belief that neither the Offeror/Bidder nor any of its principals:

- (a) are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal, state, or local department or agency; and
- (b) have, within a 3-year period preceding this certification, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery; falsification or destruction of records; making false statements; or receiving stolen property; and
- (c) are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and
- (d) are not current or former County employees. If an Offeror/Bidder is a current or former county employee, Offeror/Bidder shall provide additional information as described in paragraph (2) of this certification; and
- (e) are not considered to be an “immediate family member” of a County employee or public official. Immediate family means the employee’s or public official’s spouse, parents, step-parents, child, step-child, sibling, step-sibling, half-sibling, grandparent, grandchild, aunt, uncle, niece, nephew, or their in-laws, or an individual claimed by the public official or his/her spouse as a dependent under the United States Internal Revenue Code; and
- (f) have within a 3-year period preceding this certification had one or more public transactions or contracts (federal, state, or local) terminated for cause or default.

(2) If we are unable to certify to any of the statements in this certification, we shall attach an explanation hereto.

(3) Certification to any of the statements in this certification will be thoroughly reviewed, and may not necessarily preclude the Offeror/Bidder from consideration for award.

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

(4) Falsification of any statement in this Form shall constitute grounds for non-consideration of the Offeror's/Bidders proposal or bid or rescinding of a contract award.

Date

Authorized Representative's Signature

Print Name

Print Title

Exhibit I – Campaign Contribution Disclosure Form

CAMPAIGN CONTRIBUTION DISCLOSURE FORM
AGRXX-XX
RFP NO: 24-56
RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM

This document should be returned with RFP submittal.

Any prospective contractor seeking to enter into a contract with the Incorporated County of Los Alamos must file this form disclosing whether they, a family member or a representative of the prospective contractor has made a campaign contribution to an applicable public official during the two (2) years prior to the date on which prospective contractor submits a proposal or, in the case of a sole source or small purchase contract, the two (2) years prior to the date prospective contractor signs the contract, if the aggregate total of contributions given by the prospective contractor, a family member or a representative of the prospective contractor to the public official exceeds TWO HUNDRED FIFTY DOLLARS (\$250.00) over the two (2) year period.

THIS FORM MUST BE FILED BY ANY PROSPECTIVE CONTRACTOR WHETHER OR NOT THEY, THEIR FAMILY MEMBER, OR THEIR REPRESENTATIVE HAS MADE ANY CONTRIBUTIONS SUBJECT TO DISCLOSURE.

The following definitions apply:

“Applicable public official” means a person elected to an office or a person appointed to complete a term of an elected office, who has the authority to award or influence the award of the contract for which the prospective contractor is submitting a competitive sealed proposal or who has the authority to negotiate a sole source or small purchase contract that may be awarded without submission of a sealed competitive proposal.

“Campaign Contribution” means a gift, subscription, loan, advance or deposit of money or other things of value, including the estimated value of an in-kind contribution, that is made to or received by an applicable public official or any person authorized to raise, collect or expend contributions on that official’s behalf for the purpose of electing the official to either statewide or local office. “Campaign Contribution” includes the payment of a debt incurred in an election campaign, but does not include the value of services provided without compensation or unreimbursed travel or other personal expenses of individuals who volunteer a portion or all of their time on behalf of a candidate or political committee, nor does it include the administrative or solicitation expenses of a political committee that are paid by an organization that sponsors the committee.

“Contract” means any agreement for the procurement of items of tangible personal property, services, professional services, or construction.

“Family member” means a spouse, father, mother, child, father-in-law, mother-in-law, daughter-in-law or son-in-law of:

- (a) a prospective contractor, if the prospective contractor is a natural person; or

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

(b) an owner of a prospective contractor.

“Pendency of the procurement process” means the time period commencing with the public notice of the request for proposals and ending with the award of the contract or the cancellation of the request for proposals.

“Person” means any corporation, partnership, individual, joint venture, association or any other private legal entity.

“Prospective contractor” means a person who is subject to the competitive sealed proposal process set forth in the Procurement Code or is not required to submit a competitive sealed proposal because that person qualifies for a sole source or a small purchase contract.

“Representative of a prospective contractor” means an officer or director of a corporation, a member or manager of a limited liability corporation, a partner of a partnership or a trustee of a trust of the prospective contractor.

DISCLOSURE OF CONTRIBUTIONS: (Report any applicable contributions made to the following - COUNTY COUNCILORS: Theresa Cull; Denise Derkacs; Keith Lepsch; David Reagor; Randal Ryti; Melanee Hand; and Suzie Havemann.)

Contribution Made By:			
Relation to Prospective Contractor:			
Name of Applicable Public Official:			
Contribution(s) Date(s)	Contribution Amount(s):	Nature of Contribution(s):	Purpose of Contribution(s):
	\$		
	\$		
	\$		
	\$		
	\$		

(Attach extra pages if necessary)

Please check the box next to the applicable statement.

	CONTRIBUTIONS IN THE AGGREGATE TOTAL OVER TWO HUNDRED FIFTY DOLLARS (\$250.00) WERE MADE to an applicable public official by me, a family member or representative, and I have disclosed those contributions.
	NO CONTRIBUTIONS IN THE AGGREGATE TOTAL OVER TWO HUNDRED FIFTY DOLLARS (\$250.00) WERE MADE to an applicable public official by me, a family member or representative.

Signature

Date

Title (position)

Exhibit J – Confidential Information Disclosure Statement

Confidential Information Disclosure Statement

RFP NO: 24-56

RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM

Incorporated County of Los Alamos is a governmental entity subject to certain disclosure laws including, but not limited to, the New Mexico Inspection of Public Records Act (1978) NMSA §§14-2-1, et seq. Nothing in this Agreement is intended to diminish or expand the application of any applicable disclosure laws to any proprietary or confidential information.

This Confidential Information Disclosure Statement (“Statement”) defines obligations and waivers related to Confidential Information disclosed pursuant to the above referenced Agreement between County and Contractor. County and Contractor agree to the following:

1. Statement Coordinator – Each party designates the following person as its Statement Coordinator for coordinating the disclosure or receipt of Confidential Information:

Contractor: _____

Email: _____

County: _____

Los Alamos, New Mexico 87544

2. Definitions -

- a) **Confidential Information** - any form of information, in any format, disclosed by the Discloser to the Recipient and identified in writing as confidential.
- b) **Discloser** - the party disclosing Confidential Information.
- c) **Exception** – An exception is satisfied if the Confidential Information disclosed: (i) was in Recipient’s possession prior to receipt from Discloser, (ii) is publicly known or readily ascertainable by legal means, (iii) is lawfully received by Recipient from a third party without a duty of confidentiality, (iv) is disclosed by Discloser to a third party without a duty of confidentiality on the third party, (v) is independently developed or learned by Recipient, or (vi) is disclosed by Recipient with Discloser’s prior written approval.
- d) **Recipient** – the party receiving Confidential Information.

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

3. Obligations – Recipient shall protect and ensure its participating subcontractors, agents, or associates shall protect all Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination, or publication of the Confidential Information as Recipient uses to protect its own information of a like nature. If any person or entity requests or demands, by subpoena or otherwise, all or any portion of the Confidential Information provided by one party to another, the party receiving such request shall immediately notify the Discloser of such request or demand. The party receiving the request or demand shall independently determine whether the information sought is subject to disclosure under applicable law including the New Mexico Inspection of Public Records Act. If the party receiving the request or demand determines that the information is subject to disclosure, it shall notify the Discloser of its intent to permit the disclosure with sufficient time to permit the Discloser to invoke the jurisdiction of an appropriate court or administrative body to raise any legitimate objections or defenses it may have to the disclosure. In the absence of an appropriate order prohibiting the disclosure, the party receiving the request or demand shall permit and proceed with the disclosure without incurring any duty, obligation or liability to the Discloser.

Exhibit K – Incorporated County of Los Alamos Technical Questions Acknowledgement Required

Additional technical questions to include in On-premises & SaaS solicitations as applicable

A. Service Level Agreement / Support Maintenance.

1. **[SaaS]** Provide proposed Service Level Agreements including Uptime (scheduled and/or unscheduled downtime) and other service metrics (user response times, percent delivered within 30 seconds), and compensations for missed performance benchmarks.
2. **[On-Premise/SaaS]** Provide Support Options and all terms of support, including support hours and methods of contacting support.
3. **[On-Premise/SaaS]** Provide the communication plan for communicating system upgrades, and all other maintenances and service interruptions.
4. **[On-Premise/SaaS]** Describe the methodology for testing and certifying upgrades and patches to ensure that they work properly. Describe the mechanism of versioning roll back in case of issues.
5. **[On-Premise/SaaS]** Describe the process of applying upgrades and patches including, if there are client/user responsibilities, and a responsibility matrix for the tasks involved.
6. **[On-Premise/SaaS]** Provide a brief history of product upgrades and interim patches/fixes released in the last 18 months.
7. **[On-Premise/SaaS]** Identify the most current stable release and patch level, certified for support, for all software and firmware, and acknowledge that all software and firmware will be installed to those levels.

B. Ownership / Recovery

1. **[SaaS]** Acknowledge the following: County retains all rights to its data and materials. Use of the Contractor's system confers no ownership rights to the Contractor and County Materials and Data may be used by the Contractor only as necessary to provide contracted services.
2. **[On-Premise/SaaS]** Discuss how the solution meets statutory requirements for data ((ex. PII, HIPAA, CJIS, Gramm-Leach-Bliley Act, FIPS 199...)).
3. **[SaaS]** Discuss access to the County's data via ODBC or alternative method, and any limitations to that access.
4. **[On-Premise/SaaS]** Describe the support provided for performing legal discovery on the system.
5. **[SaaS]** Describe the method(s) of turning over County data, and providing a reader for that data, upon termination of services.

C. Administration

1. **[On-Premise/SaaS]** Describe the use of Permission Levels, Roles or other mechanisms to manage authorities to create read, update, and delete data.
2. **[On-Premise/SaaS]** Describe the system's use of Active Directory Groups and Group Policies.
3. **[On-Premise/SaaS]** Describe authentication mechanisms available.
4. **[On-Premise/SaaS]** Describe the ability of users to maintain their own profile.
5. **[On-Premise/SaaS]** Describe any interfaces or integrations with Directory Services.
6. **[On-Premise]** Describe the options available to support unattended client installation via Microsoft SCCM and Intune Platform.

D. Security

1. **[SaaS]** Describe the classification of the proposed Cloud solution. Is the solution SaaS, PaaS, IaaS or a combination of the classification types? Is the solution hosted, owned and operated, by CSP or is the solution a partnership of several CSPs including infrastructure partners?
2. **[SaaS]** Describe the security measures in-place, and available, to protect the system and its data.
3. **[SaaS]** Submit details on hosted or cloud service provider's data center and information security compliance.
4. **[SaaS]** Identify any encryption algorithms used.
5. **[SaaS]** Describe the policies that apply to, and notification measures to be used in the event of a security breach.
6. **[On-Premise/SaaS]** Do you scan your code/application for vulnerabilities during software development? If so,
 - a. What are you using for Static Application Security Testing (SAST)?
 - b. If you are using third party libraries, are you scanning those with a Software Composition Analysis (SCA) tool?
 - c. Once your solution is production ready, are you scanning it again with a Dynamic Application Security Testing (DAST) tool?

E. Compatibility & Requirements

1. **[On-Premise/SaaS]** Acknowledge review of County's Technology Standards and provide narrative as to the compatibility of the elements listed that is applicable to the proposed solution.

Desktop hardware

Windows operating system

Web Browsers

Compatibility with collaboration and web publishing tools

SSL Encryption

ESRI GIS mapping functionality

Android and IOS mobile operating systems

2. **[On-Premise/SaaS]** Does your proposed solution have specific network requirements for characteristics such as bandwidth, Protocols, TCP Ports, Latency, Packet loss, Jitter or other network characteristics? Identify and discuss those requirements.
3. **[On-Premise/SaaS]** The County has many software in use. The proposal should not compromise existing software. Discuss any known incompatibilities with other software.
4. **[On-Premise/SaaS]** Describe any dependencies with 3rd party software/services, e.g., Java, .NET, Crystal Reports, MySQL, including the supported version(s) of the software and whether the proposal includes the software, its licensing and its installation.
5. **[On-Premise/SaaS]** Identify and discuss any known hardware compatibility issues and requirements.
6. **[On-Premise/SaaS]** Describe the use and requirements of all County resources that are expected to be used in the proposal, e.g., DHCP services, DNS services, SMTP services, electrical power, uninterruptible power supplies, video conferencing, data center rack space, word processing software, cooling capacity, training facilities.

F. Business Continuity and Disaster Recovery

1. **[SaaS]** Submit information on Cloud Service Provider and physical infrastructure including locations and internet connectivity.

2. **[SaaS]** Submit Business Continuity and Disaster Recovery plans.
3. **[SaaS]** Submit descriptions of any Data Center(s) pertinent to the proposal including their Tier and salient characteristics.
4. **[SaaS]** Describe the backup plan for the proposal.
5. **[SaaS]** Describe the Who, What, When, Where, Why and How of the software escrow.
6. **[SaaS]** Describe the Who, What, When, Where, Why and How of recovering the County's data should the successful Contractor cease operations.

G. System Monitoring and Alerting

1. **[On-Premise/SaaS]** Describe the system's capabilities that support system monitoring and alerting in Netreo Omnicenter system or another monitoring and management system.

H. Hardware and Software

1. **[On-Premise/SaaS]** Submit a complete itemized schedule of all hardware contained in the proposal.
2. **[On-Premise/SaaS]** Submit a complete itemized schedule of all software contained in the proposal.
3. **[On-Premise/SaaS]** Should your solution require additional software, hardware, etc., Offerors to acknowledge that the County may separately procure the proposed hardware and software, other products or its equivalent specified by the Contractor, or substitute functionally equivalent hardware, software or other products for use in the proposed system. Confirm that such procurement or substitution shall have no effect on Contractor's warranty, support, or other obligations.

Exhibit L – Incorporated County of Los Alamos Technical Standards Acknowledgement Required



Los Alamos County Technology Standards Requirements On-Premise, Hybrid or Cloud/Hosted Solution Solicitations

The following Los Alamos County Technology Standards are required and shall be supported by the vendor, contractor, reseller hence forth called Operator, for any County solicitation requiring technology or integration to the County network and incorporated into any resultant agreement. Standards are listed with the expectation that the Operator will provide software updates to allow Los Alamos County to stay on supported versions of hardware, underlying software and protocols as outlined below.

Respondents must provide documentation that they meet the requirements in respect to the solution that they are responding with. On premise respondents do not need to comply with hosted requirements. Hosted solution respondents do not need to comply with on-premise requirements. If the solution is a hybrid of both categories of solution, then both on-premise and hosted requirements apply as applicable to the response.

Server Operating system (OS) (On-Premises)	Microsoft (MS) Windows Server 2019, 64 bit or current (Standard and Datacenter). Contractor software must be maintained to run on a supported platform service level as defined by Microsoft at the latest stable patch level. Departments will be responsible for licensing costs and must request cost estimates from Information Management (IM) Division.
Server Hardware (On-Premise)	Preferred: Use of County VMware server platform. Environment design must be submitted and reviewed by IM Division for acceptance. Proposals shall include required hardware and licensing of VMware, operating system, and proposed application-based requirements. Application with a proven Virtual installation template is preferred. Physical Server minimum hardware specifications consist of: Multi Socket/Multi Core processor Intel or AMD based server (standalone or blade server as determined by Los Alamos County IM Division with a minimum 64 GB RAM and RAID capability. Contractor software must be maintained to run on a supported platform service levels as defined by Microsoft at the latest stable patch level.
Network Infrastructure	See LAC Standards and Specifications for Building and Campus Distribution Systems Version 3 (Primarily used for building construction purposes).
Network (On-Premise)	Supported network protocol is TCP/IP (IPv4). Standards based NIC rated at 100/1000/10G copper or fiber is supported. If considering a 10G connection County IT network group shall be consulted to ensure equipment compatibility and availability at proposed site. Additional hardware cost, may be required of the project, based on project requirements, equipment and availability. The County uses Cisco technology as its default network equipment standard. Solutions shall be compatible with Cisco Network Technology.
Remote Network Access (On-Premise)	Direct remote access to the County network and server environment shall be done using the County's Cisco AnyConnect SSH VPN. Once a VPN connection is established end-point connections are supported via Microsoft RDP. Operator support accounts shall be set up in accordance with the adopted Los Alamos County IT Usage and Security Policy #1210.

Approved By: CIO

Approved Date: 01/17/2023

RFP No. 24-56
Issued by Procurement Division: **D. Rodgers**

LAC Network Account Privilege (On-Premise & Hosted)	Desktop Client Software shall function for end users with standard user privileges; user cannot install software and shall not have administrative rights.
Desk Hardware (On-Premise & Hosted)	Physical unit minimum hardware requirements consist of: Intel core i5 based processor, minimum 8 GB RAM, Intel integrated graphics 1280 capable video minimum, display port, input or HDMI, 4 USB 2/3 ports. Support deployment onto Virtual Desktop Infrastructure (VDI) platform, specifically cloud-based platforms from Microsoft Azure, Amazon Web Service (AWS) or Google Cloud Platform.
Desktop OS (On-Premise & Hosted)	Microsoft Windows 10 at current Service Pack (SP)
Internet Browser (On-Premise & Hosted)	Internal County Network: Google Chrome and Edge, at its latest version, are the installed browsers on county devices. Google Chrome is the county standard. New web Applications must be based on HTML5. Applications requiring Internet Explorer, Microsoft Silverlight, Java and Flash are not supported. Web applications requiring .NET framework shall not be considered. IM Division shall be consulted for compatibility issues prior to considering new application purchases requiring Java.
Database Software Products (On-Premise)	Supported database software is Microsoft (MS) SQL server version 2016 through current. New MS SQL Server product installations will require review, purchasing of licenses, appropriate hardware, and maintenance in support of proposed project or instance install to the County MS SQL Server Environment. MS SQL server software for new implementations shall be at within the Microsoft certified support release level or current. Server components for proposed projects require review and purchasing as part of the project initiative. Operator software must be maintained to run on a supported platform service level as defined by Microsoft. <ul style="list-style-type: none"> • Passwords are not permitted to be transported in clear\plain text. • Vendor implementation shall not use the SA password for user level functions. SA passwords shall be maintained by the County DBA. • Only database instances can be installed on the County MS-SQL Environment. If a vendor software component install is necessary on the database server, a standalone installation will be required. • Vendor software must use standard Access & Connection architecture for accessing databases on the County MS-SQL Environment. • Applications based on Microsoft Access are not supported. Applications based on SQLEXPRESS version should be reviewed and the limitation understood by the customers and the vendor. Hosted solutions shall be compliant with or provide a method to provide the County with database exports in the MS-SQL Server format.
Internet: Collaboration and Web Publishing (On-Premise & Hosted)	Use of Internet apps or links shall be considered in collaboration with the Los Alamos Information Management Division Applications group for review to ensure that compatibility and Internet publishing protocols have been satisfied prior to formation of any agreement or installation.

Approved By: CIO

Approved Date: 01/17/2023

RFP No. 24-56
Issued by Procurement Division: **D. Rodgers**

Intranet: Collaboration and Web Publishing (On-Premise & Hosted)	Microsoft SharePoint Online is the basis for the County's Intranet. Any products that will integrate or utilize the County's Intranet site shall require a compatibility consultation with IM Division before purchase and implementation. Operator software shall be maintained to run on supported platform service levels as defined by Microsoft and/or the Intranet site vendor. Proposed Intranet software products shall be accompanied by roadmap for compatibility with MS SharePoint Online.
Productivity Software (On-Premise & Hosted)	Los Alamos County uses Microsoft M365 Office Suite at its most recent version and service pack. Operator software using the Office suite must be maintained to run on supported platform service levels as defined by Microsoft.
Email (On-Premise & Hosted)	Microsoft M365 with hub transport for relay. If SMTP relay access from on premise vendor specific software is necessary, permission to use the County Email exchange shall be obtained prior to contracting or purchase of the software or solution. If SMTP relay access from hosted vendor specific software is necessary, preference is for SMTP relay to be hosted by vendor. The vendor specific solution must be supported and maintained to relay off County email domain and directed to hand off the email message to another mail server that can get the message closer to its intended recipient in accordance with service levels as defined by Microsoft for the M365 product.
Geographic Information Standards (GIS) (On-Premise & Hosted)	The County uses strictly ArcGIS products by Esri for GIS. Desktop software for end users includes ArcGIS Desktop and ArcGIS Pro. GIS web services are provided as REST endpoints from ArcGIS Server using Internet Information Services (IIS). Our enterprise geodatabase is managed using ArcSDE with Microsoft SQL Server. Supported versions are one or two iterations behind the latest ESRI-supported release. The preferred method for applications to interact with GIS is via REST services. Web applications must be hosted in either ArcGIS Online or ArcGIS Portal.
Mobile Devices	Shall conform to Los Alamos County Mobile Policy #1240. Mobile devices requiring Intranet access must be secured through the County Mobile Device Management System.
Security & SSL (On-Premise & Hosted)	<p>Intranet devices must be capable with multi-factor authentication (MFA) using the County's current MFA systems. Any requirements for access to ports from the Internet into the County Network shall be approved via a technical review by the IM Division before product(s) purchase and implementation. Cisco Secure EndPoint Antivirus and Antispyware Enterprise software are used on all intranet computing devices; vendor solutions shall work in conjunction with stated antivirus products.</p> <p>SSL (Secure Socket Layer) encryption is required for both internal and external facing web applications.</p> <p>Enterprise-wide applications shall be capable of Active Directory integration for user authentication and utilize County's MFA.</p> <p>Devices requiring wireless access must a) be domain integrated or b) have the ability to accept captive portal agreement (a web page that the user of a public-access network is obliged to view and interact with before access is granted).</p>
Records	Shall conform to Los Alamos County Records and Information Governance Policy #0310
E-Signature	Shall conform to Los Alamos County E-signature Policy #1220.

Approved By: CIO

Approved Date: 01/17/2023

RFP No. 24-56
 Issued by Procurement Division: [D. Rodgers](#)

<p>Hosted/Cloud Based Services</p>	<ul style="list-style-type: none"> • Los Alamos County is interested in taking advantage of Anything as a Service (XaaS) opportunity available through Cloud Service Providers (CSP), in Government Cloud (GCC) where required. CSP data centers must be located within the United States. • Enterprise-wide applications shall be capable of Active Directory integration for user authentication and utilize County's MFA. • Data centers must be FedRAMP certified for SaaS solutions procured by departments if they also store or may store Los Alamos National Laboratory (LANL) critical infrastructure data for County operations. Departments must verify with LANL authority to confirm that this requirement is applicable to the LANL information to be stored. • Ownership of County data held in the CSP solution shall remain with the County of Los Alamos. County may have on-demand access to the data for export/download or have the data delivered by request by the CSP with a maximum 48-hour compliance window. Exports shall be in MS-SQL format.
------------------------------------	--

Note: As applicable, RFPs must include the **Technology Standards** and the following referenced policy documents that can be found in the County's Intranet MyPlace site - <https://lacnm.sharepoint.com/SitePages/Policies-and-CMOReports.aspx>

- County IT Usage and Security Policy #1210
- Los Alamos County Records and Information Governance Policy #0310
- Los Alamos County E-signature Policy #1220

Approved By: CIO

Approved Date: 01/17/2023

RFP No. 24-56
 Issued by Procurement Division: [D. Rodgers](#)

Exhibit M – Sample Services Agreement

County requires Submission of County’s Standard Sample Service Agreement with Deviations or Exceptions Noted or Acknowledgment of No Deviations or Exceptions.

- Offeror should note any deviations or exceptions to Exhibit “M” in Offeror’s response (include those noted deviations/exceptions in the Letter of Transmittal). Provide the original language with the County’s standard terms and any suggested edits or acknowledge that Offeror has no deviations or exceptions. (Please also see “Award of Solicitation” above.)
- Offerors should provide with their Proposal any of their own standard contractual terms or provisions the County will be asked to consider if Offeror is selected for award. This may include, but is not limited to, such things as a sample Master Services Agreement or End User License Agreement and any additional governing documents referenced within those sample standard agreements. Offerors should note if their own standard contractual terms or provisions conflict with those provisions provided in Exhibit “M.”

SAMPLE SERVICES AGREEMENT

RFP NO: 24-56

RFP Name: CMRJ - INTEGRATED PUBLIC SAFETY SYSTEM

AGRXX-XX



INCORPORATED COUNTY OF LOS ALAMOS SERVICES AGREEMENT

This **SERVICES AGREEMENT** (“Agreement”) is entered into by and between the **Incorporated County of Los Alamos**, an incorporated county of the State of New Mexico (“County”), and _____, a _____ corporation (“Contractor”), to be effective for all purposes _____, 202X (“Effective Date”).

WHEREAS, [FOP RFP’S] -- the County Purchasing Officer determined in writing that the use of competitive sealed bidding was either not practical or not advantageous to County for procurement of the Services and County issued Request for Proposals No. 2X-XX (“RFP”) on _____, requesting proposals for _____, as described in the RFP; and

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

[FOR RFP'S ONLY] -- WHEREAS, Contractor timely responded to the RFP by submitting a response dated _____ (“Contractor’s Response”); and

WHEREAS, based on the evaluation factors set out in the RFP, Contractor was the successful Offeror for the services listed in the RFP; and

WHEREAS, the County Council approved this Agreement at a public meeting held on _____; and

WHEREAS, Contractor shall provide the Services, as described below, to County.

NOW, THEREFORE, for and in consideration of the premises and the covenants contained herein, County and Contractor agree as follows:

SECTION A. SERVICES:

SECTION B. TERM:

The term of this Agreement shall commence _____ and shall continue through _____, unless sooner terminated, as provided herein. At County’s sole option, the County Manager may renew this Agreement for up to _____ (____) consecutive one-year period(s), unless sooner terminated, as provided therein.

SECTION C. COMPENSATION:

1. **Amount of Compensation.** County shall pay compensation for performance of the Services in an amount not to exceed _____ (\$ _____), which amount does not include applicable New Mexico gross receipts taxes (“NMGRT”). Compensation shall be paid in accordance with the rate schedule set out in Exhibit “A,” attached hereto and made a part hereof for all purposes.
2. **Monthly Invoices.** Contractor shall submit itemized [*monthly or per the completion of the Project Phase/Task*] invoices to County’s Project Manager showing amount of compensation due, amount of any NMGRT, and total amount payable. Payment of undisputed amounts shall be due and payable thirty (30) days after County’s receipt of the invoice.

SECTION D. TAXES:

Contractor shall be solely responsible for timely and correctly billing, collecting and remitting all NMGRT levied on the amounts payable under this Agreement.

SECTION E. STATUS OF CONTRACTOR, STAFF, AND PERSONNEL:

This Agreement calls for the performance of services by Contractor as an independent contractor. Contractor is not an agent or employee of County and shall not be considered an employee of County for any purpose. Contractor, its agents, or employees shall make no representation that they are County employees, nor shall they create the appearance of being employees by using a job or position title on a name plate, business cards, or in any other manner, bearing County's name or logo. Neither Contractor nor any employee of Contractor shall be entitled to any benefits or compensation other than the compensation specified herein. Contractor shall have no authority to bind County to any agreement, contract, duty, or obligation. Contractor shall make no representations that are intended to, or create the appearance of, binding County to any agreement, contract, duty, or obligation. Contractor shall have full power to continue any outside employment or business, to employ and discharge its employees or associates as it deems appropriate without interference from County; provided, however, that Contractor shall at all times during the term of this Agreement maintain the ability to perform the obligations in a professional, timely, and reliable manner.

SECTION F. STANDARD OF PERFORMANCE:

Contractor agrees and represents that it has and shall maintain the personnel, experience, and knowledge necessary to qualify it for the particular duties to be performed under this Agreement. Contractor shall perform the Services described herein in accordance with a standard that meets the industry standard of care for performance of the Services.

SECTION G. DELIVERABLES AND USE OF DOCUMENTS:

All deliverables required under this Agreement, including material, products, reports, policies, procedures, software improvements, databases, and any other products and processes, whether in written or electronic form, shall remain the exclusive property of and shall inure to the benefit of County as works for hire; Contractor shall not use, sell, disclose, or obtain any other compensation for such works for hire. In addition, Contractor may not, with regard to all work, work product, deliverables, or works for hire required by this Agreement, apply for, in its name or otherwise, any copyright, patent, or other property right, and acknowledges that any such property right created or developed remains the exclusive right of County. Contractor shall not use deliverables in any manner for any other purpose without the express written consent of County.

SECTION H. EMPLOYEES AND SUB-CONTRACTORS:

Contractor shall be solely responsible for payment of wages, salary, or benefits to any and all employees or contractors retained by Contractor in the performance of the Services. Contractor agrees to indemnify, defend, and hold harmless County for any and all claims that may arise from Contractor's relationship to its employees and subcontractors.

SECTION I. INSURANCE:

Contractor shall obtain and maintain insurance of the types and in the amounts set out below throughout the term of this Agreement with an insurer acceptable to County. Contractor shall assure that all subcontractors maintain like insurance. Compliance with the terms and conditions of this Section is a condition precedent to County's obligation to pay compensation for the Services, and Contractor shall not provide any Services under this Agreement unless and until Contractor has met the requirements of this Section. County requires Certificates of Insurance, or other evidence acceptable to County, stating that Contractor has met its obligation to obtain and maintain insurance and to assure that subcontractors maintain like insurance. Should any of the policies described below be cancelled before the expiration date thereof, notice shall be delivered in accordance with the policy provisions. General Liability Insurance and Automobile Liability Insurance shall name County as an additional insured, and endorsed for waiver of recovery in favor of County.

1. **General Liability Insurance:** ONE MILLION DOLLARS (\$1,000,000.00) per occurrence; ONE MILLION DOLLARS (\$1,000,000.00) aggregate.
2. **Workers' Compensation:** In an amount as may be required by law. County may immediately terminate this Agreement if Contractor fails to comply with the Worker's Compensation Act and applicable rules when required to do so.
3. **Automobile Liability Insurance for Contractor and its Employees:** ONE MILLION DOLLARS (\$1,000,000.00) combined single limit per occurrence; ONE MILLION DOLLARS (\$1,000,000.00) aggregate on any owned, and/or non-owned motor vehicles used in performing Services under this Agreement.
4. **Cyber Insurance:** In addition to insurance required under the Agreement, Contractor shall, at its sole cost and expense, procure and maintain through the term of the Agreement and for two (2) years following the termination or expiration of the Agreement, cyber/network privacy insurance with limits of TWO MILLION DOLLARS (\$2,000,000) per claim/in aggregate. Such policy shall provide coverage for disclosures and/or breaches of County Data arising out of or relating to Contractor's Services. Such policy shall also include coverage for the costs associated with restoring lost or damaged County Data, sending breach notifications to affected individuals, public relations expenses, fines, and penalties. Such policy shall not contain exclusions for the acts or omissions of either Contractor, County, or their respective employees, agents, subcontractors, or volunteers, whether intentional or unintentional, resulting in or relating to any use of County Data not expressly permitted by this Agreement. Contractor must notify County at least thirty (30) days prior to the cancellation or modification of such policy. The policy shall provide coverage for the following:
 - 1) Third Party media
 - 2) Third Party Privacy and Cyber Security
 - 3) Third Party Privacy, Regulatory Defense, Awards and Fines
 - 4) Data Recovery
 - 5) Cyber Extortion and Ransomware

SECTION J. RECORDS:

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

Contractor shall maintain, throughout the term of this Agreement and for a period of six (6) years thereafter, records that indicate the date, time, and nature of the services rendered. Contractor shall make available, for inspection by County, all records, books of account, memoranda, and other documents pertaining to County at any reasonable time upon request.

SECTION K. DUTY TO ABIDE:

Contractor shall abide by all applicable federal, state, and local laws, regulations, and policies and shall perform the Services in accordance with all applicable laws, regulations, and policies during the term of this Agreement.

SECTION L. NON-DISCRIMINATION:

During the term of this Agreement, Contractor shall not discriminate against any employee or applicant for an employment position to be used in the performance of the obligations of Contractor under this Agreement, with regard to race, color, religion, sex, age, ethnicity, national origin, sexual orientation or gender identity, disability, or veteran status.

SECTION M. CHOICE OF LAW:

The interpretation and enforcement of this Agreement shall be governed by and construed in accordance with the laws of the State of New Mexico.

SECTION N: VENUE, FORUM NON-CONVENIENS, EXCLUSIVE STATE JURISDICTION:

County and Contractor knowingly, voluntarily, intentionally, and irrevocably agree that any and all legal proceedings related to this Agreement, or to any rights or any relationship between the parties arising therefrom, shall be solely and exclusively initiated, filed, tried, and maintained in the First Judicial Circuit of the State of New Mexico. County and Contractor each expressly and irrevocably waive any right otherwise provided by any applicable law to remove the matter to any other state or federal venue, consents to the jurisdiction of the First Judicial Circuit of the State of New Mexico in any such legal proceeding, waives any objection it may have to the laying of the jurisdiction of any such legal proceeding. County and Contractor also agree that this term is a material inducement for each to enter this Agreement, and that both County and Contractor warrant and represent that each have had the opportunity to review this term with legal counsel.

SECTION O: WAIVER OF JURY TRIAL:

In the event of any action or proceeding, (including without limitation, any claim, counterclaim, cross-claim or third party claim) arising out of or, relating to this Agreement, or the transaction

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

contemplated by this Agreement, County and Contractor KNOWINGLY, VOLUNTARILY, INTENTIONALLY, AND IRREVOCABLY WAIVE ANY RIGHT TO A JURY TRIAL, and agree that a court shall determine and adjudicate all issues of law and fact with a jury trial being expressly waived. County and Contractor also agree that this waiver of a jury trial was a material inducement for each to enter this Agreement, and that both County and Contractor warrant and represent that each have had the opportunity to review this jury waiver with legal counsel.

SECTION P. INDEMNITY:

Contractor shall indemnify, defend, and hold harmless County, its Council members, employees, agents, and representatives, from and against all liability, claims, demands, actions (legal or equitable), damages, losses, costs, or expenses, including attorney fees, of any kind or nature, to the extent that the liability, claims, demands, actions, damages, losses, costs, and expenses are caused by, or arise out of, the acts or omissions of the Contractor or Contractor's officers, employees, agents representatives, and subcontractors in the performance or breach of the Services under this Agreement.

SECTION Q. FORCE MAJEURE:

Neither County nor Contractor shall be liable for any delay in the performance of this Agreement, nor for any other breach, nor for any loss or damage arising from uncontrollable forces such as fire, theft, storm, war, or any other force majeure that could not have been reasonably avoided by exercise of due diligence.

SECTION R. NON-ASSIGNMENT:

Contractor shall not assign this Agreement or any privileges or obligations herein, and shall not novate this Agreement to another without the prior written consent of the [County Manager/County Utilities Manager].

SECTION S. LICENSES:

Contractor shall maintain all required licenses including, without limitation, all necessary professional and business licenses, throughout the term of this Agreement. Contractor shall require and shall assure that all of Contractor's employees and subcontractors maintain all required licenses including, without limitation, all necessary professional and business licenses.

SECTION T. PROHIBITED INTERESTS:

Contractor agrees that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services hereunder. Contractor further agrees that it shall not employ any person having such an interest to perform services under this Agreement. No County Council member or other elected official

of County, or manager or employee of County shall solicit, demand, accept, or agree to accept, a gratuity or offer of employment contrary to Section 31-282 of the Los Alamos County Code.

SECTION U. TERMINATION:

1. **Generally.** The [County Manager/County Utilities Manager] may terminate this Agreement with or without cause upon ten (10) days prior written notice to Contractor. Upon such termination, Contractor shall be paid for Services actually completed to the satisfaction of County at the rate set out in Section C. Contractor shall render a final report of the Services performed to the date of termination, and shall turn over to County originals of all materials prepared pursuant to this Agreement.
2. **Funding.** This Agreement shall terminate without further action by County on the first day of any County fiscal year for which funds to pay compensation hereunder are not appropriated by County Council. County shall make reasonable efforts to give Contractor at least ninety (90) days advance notice that funds have not been and are not expected to be appropriated for that purpose.

SECTION V. NOTICE: Any notices required under this Agreement shall be made in writing, postage prepaid to the following addresses, and shall be deemed given upon hand delivery, verified delivery by telecopy (followed by copy sent by United States Mail), or three (3) days after deposit in the United States Mail:

County:	Contractor:
Project Manager	
Incorporated County of Los Alamos	
Address	
Los Alamos, New Mexico 87544	

With a copy to:
County Attorney's Office
1000 Central Avenue, Suite 350
Los Alamos, New Mexico 87544

SECTION W. INVALIDITY OF PRIOR AGREEMENTS:

This Agreement supersedes all prior contracts or agreements, either oral or written, that may exist between the parties with reference to the services described herein and expresses the entire agreement and understanding between the parties with reference to said services. It cannot be modified or changed by any oral promise made by any person, officer, or employee, nor shall any written modification of it be binding on County until approved in writing by both authorized representatives of County and Contractor. In the event of any conflict between the terms, conditions, and provisions of this Agreement, and the terms, conditions and provisions of any

exhibits or attachments, the terms, conditions and provisions of this Agreement shall control and take precedence.

SECTION X. NO IMPLIED WAIVERS:

The failure of County to enforce any provision of this Agreement is not a waiver by County of the provisions, or of the right thereafter, to enforce any provision(s).

SECTION Y. SEVERABILITY:

If any provision of this Agreement is held to be unenforceable for any reason: (i) such provision shall be reformed only to the extent necessary to make the intent of the language and purpose of the Agreement enforceable; and (ii) all other provisions of this Agreement shall remain in effect so long as the substantive purpose of the Agreement is possible.

SECTION Z. CAMPAIGN CONTRIBUTION DISCLOSURE FORM:

A Campaign Contribution Disclosure Form is attached as [Exhibit I](#). Contractor must submit this form with this Agreement, if applicable.

OR

SECTION Z. CAMPAIGN CONTRIBUTION DISCLOSURE FORM:

A Campaign Contribution Disclosure Form was submitted as part of the Contractor's Response and is incorporated herein by reference for all purposes.

SECTION AA. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES:

Pursuant to NMSA 1978 § 14-16-7, this Agreement may be signed by electronic signature.

SECTION AB. DUPLICATE ORIGINAL DOCUMENTS:

This document may be executed in two (2) counterparts, each of which shall be deemed an original.

SECTION AC. CONFIDENTIAL INFORMATION:

Any confidential information of one party that is provided to the other party during the term of this Agreement shall be kept confidential and shall not be made available to any individual or organization in accordance with the Confidential Information Disclosure Statement in Exhibit "C." The Confidential Information Disclosure Statement shall be completed by Contractor as a

condition precedent and submitted as part of this Agreement. Its terms shall govern as if fully set forth herein.

SECTION AD. NEGOTIATED TERMS:

This Agreement reflects negotiated terms between the parties, and each party has participated in the preparation of this Agreement with the opportunity to be represented by counsel, such that neither party shall be considered to be the drafter of this Agreement or any of its provisions for the purpose of any statute, case law, or rule of interpretation or construction that would or might cause any provision to be construed against the drafter of this Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement on the date(s) set forth opposite the signatures of their authorized representatives to be effective for all purposes on the date first written above.

ATTEST

INCORPORATED COUNTY OF LOS ALAMOS

NAOMI D. MAESTAS
COUNTY CLERK

BY: _____
STEVEN LYNNE **DATE**
COUNTY MANAGER

APPROVED AS TO FORM:

J. ALVIN LEAPHART
COUNTY ATTORNEY

_____, A _____ CORPORATION

Exhibit N – LInX Interface Questionnaire



LInX Member Agency Questions for RMS / CAD Vendors

Background: Currently, all Law Enforcement Information Exchange (LInX) regional systems have the ability to ingest data submitted conforming to the NEIM standard, specifically GJXDM (Global Justice Extensible Markup Language Data Model). Further information on GJXDM can be found at the following DOJ website: <http://it.ojp.gov/jxdm/>.

Purpose of this document: Law Enforcement Agencies (LEAs) routinely participate in a variety of information sharing initiatives. To support these initiatives, it is critical for LEAs to have the capability to export data from existing information systems in an industry standard, NIEM compliant data format. Below are a number of questions that we recommend our LInX member agencies ask vendors when considering a new Law Enforcement Records Management and/or Computer Aided Dispatch System.

1. Does your product (Records Management System or Computer Aided Dispatch System) include a Global Justice XML Data Export Module? Yes No
2. If your company does not have an existing product/module, are there plans to develop an export module and what is your implementation timeline?
 Yes No Timeline _____
3. Does the product provide the capability to export all law enforcement data from your RMS and/or CAD including
 - Calls for Service - Law Enforcement Only
 - Incident Reports
 - Accident Reports
 - Warrants
 - Arrest Records
 - Booking Records
 - Field interviews / Contacts
 - Pawn Shop Records
 - Citations
 - Traffic Stops
 - Sexual Offender Registry
 - Other _____
 - Mugshots and photos with any associated record types
 - Narratives and supplemental narratives
4. Does your export module allow the agency to control what data can be exported and when?
5. Does this ability to control what data can be exported, include the ability to restrict the export of "sensitive" records?
6. Is there extra cost to obtain this export module?
7. Is there an ongoing annual maintenance cost for this export module?
8. Is your product/module currently being used by an agency that is a participating member of LInX?
9. Can your company provide an agency point of contact or agency references for Law Enforcement agencies that are currently using this export capability?



CAD / RMS Vendors

****IMPORTANT INFO REGARDING INTERFACING WITH LInX****

Keep in mind when responding to RFPs / RFIs / Contracts that there is work that will need to be completed on the LInX Integrator side and included in your pricing to your customer.

When each of the LInX agencies initially signed an MOU and approved their data to go into LInX the one time data conversion costs were covered by either grant funds from the LInX Region and/or funds through the Naval Criminal Investigative Service (NCIS). It is the responsibility of the agency to ensure any changes to their systems or replacements of their systems include costs to ensure the integration of their data into LInX. It cannot be assumed that these costs are automatically covered for your customer.

The work to bring in data from an agency's RMS and/or CAD system includes:

- Data Mapping
 - Testing
 - Agency Acceptance
 - LInX Region Acceptance
 - Final Connection with LInX for daily updates
1. The LInX Integrator costs depend on the complexity of the RMS or CAD system, the level of customizations an agency makes to the base product, the amount of data to be ingested into LInX, and whether or not the data extract is utilizing an industry standard format for LInX data ingestion. The LInX Integrator costs can be anywhere from \$8,000 to \$40,000 depending on these variables.
 2. Keep in mind that each agency's implementation of the same version of the RMS or CAD system purchased can be different thus adding additional work to the above.
 3. If your company has completed or are working on the capability to export data from your CAD or RMS system an industry standard, NIEM compliant data format it still needs to be tested and certified to be ingested into LInX. This is the ideal way to ingest data into LInX as overall it will save on costs to the customers including integrator costs. Further information can be found at the following DOJ website: <http://it.ojp.gov/jxdm/>.
 4. All LInX Regions are or will be connected to N-DEx and thus the agency's feeding into LInX will be able to also go straight into N-DEx without any additional work or additional costs.
 5. If you have any additional questions regarding agency sharing with LInX, please refer to the LInX Quick Reference to Data Sharing document. To obtain a copy of this please contact:

Mark Harris	Office: (703) 556-1318
LInX Program Manager	Cellular: (571) 235-9675
Northrop Grumman Corporation	mark2.harris@ngc.com



Exhibit O – CJIS Security Addendum

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

06/01/2020
CJISD-ITS-DOC-08140-5.9

H-2

RFP No. 24-56
Issued by Procurement Division: [D. Rodgers](#)

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

- 4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.
- 4.02 Security violations can justify termination of the appended agreement.
- 4.03 Upon notification, the FBI reserves the right to:
- a. Investigate or decline to investigate any report of unauthorized use;
 - b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.
- 5.00 Audit
- 5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.
- 6.00 Scope and Authority
- 6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
- 6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
- 6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- 6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.
- 6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

Exhibit P – Sample Reports

See *LA Forms.zip* file, and advise if each report is a “standard” (available) report, or if it would require a custom report. If a custom report is required for any of the associated reports, please include a price for each one on the Cost Sheet and as a narrative response as Appendix P in vendor proposal document(s).

Exhibit Q – Addenda Questions from RFP 23-62

Addendum 2:

1. Will the County accept a partial response to the RFP for only the JMS portion?
Response: A proposal for services for just one component would be considered non-responsive.
2. During the Pre-Proposal Conference the County mentioned that a single solution provider is desired, would a solution consisting of multiple providers with technical support coming from each of the providers be considered?
Response: The County intends to contract with a single Contractor. As stated in the needs statement, the County invites proposals from qualified firms that possess the qualifications, experience, and knowledge to provide a fully integrated Computer Aided Dispatch (CAD) system, Mobile Data System (MDS), Law Enforcement Records Management System (LERMS), Jail Management System (JMS) and associated interfaces including Fire Records Management System (FRMS) and electronic Patient Care Reporting (ePCR).

Addendum 3:

3. Is Animal Control required or optional? It is in both the required section and in the optional section on the cost form.
Response: Animal Control is a sworn division of the Police Department, and functionality to support complete reporting duties up through prosecution is required. A separate animal control module is optional.
4. How many CAD dispatchers need to be trained?
Response: Sixteen (16).
5. How many civil clerks do civil processing?
Response: Four (4).
6. How many field deputies do civil processing?
Response: All field officers may be tasked with service of civil process, with a current total of thirty-five (35) field officers.
7. How many sworn officers does the County have?
Response: Forty-three (43) including Animal Control.
8. How many career firefighters does the County have?
Response: One hundred forty (140).

9. For interface item IGen-26, “The system interfaces to a radio console to provide transmitter steering (e.g., Harris Symphony, Motorola MCC7500, Zetron),” is this a CAD requirement or a radio system management requirement? Please provide more detail.
Response: This item is related to CAD initiated radio-based paging, and assumes that the capability would be necessary for any CAD-initiated paging application function that provides comprehensive paging capabilities that the County may be required to leverage.

Addendum 4:

10. Will the ECC please provide clarification on the following: a. The RFP lists 16 Personnel - please provide a breakdown of full-time dispatchers, part time dispatchers, and supervisors)
RESPONSE: All positions cover shifts. At this time, we only have full time employees. Position breakdown as follows: Emergency Communications Manager, Deputy Emergency Comm. Manager, four (4) Emergency Communication Shift Supervisors, and ten (10) Emergency Communications Specialists 1 and
11. The RFP lists 9 CAD workstations - how many of these are full-time positions (i.e., 24/7/365 staffing)?
RESPONSE: All CAD workstations should be running 24/7/365 and waiting for someone to log in.
12. Additionally, how many CAD workstations are at the primary location and how many are at the secondary location?
RESPONSE: Six (6) stations are at the primary location, with three (3) stations at the secondary location.
13. On page 21 of the RFP it's indicated that 15 devices need access to full CAD. Are these in addition to the 9 seats listed previously in the RFP, or does that 15 devices include the 9 seats?
RESPONSE: This would include the nine (9) seats previously listed.
14. Please confirm the ECC needs 2 mobile CAD/Mapping licenses for mobile command units.
RESPONSE: CAD Administrators use mobile CAD/mapping licenses to test and train MDTs/MDCs.
15. Will the Los Alamos Fire Department please provide how many apparatus will require mobile capabilities?
Response: 70, please see Section 2.3.4, page 14 in the RFP.
16. Does the Los Alamos County Sheriff plan to be included in this response? If so, please answer the following:

RESPONSE: No. All law enforcement functions are performed by the Police Department as Los Alamos is a county and city consolidated.

17. Will the County please provide total numbers for each of the following: a. Number of CAD users

RESPONSE: 16 full CAD users, please see 2.3.1 Los Alamos County Emergency Communications Center, page 12.

18. Number of CAD seats i. Number of CAD dispatcher/call-taker seats

RESPONSE: Six (6). Supervisors are working supervisors and fill both duties. Please see 2.3.2 Los Alamos Police Department, page 13; 2.3.4 Los Alamos County Fire Department, page 14 in the RFP.

19. Number of CAD backup/supervisory seats

RESPONSE: Three (3).

20. Number of mobile units

RESPONSE: 70 LAFD, 35 LAPD and two ECC. Total of 102,

21. Number of sworn officers/users

RESPONSE: 43 sworn officers.

22. Number of jail beds and/or jail bed equivalents

RESPONSE: 32, please see 2.3.3 Los Alamos County Detention Center, page 14 in the RFP.

23. Regarding data conversion, what type of information does the County desire to have converted:

RESPONSE: See section 3.9 Legacy Data Conversions, pages 31-32 in the RFP.

24. CAD records (i.e., calls for service, unit dispatch history)

RESPONSE: Please see page 32 of the RFP. Calls for service to include transfer or informational only calls for service in entirety with nature, comments, unit times, person/vehicle/license, system notes, ProQA information, etc.; unit history; location history; location maps/notes/contacts/etc.; vehicle files; person files; license files; report files; SOP files; tow files; etc.

25. RMS records (i.e., incident/case reports, property/evidence, warrants, citations)

RESPONSE: See section 3.9 Legacy Data Conversions, pages 31-32 in the RFP.

26. JMS records (i.e., jail bookings)

RESPONSE: See section 3.9 Legacy Data Conversions, pages 31-32 in the RFP.

27. Civil records (i.e., garnishments, seizures, subpoenas)

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

RESPONSE: See section 3.9 Legacy Data Conversions, pages 31-32 in the RFP.

28. Administration records (i.e., equipment, inventory, fleet management, K9)

RESPONSE: N/A at this time.

29. Personnel records (i.e., training, certifications, commendations)

RESPONSE: N/A at this time.

30. Document Management System (DMS)

RESPONSE: N/A at this time outside of attachments to CAD, RMS, JMS.

31. Will the agency please provide the following information about their existing solutions (CAD, Mobile, RMS, and JMS) for data conversion: a. Name of the vendor

RESPONSE: Infor for CAD, Executive Information Services (EIS) for RMS and JMS. Please see 2.3 Agency Background, pages 12, 13, and 14 in the RFP.

32. Type of Database Management System (DBMS)

RESPONSE: MS SQL Server (currently on v2014; to be migrated to v2022 soon)

33. Size of attachments/data to be converted

RESPONSE: Databases are: ~60gb for CAD/Mobile and ~67gb for RMS/JMS

Addendum #5:

34. Com-205 since it doesn't have a drop down available are we supposed to manually enter our response?

RESPONSE: Yes, please write the response in the "Comments" field of COM-205.

35. Also, the excel sheet cuts off the description of capability on some of the tabs for instance CAD-75.

RESPONSE: This can occur when they are not viewed in fullscreen mode. The functional specification worksheets are best viewed in fullscreen mode. If upon doing this there is still a problem, please respond with which specific specifications you are unable to fully view.

36. Tab CAD - CAD-684 please elaborate on the special features indicator question. We need to know what you refer to as special features for a unit.

RESPONSE: CAD-684 - "Special Features Indicator" refers to additional features/abilities of a unit beyond its "type," e.g., AED in unit, K9, Spanish Speaking, etc.

37. Can the Excel functional spreadsheets, be submitted as Excel documents rather than PDF Documents?

RESPONSE: Yes, please submit the Excel functional spreadsheets as Excel documents.

Exhibit R – E-Signature Policy



INCORPORATED COUNTY OF LOS ALAMOS ADMINISTRATIVE PROCEDURE GUIDELINE

Index No. 1220

Effective: October 1, 2013

E-SIGNATURE POLICY

I. Purpose

This policy is to allow for e-signature use at LAC by means of methods that are practical, secure, and balance risk and cost. It is not the intent of this policy to eliminate all risk but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of e-signature, and that the level of user authentication used is reasonable for the type of transaction conducted.

A. Electronic Signatures Acts

Both federal and state law address electronic signatures and give electronic contracts the same weight as those executed on paper. The federal act is known as the "Electronic Signatures in Global and National Commerce Act," (Act) and is found at 15 U.S.C. Sections 7001-7006, 7021 & 7031. The New Mexico act is known as the "Uniform Electronic Transactions Act," and is found at Sections 14-16-1 through 14-16-19, N.M.S.A. (1978). Links to these statutes are provided below. All references herein are to the New Mexico act unless otherwise specified. The act has some specific exemptions or preemptions. *Although the act enables documents to be signed electronically, the ability to do so arises only when both parties agree to conduct transactions by electronic means. Any LAC department using E-signatures shall also provide methods for conducting transactions with its customers that do not require E-signatures in the event the customer declines to agree to such to conduct transactions by electronic means.* The act specifically avoids stipulating any 'approved' form of electronic signature, instead leaving the method open to interpretation by the marketplace. Any number of methods is acceptable under the act. Methods include simply pressing an / Accept button, digital certificates, smart cards and biometrics.

E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Examples of transaction risks include: fraud, repudiation, authentication, hacking, security and financial loss. The quality and security of the e-signature method shall be commensurate with the risk and needed assurance of the authenticity of the signer. *Authentication is a*

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

119

Version: 04212022

way to ensure that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign".

II. Policy

- A. It is the policy of LAC that every user shall have unique identifying credentials. Authentication entails verifying the user's unique credentials, such as username and password, or a digital certificate.
- B. Under this policy LAC departments may implement use of e-signatures, but shall also maintain alternative processes available for any consumer who declines to conduct transactions by electronic means. The LAC department is the organization conducting business by means of an e-signature. Implemented e-signatures will be reviewed periodically for appropriateness, and continued applicability.
- C. An e-signature may be accepted in all situations if requirement of a signature/approval is stated or implied. This policy does not supersede situations where laws specifically require a written signature or where a party declines to conduct transactions by electronic means.

III. Responsibility

- A. Security and access to LAC specific information is determined by the Access Control Authority (ACA) for the electronic system. ACA's shall have the ability to develop enabling procedures and are responsible for compliance with all legal obligations related to information, as well as determining the utilization, access, and release of data under their jurisdiction. ACA's are a representative from the requesting department or other designated representative (i.e., IT liaison, TAG representative). In some instances there are multiple ACA's for various systems. The ACA will ensure that appropriate controls and monitoring of required software/hardware required for implementation are in place.
- B. LAC departments shall complete LAC risk assessment tool (E-Signature Authentication Request Process) and shall describe the reason for risk, identify the steps that will be taken to mitigate the risk and obtain the signed approval of the County Administrator. LAC departments shall conduct periodical reviews of every implementation, no less than every three years, which will include an evaluation of the e-signature use to determine whether any applicable legal, business, or data requirements have increased the risk of the e-signature implementation.
- C. The Information Management Division (IMD) shall assist LAC department ACA's in preparation of their application and provide technological expertise (i.e., IT liaison).
- D. III.4. The ACA may, after consultation with the County Attorney, reject any E-Signature application deemed in violation of or failing to meet statutory or regulatory requirements. The ACA, after consultation with the County Attorney, shall establish specifications for recording, documenting, and/or auditing the e-signature as required for non-repudiation and other legal requirements.
- E. The County Administrator shall review and have final approval of each e-signature application.

- F. Records Information Management (RIM) shall retain a formal record of the risk assessment evaluation, e-signature method selection, and justification.

IV. Procedure

The E-Signature Authentication Request Process tool outlines the process required by a department to apply for an e-signature implementation and shall address known identified risks.

- A. An evaluation will be performed by the ACA to identify risks associated with using an e-signature and to determine the quality and security of the e-signature method required. An evaluation will be made using the E-Signature Authorization Request Process tool. The reports resulting from the assessment shall be included as part of the official record for this e-signature implementation and submitted with the proposal.
- B. Requests for LAC e-signature transactions shall be evaluated by the ACA in conjunction with IMD, who will determine whether to recommend an e-signature method for approval, by understanding the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used. The IMD review will include process, security and records review with a recommendation to the department on whether or not to proceed.
- C. The ACA will request a review of the application from the County Attorney. Once that review has been completed and recommendation to proceed has been granted, the ACA will seek authorization to implement e-Signature from the County Administrator.
- D. The signed document shall be included as part of the official record for this e-signature implementation.
- E. Once approved, the implementation process will likely differ for each transaction and for each LAC department or affiliated body, as it is dependent on many factors such as records management requirements, technical environment, appropriate assurance level, and the nature of the transaction.
- F. Software and/or hardware required for e-signatures, such as Public Key Infrastructure (PKI) certificates, “fobs”, or “dongles”, or other credential devices shall be purchased by the department or affiliated body.
- G.

V. Resources and Links

- A. Electronic Signatures in Global and National Commerce Act (ESIGN):

[http://frwebgate.access.gpo.gov/cgi-](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)

[bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)

- B. NIST Electronic Authentication Guidelines: 800-63;

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

C. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Sections

7001-7006, 7021 & 7031; <http://uscode.house.gov/download/pls/15C96.txt>

D. Uniform Electronic Transactions Act, Sections 14-16-1 through 14-16-19,

N.M.S.A. (1978);

<http://www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0>

VI. Definitions

Access Control Authority (ACA)	Department representative, or designee, who understands the data and manages the request for e-signature application process and implementation.
Affiliated Body	Board or Commission who act on behalf of a LAC Department.
Authentication	A method to ensure that the user who attempts to perform functions in a system is in fact the user who is authorized to do so in order to ascertain the identity of the originator, verify the integrity of the electronic data and establish the link between the data and the originator.
Electronic Record	Computer-generated information such as an e-mail message, document or image file created or received by the County in pursuance of law or in connection with the transactions of public business.
Electronic Signature (E-Signature)	The electronic signing of a document consisting of establishing a verifiable link between the originator and the document using an electronic sound, symbol, or process attached to or logically associated with a record and execute or adopted by a person with the intent to sign the record.
Non-repudiation	Specific identification of a user plus the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction.
Record	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.
TAG (Technology Advisory Group)	This group provides technological oversight to LAC and any member thereof may act as an ACA.
Transaction	Specific actions that users can perform to achieve a desirable result. A transaction is an actor, plus an action, resulting in a desired outcome.


HARRY BURGESS
COUNTY ADMINISTRATOR

12/1/13
DATE

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

Exhibit S – Records And Information Management Governance Policy



Index No. 0310

Revision Date: November 28, 2017

RECORDS AND INFORMATION MANAGEMENT GOVERNANCE POLICY

I. Purpose

The purpose of this policy is to establish consistent record and information management governance practices for all County employees, contractor employees, governing and advisory boards and commissions, appointed and elected officials who create records in connection with the transactions of County business. The Incorporated County of Los Alamos is committed to an effective Records and Information Management (RIM) program that includes all legal/regulatory requirements for protection, confidentiality and security and will show due diligence and best efforts in the governance of electronic information and hardcopy records. The Incorporated County of Los Alamos (ICLA) recognizes the need for the optimization of space and cost of retaining public records in any medium that have met their required retention within its custody. This policy applies to all record formats, created and stored on paper, electronic (in all its variations), e-mail, social media and web based platforms or any other mediums where County records may reside.

II. Definitions

- A. **Active Record:** Record needed to perform current operations, subject to frequent use, and usually located near the user, also known as a current record.
- B. **Appraisal:** Records analysis; the process of evaluating records based on their current operational, regulatory, legal, fiscal and historical significance, their informational value, and their arrangement and relationship to other records.
- C. **Confidential Information:** Information that can be found in records that may pertain to personal identifiable information (PII) or that should be protected and private under the Inspection of Public Records Act (§14-2-1 NMSA 1978) or as otherwise provided by law or County policy.
- D. **Disposition:** Destruction of records; prior notice to State Records Administrator

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

123

Version: 04212022

(§ 14-1-8, NMSA 1978). An official charged with the custody of any records and who intends to destroy those records, shall give notice by registered or certified mail to the State Records Administrator, State Records Center, Santa Fe, New Mexico, of the date of the proposed destruction and the type and date of the records intended to destroy. The notice shall be sent at least sixty days before the date of the proposed destruction. If the State Records Administrator wishes to preserve any of the records, the official shall allow the State Records Administrator to have the documents by calling for them at the place of storage.

- E. **Electronic Record:** Data or information that has been captured and fixed for storage and manipulation in an automated system and that requires the use of the system to render it intelligible by a person. Computer-generated information such as an e-mail message, document or image file created or received by the County in pursuance of law or in connection with the transactions of public business.
- F. **E-mail:** Information transmitted electronically over a communication network. A system that enables people to compose, send, receive and manage electronic messages and images across networks.
- G. **Essential Information:** Records designated by management as essential to the operational functions outside its normal parameters to provide business continuity during an emergency response.
- H. **File Plan:** A hierarchical structure of folders within a filing structure that provides a coherent location in which records can be stored, searched or retrieved.
- I. **Generally Accepted Recordkeeping Principles:** Through the use thereof allow an organization to create, organize, secure, maintain and use records in a way that effectively supports the activity of that organization. These principles are as follows:
 - (1) **Principle of Accountability:** The County shall create a recordkeeping program and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel and ensure audit ability of the program.
 - (2) **Principle of Availability:** The County shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
 - (3) **Principle of Compliance:** The County shall construct a recordkeeping program that complies with applicable laws for maintaining records, as well as the organization's policies as they pertain to records and information management.
 - (4) **Principle of Disposition:** The County shall provide secure and appropriate disposition for records that are no longer required to be maintained under applicable laws.
 - (5) **Principle of Integrity:** The County shall construct a recordkeeping program where records and information generated or managed by or for the County has a reasonable and suitable guarantee of authenticity and reliability.

- (6) **Principle of Protection:** The County shall construct a recordkeeping program that ensures a reasonable level of protection to records and information that are private, confidential, privileged, or essential to business continuity.
 - (7) **Principle of Retention:** The County shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational and historical requirements.
 - (8) **Principle of Transparency:** The processes and activities of the County's recordkeeping program shall be structured and documented in a manner that is open and verifiable and is available to all personnel and interested parties.
- J. **Inactive Record:** A record no longer needed to conduct current business but preserved until it meets the end of its retention period.
- K. **Inspection of Public Records Act, §14-2-1 et seq., NMSA 1978:** The law that requires a representative government to provide access to its public records at the request from a person within a designated timeframe with few noted exceptions. It states that all persons are entitled to the greatest possible information regarding the affairs of government and the official acts of public officers and employees. This law can be found at <http://www.nmag.gov/office/Divisions/Civ/OMAIPRA/default.aspx>
- L. **Inventory:** A detailed database created by the records staff that lists all inactive records stored in a centralized records location for ease in maintenance and retrieval.
- M. **Lifecycle of Records:** Begins with the creation of the record, its use, storage in a format that is readable, its maintenance, retention and final disposition of all County records.
- N. **Metadata:** Data describing context, content, and structure of records and their management through time. RIM has selected the following metadata string to capture information in a consistent manner, these include: ICLA File Plan Designation, Record Series or Citation, New Mexico Administrative Code Record Function, Incorporated County of Los Alamos Record Description, Creation and End Dates, Trigger Date, Disposition Date, Record Value and Record Classification.
- O. **Migrated:** Method of preserving information to ensure continued access to information in any format. This includes the preservation of materials resulting from digital reformatting, but particularly information that is created digitally and has no analog counterpart.
- P. **Naming Structure:** Specific metadata used to describe the contents of the record and to establish consistency within a records management program which also provides ease in searching, retrieval and retention.
- Q. **NMAC:** New Mexico Administrative Code (1978) providing rules as well as referring to and interpreting statutes for governing public information.

- R. **Non-record Materials:** The following specific types of materials are defined as non-record and may be disposed of at the convenience of the County when they have no more value/use to the County: extra copies of correspondence and other documents preserved only for convenience of reference; blank forms, books, etc., which are outdated; materials neither made nor received in pursuance of statutory requirement nor in connection with the functional responsibility of the office/county; preliminary drafts of letters, reports, and memoranda which do not represent significant basic steps in preparation of record documents; shorthand notes, steno tapes, mechanical recordings which have been transcribed, except where noted on the County's retention schedule; routing and other interdepartmental forms which do not add any significant material to the activity concerned; stocks of publication already sent to archives and processed documents preserved for supply purposes only; form and guide letters, sample letters, form paragraphs. All other materials either related or received in pursuance of statutory requirements or in connection with the transaction of public business which belongs to the office concerned are government property and not personal property of the officer or employees concerned. Therefore, any material not included in the above definition cannot be destroyed, given or taken away, or sold without complying with all the statutory requirements specifically relating to said records.
- S. **Personal devices:** To include personally owned computers, flash drives, external hard drives, smartphones, other mobile/cellular phones, tablet computers, e-readers, portable media devices, PDAs, portable gaming devices, ultra-mobile personal computers (UMPCs), laptops/notebook computers and any other mobile device capable of storing data and connecting to a network.
- T. **Physical records:** To include calendars, appointment books, memos, correspondence, reports, studies, projects in a paper format as well as all other physical media, including optical media (magnetic media), microfilm, microfiche, which stores public information created in the course of conducting or related to County business.
- U. **Public Records:** Means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, made or received by any agency in pursuance of law or in connection with the transaction of public business and preserved, or appropriate for preservation, by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government or because of the informational and historical value of data contained therein. Library or museum material of the state library, state institutions and state museums, extra copies of documents preserved only for convenience of reference and stocks of publications and processed documents are not included (§14-3-2 NMSA 1978).
- V. **Records and Information Management (RIM) Program Manager:** The Incorporated County of Los Alamos employee, who will serve as the person responsible for this information governance policy and implementation. This employee is also authorized to transfer, withdraw or destroy County records with the approval from the New Mexico State Records Administrator.

- W. **Record Center:** A County storage facility where inactive records are managed, organized, appraised, inventoried, protected and tracked for retrieval, audit, retention and final disposition. A temperature and humidity controlled facility is preferred to secure, protect and maintain the County's legacy of information for as long as required.
- X. **Records and Information Management (RIM):** Field of management responsible for the efficient and systematic control of the creation, receipt, use, maintenance, and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in all record formats and mediums.
- Y. **Records Personnel:** Staff, trained and authorized by the County RIM Program Manager to handle County records under this established recordkeeping policy, procedures and principles including copies of those public records maintained by the County Clerk, not otherwise stored or managed pursuant to New Mexico State Statute or the County Charter/Code.
- Z. **Retention Schedule:** A comprehensive list of records series titles/functions, indicating for each series the minimum length of time it is to be maintained. Records may be kept longer with justification and nominal risk to the County.
- AA. **Social Media and Web Based Services and Platforms:** External and internal Web sites or services most of which integrate web technology, social interaction and user-generated content to collaborate, combine and share information. These provide a variety of ways for users to interact. These platforms may be operated by nongovernmental third part entities. Examples of social network services include but not limited to Facebook, Twitter and Linked In.
- BB. **Third-party repository:** The storage of data online in the cloud or on other social media sites wherein an organization's data is stored in and accessible from multiple distributed and connected resources. The ICLA is fully responsible for any and all records and information transferred and stored in an offsite repository.

III. Policy

It is the policy of the Incorporated County of Los Alamos that all Public Records will be responsibly managed in accordance with the Public Records Act (NMSA 1978, §14-3-1 et seq.), the Inspection of Public Records Act (IPRA) NMSA 1978, §14-2-1 et seq., the Incorporated County of Los Alamos Retention Schedule and recordkeeping standards and procedures, 1.21.2 New Mexico Administrative Code (NMAC) Retention and Disposition of Public Records, 1.21.3 NMAC Local Government Records Management Guidance and other applicable rules, statutes and regulations issued by the New Mexico Commission of Public Records, except as expressly referenced and modified herein. This includes 1.13.3 NMAC (Management of Electronic Records), 1.13.4 NMAC (Management of Electronic Messaging), 1.12.7

Information Technology (Electronic Authentication) as well as other Federal retention rules and schedules that pertain to specified record series created by specific divisions.

It is the policy of the Incorporated County of Los Alamos to provide employees, appointed and elected officials the applicable records management training to assist in the performance of their work. All resources and services shall be managed in a lawful manner by all County employees, appointed and elected offices, or contractors. County employees shall classify information (using the specified naming structure format) and retention schedule to ensure electronic repositories are in compliance with this policy and applicable law.

County employees shall have no expectation of privacy in anything they send or receive including electronic messaging in the course of conducting County business. All records created while employed, appointed or elected with the Incorporated County of Los Alamos are the property of the County and cannot be destroyed, distributed, sold or stored without complying with this policy.

IV. Responsibility

All affiliated County personnel are required to follow the approved Incorporated County of Los Alamos Retention Schedule by reference for all recordkeeping purposes and ensure the Generally Accepted Recordkeeping Principles, which include accountability, integrity, protection, compliance, availability and transparency apply to all County records while in their custody. The principles of retention and disposition shall be the responsibility of the County's RIM personnel to ensure haphazard or indiscriminate dumping is avoided.

All inactive physical records are required to be centrally located and managed by the RIM personnel to ensure records can be easily located and securely managed. All physical records transferred to the County's Record Center shall include on the outside of each file the title and description of the record, the creation and end dates, and indication whether the record contains confidential or essential information. Active records will remain within Division offices for operational use for as long as needed. Once inactive, records shall be transferred by the Departmental Records Data Liaison to the County's Record Center for evaluation, appraisal, inventory, storage, maintenance and final disposition.

Electronic records will be managed in place by the record creator on user controlled storage, under this established record management criteria. To create consistency and uniformity, records shall use the following Naming Structure format: *yyyymmdd_Title of Record_creator's first initial and complete last name. Example: 20160923_Information Governance Policy_BRicci*. This will allow the creator to file the e-record within the County's centralized File Plan by year thus improving the ease for retrieval and final disposition. Electronic records include those records on network drives, cloud repositories, external hard drives, USB flash drives, digital assistants to

include mobile devices, and digital cameras. Active electronic records will remain the responsibility of the creator who shall maintain the official record under these established recordkeeping practices. The naming structure format does not pertain to input of content in an established database. When entering content in a database, end-user is not required to name the record but must comply with the standards established within the designated system. Only one copy needs to be maintained as the official record to satisfy the retention requirements of the Public Records Act. All duplicated files are considered reference material and shall be deleted as non-record including drafts in any form, which do not add significant material or value to the activity concerned.

The maintenance and accessibility of inactive electronic records shall be safeguarded by the Information Management (IM) Division against deliberate tampering, alteration or in any way change the content of the record for fraudulent purposes. The Incorporated County of Los Alamos RIM Program Manager shall work with IM to ensure electronic records are migrated when records have not met retention and where there is hardware or software obsolescence or when records are stored within a third party repository. Records shall be migrated to a new hardware or software or be converted to a human readable form. RIM and IM will determine appropriate time periods to insure that they are protected from accidental or deliberate loss. Permanent archival or long-term records in physical and on electronic media shall be maintained by RIM and stored in an appropriate environmental setting.

V. Procedures

- A. **Record/Data Liaison (RDL).** Each Department or affiliated body or group shall designate a County Record/Data Liaison (RDL) who understands the records created by the Department or group and who will be the point of contact for the County's RIM Program Manager and the County's Records Center. This responsibility shall become part of the Records/Data Liaison's job duties. All RDL's are required to attend County RIM Training Sessions given or sponsored by the County RIM Program Manager to include and implement all recordkeeping principles. The Records/Data Liaison shall actively support the Records and Information Management policies and procedures and will be the person(s) who reports on all record training and communication at department, affiliated body or group meetings. Any record concerns or issues shall be directed to the County's RIM Program Manager, RIM personnel, designee or subsequent chain of command.
- B. **Record Retention Rules, Schedules, File Plans and Data Entry Portal.** Each department's RDL will determine which records are inactive and shall prepare physical records to be transferred to the County Records Center by boxing the records in designated boxes and by entering each file's metadata into the Data Entry Portal inventory forms. The Data Entry Portal is accessible to all RDL's via the Incorporated County of Los Alamos Intranet. RIM personnel will evaluate, verify and quality check the data entered into the Data Entry Portal against the

actual records and will either accept or reject the box. At the end of each fiscal and calendar year, a Disposition Report will be generated by the RIM personnel on all inventoried records by division and distributed to each RDL. A 30-day review period will be allowed for notice and comment by Department management or affiliated body or group. If no issues, audits or holds pertain to the records listed, the County's RIM Program Manager will proceed with approval from State Records Administrator for final disposition. Once granted, all record formats will be destroyed and disposed of accordingly. Destruction of all records is performed on location in a confidential manner supervised by the RIM personnel with final Certificate of Destruction maintained on file.

- C. **Public Records Requests.** All public record requests shall be the responsibility of the Records Custodian designated by the County Manager. Together with the Records Center, all Record/Data Liaisons shall provide requested records within the designated timeframe under their custody as required by the Inspection of Public Records Act.
- D. **Storage.** All County inactive records shall be stored in the County's Records Center. Electronic records including email shall be responsibly managed on County computing platforms and County managed storage appliances in compliance with current policies. Individuals who choose to use their personal devices to conduct County business must follow the County's records and information management policies and procedures. The designated IM personnel must be informed by the individual using any personal device and will maintain a current listing of those individuals who use personal devices to conduct County business. County information stored may be subject to inspection and discovery under applicable public records laws, county policy and discovery mechanisms, respectively.

When an employee's employment ends with the County, all records created by the employee that are inactive shall be gathered by the designated Records/Data Liaison and transferred to County's Record Center for evaluation, inventory, storage and/or final disposition. Active records shall be distributed by the RDL to the new designee. RIM and IM policies and procedures pertain to all issued equipment that store the County's public records.


- E. **Social Media and Web-Based Platforms.** County employees utilizing social media in the course of County business shall follow the County's Social Media policy. Such employees shall be responsible for all public records created on third-party sites and shall maintain an archive of all information posted with all supporting documents attached in a readable format and in compliance with existing policies. Official records posted under this category must follow this policy and the accepted Incorporated County of Los Alamos Retention Schedule for the entire lifecycle of these public records.

- F. **Reporting.** The Records personnel will provide the County Manager and County Council with reports on the Records and Information Management program as requested.
- G. **Elected and Appointed Officials.** The Records personnel will support all elected or appointed offices of the County Council, Boards and Commissions, County Assessor, Clerk, Sheriff, Municipal and Probate Judges and Municipal Court to utilize the accepted Retention Schedule or a specific schedule that pertains solely to their office.

VI. Additional Regulatory Requirements

This policy shall not be construed in a manner that is inconsistent with statutory regulations and requirements within the Incorporated County of Los Alamos Charter.

Prepared by: RIM Program Manager



Harry Burgess
County Manager

11/30/17
Date

1210

Exhibit T – IT Usage and Security Policy

Information Technology Usage and Security Policy Los Alamos County

July 30, 2007

Approved

Los Alamos County Administrator

Max H. Baker

Date

7/30/07

RFP No. 24-56

Issued by Procurement Division: [D. Rodgers](#)

132

Version: 04212022

1.	<i>Introduction</i>	3
2.	<i>Policy Direction and Maintenance</i>	3
3.	<i>Principles</i>	3
4.	<i>Security Program Components</i>	3
5.	<i>Risk Identification</i>	4
6.	<i>DOE Requirements</i>	4
7.	<i>Physical Security</i>	4
8.	<i>Access Management</i>	5
9.	<i>Requesting Account Access</i>	6
10.	<i>Naming Conventions</i>	6
11.	<i>Password Creation</i>	6
12.	<i>Account Control</i>	6
13.	<i>Account Suspension and Termination</i>	7
14.	<i>Security Training</i>	7
15.	<i>Data Security</i>	8
16.	<i>Usage Policy Overview</i>	9
17.	<i>Usage Policy: Prohibited Use</i>	10
18.	<i>Usage Policy: Personal Use of County IT Assets</i>	12
19.	<i>Remote Computing</i>	12
20.	<i>Enforcement and Sanctions</i>	13
21.	<i>Technology Components of Security</i>	14
22.	<i>Backup and Recovery</i>	15
23.	<i>Definitions</i>	15
	<i>Appendix A: Acknowledgement Form</i>	17
	<i>Appendix B: Master Computer Protection Plan</i>	18
	<i>Appendix C: ITD Supported Applications</i>	22

1. Introduction

This policy provides guidance to users of Los Alamos County (the County) information technology (IT) assets on proper use and protection of computing and communications resources, including: the Internet; email; the Integrated County Network (ICN); phones; data; desktop computers; personal devices (e.g. PDA's); servers; and applications.

These assets provide critical support for service delivery to County residents and visitors.

2. Policy Direction and Maintenance

The County must take prudent and reasonable measures to secure its systems and data to (1) meet legal and regulatory obligations and (2) for effective County operation. The Information Technology Division (ITD) prepares this policy based on direction from the IT Management Oversight Committee and approval by the County Administrator. It applies to all users of County IT assets.

ITD will update this policy at least yearly. Copies are available in every department and maintained on the County's web site. Questions about this policy should be referred to the Information Technology Division.

3. Principles

This policy and accompanying programs are based on several principles:

- 3.1. Compliance with DOE requirements (see below);
- 3.2. An optimum balance of security and productivity;
- 3.3. Providing defense in depth for known threats with flexibility to respond quickly to unknown or unexpected threats;
- 3.4. Being risk based - correlate security investments with risk;
- 3.5. Identifying roles and responsibilities for personnel, supervisors, and IT personnel;
- 3.6. Providing engineered solutions where possible to minimize the impact of risky human behaviors; and
- 3.7. Incorporating a process of incremental security improvement.

4. Security Program Components

The County's computing and communications security programs consist of administrative and technical components. Administrative components include the following:

- 4.1. Incident reporting and response;
- 4.2. Well-defined and documented usage policy;
- 4.3. Regular policy update and publication;
- 4.4. Training of personnel and supervisors; and
- 4.5. Account management and control.

The technology components include the following:

- 4.6. Physical security;
- 4.7. Infrastructure design;
- 4.8. Perimeter network defense; and
- 4.9. Inside network defense.

5. Risk Identification

Risks to County IT assets fall into three major categories. Major risks and their potential impact are defined below

- 5.1. **First, service interruption and/or destruction of data by untargeted attacks, e.g.** email viruses, worms, denial of service attacks, etc. This is the most common and well-publicized threat that affects County IT operations. This can take down networks, servers, and desktops, can damage data, and compromise County operations.
- 5.2. **Second, misuse of legitimate access to County assets.** While illegal, this problem usually represents a minimal actual loss to the County with respect to IT resources. Examples are County employees running their own businesses on County equipment and misuse of phones, computers, and/or Internet access. However, asset misuse also may represent systematic, planned use of IT assets to divert material resources to personal advantage, e.g. embezzlement. In such cases, losses may be substantial.
- 5.3. **Third, a targeted attack by an individual using illegitimate access.** This is the classic "hacking" portrayed in movies and fiction. While comparatively rare, it can be devastating if successfully pursued by a skilled and malicious individual.

6. DOE Requirements

Due to the contracts Los Alamos County has with the U.S. Department of Energy (DOE), there are certain requirements imposed on the County and its employees. By virtue of these contracts, the County will impose these same requirements on all IT users regardless of whether or not they are County employees. These requirements pertain to ensuring that information is not disclosed to unauthorized viewers. DOE requires that all account holders be diligent in determining if data is sensitive and seeing that it is protected from unauthorized viewers. Fire Chief's Directive 100.15A also addresses this requirement. It is the account holder's responsibility to bring to their supervisor's attention questions about whether information needs to be protected from unauthorized access so that inadvertent disclosure does not occur. The specific DOE requirements are detailed in the *Master Computer Protection Plan* included in Appendix B.

7. Physical Security

The occupier of County owned or leased physical space has responsibility for the physical security of IT resources in their areas. The level of physical security should be proportionate to the possible impact on the County of systems compromise or loss. For example, the level of physical security for a generic personal computer used by someone without access to County financial or material resources is not expected to have the same level of physical security as a

computer commonly used by someone with wide access to County financial data and transactions. In general, this means acceptance of the following responsibilities.

7.1. Responsibilities for all users:

- 7.1.1. Locking rooms except during business hours;
- 7.1.2. Not leaving computers unattended and logged in without password protection for extended periods of time;
- 7.1.3. Challenging visitors and unfamiliar people if found using County computer resources;
- 7.1.4. Not physically keeping passwords in the vicinity of a computer (e.g. in a desk drawer, pasted under the keyboard, etc.);
- 7.1.5. Maintaining physical control over mobile computing and communications units (laptops, PDA's, phones) and notifying ITD immediately if a unit is lost or stolen.
- 7.1.6. Not connecting a computing device to the network or reconfiguring a computing device connected to the network without contacting ITD;
- 7.1.7. Prompt reporting of any compromise of computing or communications devices or of passwords; and
- 7.1.8. Releasing unneeded resources, including access authorizations.

7.2. Supervisors have these additional responsibilities:

- 7.2.1. Limiting the number of computers used for critical transactions, e.g. financial adjustments;
- 7.2.2. Physical control over their computing and/or communication environments;
- 7.2.3. Coordinating with ITD installation, removal, and reconfiguring of equipment with network and computing capabilities (e.g. copiers);
- 7.2.4. Understanding and supporting the administrative components of the computer security policy; and
- 7.2.5. Reporting personnel changes in their organizations to ITD.

7.3. The ITD has the following additional responsibilities:

- 7.3.1. Physical security of servers and the Integrated Computer Network (ICN)
- 7.3.2. Training of users in computer security;
- 7.3.3. Assisting other County personnel in addressing security issues; and
- 7.3.4. Policy review and update.

8. Access Management

Access management is a key component of perimeter defense. Stopping the illegitimate user is a primary defense against illegitimate use (Risk 3). Good access management also enables monitoring of users' computing and communications activities, thereby greatly reducing the risk of misuse (Risk 2).

Any County employee or contractor may be authorized to use a specified set of County IT assets. An account is established for use by only one person for whom access has been requested and granted. This person becomes the account "owner" and is responsible for all activity taking place through that account. Supervisors are responsible for specifying the scope of the access.

9. Requesting Account Access

All access requests must come from a person having a County supervisory role (hereafter designated a County supervisor or, simply, a supervisor) and state the applications and specific functions required for an employee, elected or appointed official, volunteer, or contractor. (A list of available applications is included in Appendix C.) Requests should be received by the ITD at least one week prior to the user's need for access. Requests for contractor or volunteer access must be for a specified time period less than twelve (12) months, at which time the access may be renewed if so requested. Accounts will be requested by the supervisor via email (call the ITD help desk for instructions) or paper form and include a signed copy of the *Account Holder and Computer User Responsibilities* form (Appendix A) authorizing the account. This form must be used for any new account authorization including new hires, job changes, or any other change requiring different system access. Requests for direct dial-in access to the network must also be made on this form.

10. Naming Conventions

There are currently two naming conventions for accounts. For Windows-based systems, accounts are named using the employee's last name and first initial and, if necessary, a sequential number or middle initial. For AIX or Linux systems, accounts are named using the employee's first initial, last initial and a sequential number.

11. Password Creation

Each account requires a password. Since the password is the only thing keeping others from accessing your account, it is important that it be something that no one else can guess easily. Users should follow these standards when creating a password.

- 11.1. The password should be at least 8 characters long and must not be a word commonly found in the dictionary.
- 11.2. A password should not be a name of a family member, pet, or anything else that is commonly associated with the account-holder.
- 11.3. The password should contain at least two of the following categories: letters; numbers; and special characters.
- 11.4. The password should not contain repeating groups, e.g. abcabc or runs, e.g. mnopqrs

12. Account Control

Once set, your password is the primary defense used to prevent unauthorized access to IT resources. The County has set the following standards for password control:

- 12.1. Set up all computers with password protection that automatically activates after a short time period of inactivity (five minutes is recommended) to prevent unauthorized use of the computer (call the help desk if you need assistance);

- 12.2. Do not share your password with anyone (except as noted below);
- 12.3. Do not allow any other person to use your account (i.e. password);
- 12.4. Your password must not be written anywhere where it can be easily found. For example, don't write your password on your keyboard, on a post-it note on your monitor, or on a note in your desk; and
- 12.5. The system will require you to change your password every 90 days. The new password you choose must not be one that you have used previously. If you suspect that your password has been compromised, call the help desk immediately.
- 12.6. The County follows current industry best practice for passwords. Users are required to choose and maintain strong passwords for access to County computer resources.

Maintaining account security is a serious matter. In addition to safeguarding County information the County must enforce strict computer security to be in compliance with its contract with DOE. Sharing of passwords or other conduct that compromise the security of County IT assets or the ability of the County to perform its functions may subject the account holder to disciplinary action as defined in this policy. Account holders may share their passwords with ITD personnel in order to facilitate repair or recovery of systems or data. All such password sharing should be considered non-standard operating practice. Account holders will change their password immediately once the condition requiring the non-standard operating practice has been addressed. The account holder is still responsible for all activities in their account carried out under their password.

13. Account Suspension and Termination

If an account holder will be on leave from work for thirty (30) days or more, their supervisor must inform ITD so that the account may be temporarily suspended. Users or supervisors should immediately request account suspension and contact ITD if they have reason to believe that an account may have been compromised or is being misused.

Upon the termination of an account holder's employment or association with Los Alamos County, the supervisor should identify the access needed by coworkers or supervisors to the account holder's files and e-mail. This access will be provided for a period of two months, during which time it is the supervisor's responsibility to move items they wish to keep. At the end of two months, ITD will terminate the account and delete all remaining files. ITD will work with the department involved to transfer any important documents or data files to another designated person so that information is not lost. As part of the exit procedure, account holders must return to ITD or the supervisor all County-owned equipment.

14. Security Training

The County organization responsible for authorizing account access is responsible for training personnel in both desktop computer applications and organizational-specific applications. On request, ITD will work with County organizations on improving applications security and on finding courses to improve employee IT skills. The County recognizes the importance of computing skills for its employees and encourages County organizations to work with ITD on training needs.

ITD is responsible for network and desktop computer security training. Prior to receiving access and passwords a new account holder is required to successfully complete basic security training provided by ITD. This training covers password management, basic physical security, user responsibilities, and usage policies. The training includes an acknowledgment by the new account holders that they (1) have received computer training; (2) understand their rights and responsibilities as defined in this policy; and (3) recognize and understand the penalties for violating this policy. Updated IT security training will be provided by ITD and will be mandatory for account holders at least every five years. Account holders will sign an updated "Account Holder and Computer User Responsibilities" form whenever updated IT security training occurs.

Security questions should be directed to the help desk staff or, after hours, to the on-call IT staff member.

15. Data Security

15.1. The County is responsible for data that may be subject to laws and regulations regarding unauthorized disclosure, may be misused for personal gain, and/or may be of a proprietary nature. Therefore, all account holders must be aware of their responsibilities with respect to the access to, and use of, data in County IT systems. Non-ITD supervisors have the following responsibilities:

- 15.1.1. Knowing the potential risk of release or misuse of data and applications under their control or under the control of their subordinates;
- 15.1.2. Defining access policy with respect to applications, desktop hardware, and data and managing access rights consistent with such risk;
- 15.1.3. Allocating appropriate access authorizations to ITD personnel in writing or through normal application authorizations (at least one ITD staff will normally have the highest level of authorization);
- 15.1.4. Managing the access right allocation, modification, and termination within the capabilities of their applications package(s);
- 15.1.5. Training account holders with access rights on their responsibilities with respect to release and use of the data and use of the applications; and
- 15.1.6. Ensuring that any non-employee personnel with access to County data through their organization (whether such personnel have accounts or not) are fully aware of their responsibilities with respect to the data.

15.2. Personnel with access rights to County data have the following responsibilities:

- 15.2.1. Understanding the rights and duties with respect to the data and application system functions to which they have access;
- 15.2.2. Understanding the potential risk of release or misuse of data and applications under their control; and
- 15.2.3. Immediately communicating to supervisors and ITD any actual or suspected violation of County policies or practices with respect to misuse of data.

15.3. ITD personnel have the following responsibilities:

- 15.3.1. ITD personnel shall not modify data in any applications system without the consent of the supervisor responsible for the accuracy and reliability of that data;
- 15.3.2. ITD personnel may make immediate modifications with verbal authorization from an appropriate supervisor if a system is experiencing severe operational problems and ITD intervention is necessary to restore functionality to the system;
- 15.3.3. ITD personnel modifying applications data will normally inform the appropriate supervisor(s) in writing of their activities and results. If ITD activities bypass the audit/security controls in a system, ITD personnel are required to document their changes in writing to both the supervisor and ITD management;
- 15.3.4. ITD personnel should assist supervisors and personnel in understanding the potential risk of release or misuse of data and applications under their control; and
- 15.3.5. ITD personnel are responsible for hardware and software tool security (e.g. operating systems, data base systems). ITD personnel who become aware of actual or suspected breach of that security shall immediately report such breach to the appropriate applications supervisor and ITD management.

16. Usage Policy Overview

IT resources are critical assets for County operations. To encourage the effective and appropriate use of the County's IT resources, the following usage policies apply to all account holders.

- 16.1. County account holders are expected to use IT assets to maintain their job performance, provide services to customers, and support County operations. The specific tasks to be performed are specified by supervisors, but normally include the following:
 - 16.1.1. Regular and timely usage of email;
 - 16.1.2. Knowledge of desktop computing basics;
 - 16.1.3. Familiarization with computer applications necessary to perform their job functions; and
 - 16.1.4. Usage of the Internet as an information resource for acquiring and using information relevant to their work.
- 16.2. Account holders shall utilize County IT resources solely for County business purposes except as otherwise specifically allowed by this policy and shall conduct themselves in a manner consistent with appropriate standards as established by existing County policies, rules, regulations and guidelines. All existing County policies, rules, regulations and guidelines relating to intellectual property protection, privacy, misuse of County equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality apply to use of IT resources.
- 16.3. All data stored on networked data storage will be backed up nightly Monday through Friday by ITD. The account-holder is responsible for removing data files that are no longer needed in order to effectively manage limited storage space. The account holder

is responsible for creating and maintaining backups of data on non-networked drives or data that needs to be backed up more frequently than nightly.

- 16.4. Should an account holder suspect their computer is infected with a virus or other unwanted software, or suspect their computer is not protected against viruses, they should immediately disconnect their computer from the network and contact ITD.
- 16.5. Account holders should take appropriate protective measures to minimize the probability that their addresses will become targets for spam.
- 16.6. Account holders shall have no expectations of privacy with respect to County IT resource usage. Data that is protected or otherwise confidential by operation of local, state or federal law, rule, regulation or policy must be protected by the account holder.
- 16.7. Computer-based data available to the public under the New Mexico Inspection of Public Records Act, § 14-2-1 *et. seq.*, NMSA 1978 Comp. shall be released, if requested, consistent with and as required by the Act.

17. Usage Policy: Prohibited Use

IT resources are powerful tools purchased to increase productivity and improve the employee's work environment. Misuse of these powerful tools may subject an account holder to disciplinary action. Misuse that is intentional, ongoing, or extensive will be grounds for severe disciplinary action. Account holders should be thoroughly aware of the following prohibited uses, and, if any questions arise, contact Human Resources or ITD.

- 17.1. Account holders shall use County IT resources only for official County business unless otherwise specifically allowed in this policy.
- 17.2. Account holders shall not upload or otherwise transfer out of the County's direct control any software licensed to the County nor data owned or licensed by the County without explicit authorization from the supervisor responsible for the software or data.
- 17.3. Account holders shall not use IT resources to reveal confidential or sensitive information, client data, or any other information covered by existing county, state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Account holders who engage in the unauthorized or otherwise illegal release of confidential information via the County's IT resources, including but not limited to newsgroups or chat rooms, shall be subject to sanctions imposed by existing County policies and procedures associated with unauthorized release of such information or other relevant and appropriate policies, procedures, rules and regulations in addition to disciplinary action arising from misuse of IT resources.
- 17.4. IT assets may not be used to solicit or forward commercial ventures, religious or political causes, solicitation of Union membership or the conducting of official Union business, or solicitations for outside organizations, except as may be specifically authorized by the County Administrator. This does not limit an account holder's rights and responsibilities to distribute any document or information used in legitimate County operations, e.g. vendor proposals, zoning or permit requests, etc.

- 17.5. Account holders shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings. In particular, according to the US Copyright Law, illegal reproduction of software can be subject to civil damages of as much as \$100,000 per work copied, and criminal penalties, including fines and imprisonment. Los Alamos County prohibits the illegal duplication of software or acquiring or using illegal copies of software.
- 17.6. Account holders shall not load executable software, including freeware and shareware, on their personal computers unless directly applicable to performing their job responsibilities and approved by their supervisor and ITD. If a supervisor or County contract manager has determined that privately owned software or shareware or freeware is necessary for an account holder to perform his or her duties, and it cannot be purchased by the County, it must be approved in writing by ITD before installation on a Los Alamos County computer. Approval will require 1) proof of ownership 2) virus checking by ITD personnel; 3) that the software be compatible, in ITD's judgment, with existing County hardware and software.
- 17.7. Account holders shall not use County IT resources to download or distribute pirated software or data, including music or video files.
- 17.8. Account holders shall not use County IT resources to deliberately propagate any malicious code.
- 17.9. Account holders shall not use County IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the County's IT resources.
- 17.10. Unauthorized dial-up access to the Internet is prohibited from any device that is attached to any part of the County's network. Account holders shall not use the County's IT resources to establish connections to non-County Internet service providers unless they are authorized to do so in writing by ITD.
- 17.11. Account holders shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using County IT resources. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties. The account holder shall report to ITD and the account holder's supervisor the repeated receipt of such material.
- 17.12. Account holders are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- 17.13. Account holders shall not use County IT resources to override or circumvent any security mechanism belonging to the County or any other government agency, organization or company.

- 17.14. Account holders shall not use County IT resources for illegal activity, gambling, or to violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

18. Usage Policy: Personal Use of County IT Assets

Occasional and incidental personal use of the County's IT resources, including Internet, email, and phones is allowed subject to limitations. If account holders have any questions about allowable personal use, they should consult their supervisors. Departments may set departmental personal use policies differing from this policy with the approval of the County Administrator. After approval, those policies shall be forwarded to ITD for inclusion in this policy as an Appendix.

Personal use of County IT resources is not considered occasional and incidental if such use:

- 18.1. materially interferes with the use of IT resources by County staff, agents, representatives, officials or contractors;
- 18.2. burdens the County with additional costs;
- 18.3. interferes with the account holder's employment duties or other obligations to the County;
- 18.4. consumes a consequential amount of an account holder's time on the job;
- 18.5. includes any activity that is prohibited under this policy;
- 18.6. is a part of an ongoing for-profit business activity or unauthorized non-profit business activity; or
- 18.7. might reasonably be expected to cast the County, its employees, agents or representatives in a bad light or subject them to public ridicule

Note that allowing occasional and incidental use does not confer any expectation of privacy or ownership as a result of personal use. All email, phone records, systems and Internet access records, and data on County equipment may be public records subject to disclosure under the New Mexico Inspection of Public Records Act, whether used for County business or for incidental personal use. Employees should assume that any records, including personal records stored on County equipment, may be disclosed under that Act. The contents of such records may be disclosed within the County as allowed in Section 20 and approved in Appendix A without the knowledge of the employee.

19. Remote Computing

The County may allow or require selected account holders to access the County network and systems from home or while traveling. This access is granted for the convenience of the County and places specific obligations on the remote access account holder.

Systems security on County-owned laptops must meet the same requirements as systems security on any other County-owned machine. If account holders have any questions, they should call the ITD help desk.

Access to County email through the Internet does not require any special software or controls, although the County recommends all users have up-to-date anti-virus software on personal

machines. The County also recommends account-holders acquire anti-spyware software, install a firewall, and use caution when downloading software on their personal machine.

Account users who access the County network behind the firewall will need to have a County-owned laptop for this purpose. The County-owned laptop will conform to all provisions of this policy and, upon request, will be brought into ITD for review of machine setup, security, and operating practices. Such review shall be conducted upon reasonable notice to the account-holder. If County account-holders have any questions about remote access responsibilities, they should call the help desk.

Access of mobile devices including Personal Data Assistants (PDAs), Internet Enabled Cellular Phones, Wearable Computers, Flash Drives, Wireless Access Points, Switches, and Portable Computers to the County network will be allowed as follows:

The user of the mobile device will accept responsibility for taking reasonable precautions in protecting the data on the mobile device and agrees to adhere to this policy. The mobile device user will not be allowed to have administrative rights on the network unless granted by a special exception by the IT Systems Manager or designee. The user of the mobile device agrees to abide by the IT Technology Usage and Computer Security Policy. Any device that is connected at any time to the County network must adhere to the following:

- a. Devices connected to the County network must be determined to be a benefit to the County and to not impede the ability of the IT division to provide support to the County by the IT Manager or designee rather than a convenience.
- b. The Department Director or designee must submit the request to add the device.
- c. Any mobile device that can store County data must support encryption of the data; County data on mobile devices must be encrypted at all times.
- d. All mobile devices owned by the County or allowed on the County network must be identified by their MAC address to the IT division before being connected.
- e. The mobile device operator must be identified by name and contact information to the IT division.
- f. The mobile device operator must be familiar with the Information Technology Usage and Security Policy for Los Alamos County.

Devices not owned by the County on the County network are subject to software audit to ensure that no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.

20. Enforcement and Sanctions

The County may install software and/or hardware to monitor and record IT resource usage, including email, Internet usage, telephone usage, and all files stored on County systems. All automated monitoring will be set up by ITD staff, must meet the authorizing criteria below, be authorized in writing, specify a time period, specify the assets to be monitored, and specify who will have access to the results.

The County Administrator may authorize ITD to perform temporary or permanent monitoring of individuals, organizational units, or all County account holders. Based on a complaint or a supervisor's request, a Department Head, with the concurrence of Human Resources, may authorize ITD to monitor an individual account holder. Records of such monitoring as well as the contents of monitored accounts are subject to standard County personnel records management and retention policies.

This policy on monitoring does not change supervisory responsibility for normal oversight of work activities. Supervisors with concerns about specific employees or activities should bring those concerns to Human Resources. This policy also does not change the responsibility for all account holders to report suspected misuse of County IT resources.

Serious disciplinary action, consistent with the County's Personnel Rules and Regulations, up to and including termination of employment may result from activity prohibited by this Policy. In the case of a contractor, the County may seek damages, penalties and any remedy available at law or in equity. Illegal activity involving County IT resource usage may be referred to appropriate authorities for prosecution.

In agencies or offices where exceptions to this policy are within legitimate job responsibilities, the County Administrator, or the Administrator's designee, may exempt one or more account holders from relevant portions of this policy. The exemption will be in writing with copies to the supervisor, Human Resources, and ITD.

ITD may immediately disable any account that is reasonably suspected of misuse or a security breach. ITD will immediately notify the relevant County supervisor(s) and Human Resources and retrieve pertinent account holder data and access records.

21. Technology Components of Security

ITD is responsible for putting in place technology-based perimeter defenses and insider defenses. The details of these defenses will not be released except on a need-to-know basis because of the potential guidance such details could give to individuals attempting unauthorized use. The sections containing the details are marked appropriately and are included in copies of this plan held by members of the Management Oversight Committee and ITD Staff.

Defenses include such tools as: network firewalls; virus detection and cleaning software and/or hardware; need-to-know separation; centralized account management and activity recording; and IT asset monitoring software and hardware.

Discussion of these security protection details outside of the Management Oversight Committee members and ITD staff and ITD's contactors without approval of the County Administrator or the Administrator's designee is a violation of this policy.

ITD is also responsible for establishing and enforcing all WLAN technology standards and will be the sole provider of design, specification, operation, maintenance and management services for all wireless access points. Employees may not independently install or operate WLAN access points in their departments. Only County employees and authorized visitors may use the County WLAN based upon the needs of the County; exceptions must be authorized by the IT Manager or designee. All WLANs must be configured according to County IT security standards. ITD is

responsible for managing the security of the County WLAN. All WLAN communications must be encrypted. All wireless devices using the County WLAN must be registered with ITD.

22. Backup and Recovery

All network data will be backed up regularly by ITD and stored offsite to minimize loss in the case of equipment or software failure. ITD will also maintain redundant hardware and automated failover for critical applications. Details are included in the ITD Disaster Recovery Plan.

Account holders should not store valuable County files or other County data on their personal computer. Central drives backed up as part of ITD's regular backup process are provided for storage of such files and data. Questions about this process or data backup/recovery should be referred to the help desk.

23. Definitions

As used in this policy:

- 23.1. **access** means the ability to read, change, or enter data using a computer or an information system.
- 23.2. **equipment** means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.
- 23.3. **County-owned** includes equipment the county leases or controls under contract.
- 23.4. **freeware or shareware** means software that is available free of charge and available for download from the Internet. Freeware is protected by a copyright and is subject to applicable copyright laws.
- 23.5. **information technology resources (IT resources)** means computer hardware, software, databases, electronic message systems, communication equipment, computer networks, telecommunications circuits, or any information used by a County agency to support programs or operations that is generated by, transmitted within, or stored on any electronic media.
- 23.6. **malicious code** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.
- 23.7. **pirated software** means licensable software installed on a computer system for which a license has not been purchased or legally obtained.
- 23.8. **physical control** means knowing where your information technology resources are and knowing that they are not being misused.
- 23.9. **reconfigure** means any software, hardware, or parameter change that changes network address, computer name, operating system (e.g. Windows to Linux), computer security software, or function (e.g. creates a server from a workstation).
- 23.10. **security mechanism** means a firewall, proxy, Internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or the unauthorized use, damage, destruction, or modification of data and software.

- 23.11. **sexually explicit or extremist materials** means images, documents, or sounds that can reasonably be construed as:
- 23.11.1. Discriminatory or harassing;
 - 23.11.2. defamatory or libelous;
 - 23.11.3. obscene, of a primarily sexual nature, or pornographic;
 - 23.11.4. threatening to an individual's physical or mental well-being; or
 - 23.11.5. read or heard for any purpose that is illegal.
- 23.12. **strong password** means a password that is case sensitive; at least eight characters in length; and containing at least one capital letter, one lower case letter, one number, and one special character. This reduces the likelihood of guessing a password, but because the user can create their own password, it is not completely secure. An individual attempting to crack an eight character strong password using a single computer would take approximately 321 days compared to a six character mixed password which would take about 5.8 hours to crack. Most hackers use multiple computers to try and crack passwords.
- 23.13. **virtual private network (VPN)** means an encrypted communication link established between a remote device and the County network via the internet.
- 23.14. **WLAN** means a wireless local area network in which a mobile user can connect to a local area network through a wireless (radio) connection.
- 23.15. **Account holder** means an individual who has been authorized to access County IT resources and given an account, who is using County IT resources, and who meets one of the following criteria.
- 23.15.1. an employee of Los Alamos County;
 - 23.15.2. an elected official of Los Alamos County;
 - 23.15.3. an individual working under contract to the County; or
 - 23.15.4. a volunteer providing service to the County.

Appendix A: Acknowledgement Form

Los Alamos County

Information Technology Account Holder Acknowledgement Form

I understand that Los Alamos County information technology resources are for official business only, except where there is occasional and incidental personal use allowed by policy. There shall be no expectation of privacy in the use of Los Alamos County information technology resources. My information technology resources, including county-owned equipment used offsite, and all software programs and associated data are subject to waste, fraud, and abuse audits and monitoring by assigned County personnel at any time. I understand that audits and monitoring of County information technology resources that I use may be authorized and conducted without my knowledge and I hereby consent to any such audits and monitoring, except that audits of County equipment maintained offsite may be conducted only upon reasonable notice and at reasonable times.

I have read this form and the Los Alamos County Information Technology Usage and Security Policy. I acknowledge my responsibilities as an account holder, and agree to follow all the procedures and requirements set out in the Los Alamos County Information Technology Usage and Security Policy. I understand this document will be kept in my Personnel folder during my employment with Los Alamos County or, in the case of a contractor, the County contract file.

Account Name _____ Date _____

User Name _____ Number/Contract No. _____

User Signature _____

I validate that the above user has a need to access Los Alamos County computing resources in the performance of his/her duties and has a need-to-know for the information processed by the Los Alamos County computing resources related to his/her duties.

Supervisor/County contract supervisor/County Administrator Name Date

Supervisor/County contract supervisor/County Administrator Signature

**Los Alamos County
Computer Security Policy
Appendix B**

Appendix B: Master Computer Protection Plan

MASTER COMPUTER PROTECTION PLAN

Incorporated County of Los Alamos

In fulfillment of the requirements of DOE Order 1360.2B, "Unclassified
Computer Security Program."

M. Wayne Budwine
U.S. Department of Energy
Computer Security Operations
Manager Representative

Date

**Los Alamos County
Computer Security Policy
Appendix B**

Purpose

This Master Computer Protection Plan (MCP) addresses the requirements and responsibilities for establishing and maintaining a secure operating environment for computer systems that process unclassified and sensitive unclassified information. Unclassified information is that which is open for public use with no restrictions. Refer to the attachment for the definition of sensitive unclassified information.

Scope

This MCP applies to all Incorporated County of Los Alamos, hereinafter referred to as County, computer systems that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of unclassified data and information located on County-controlled property, as well as those used outside of County-controlled property by its employees.

Responsible Personnel

The following personnel are responsible for protecting information from unauthorized access, disclosure, modification, and destruction: (1) County Administrator, (2) County Information Technology (IT) Director, and (3) Computer Users. Computer users have primary protection responsibility for their systems, their primary and backup storage media, and the data on them. The IT Department has primary protection responsibility for centrally maintained systems, their associated media, and the data on them.

Administrative Safeguards

Computer users will be authorized, in writing, by their supervisors, County contract managers, or higher-level management, for access to information on a need-to-know basis. This information is to be utilized for official purposes only. Users will acknowledge their responsibilities by executing an *Account Holder and Computer Users Responsibilities* form included in the *Los Alamos County Computer Security Policy*.

County computer training provided to every computer user will address the requirements for maintaining a secure operating environment. Periodic security awareness training will be accomplished through initial briefings, completion of the *Account Holder and Computer Users Responsibilities* form, meetings, or by distribution of pamphlets, flyers, and memoranda.

Periodic reviews to detect and deter computer misuse and abuse will be conducted. The County will also conduct computer security self-assessment reviews, at

**Los Alamos County
Computer Security Policy
Appendix B**

least annually, to verify that information is being protected. As part of that annual review, this MCPP will be reviewed and updated as necessary. DOE will conduct periodic random program reviews to verify compliance with computer security requirements.

Disaster recovery/contingency planning should address information for backup and recovery as well as alternative processing measures to be activated should a computer system fail to operate. These plans will vary in detail based on the system and the need for its availability. Generally, a disaster recovery/contingency plan for a microcomputer is as simple as finding another compatible system to use. Extensive testing of these plans is not required.

Technical Safeguards

Anti-viral software is required on all systems. Media not originating on a County computer is to be checked for potential viruses prior to being placed into service. Computer users are encouraged to protect sensitive information by employing password screen savers, computer locks, desk or office locks, or other means of securing their workstations.

If available, user IDs, passwords, and audit trails will be utilized to control and monitor access to information on multi-user systems. Each user ID and password combination is intended for use by a single individual and should not be shared with or revealed to any other individual.

Prior to computers being released from the County, systems will be sanitized or memory overwritten so that no information is retained. This is to ensure that sensitive unclassified information is not revealed to unauthorized individuals.

DOE will be notified prior to any Internet connections and appropriate security measures will be implemented.

Physical Safeguards

The security environment is dependent upon the physical location of the computer system. Best business practices will be used to ensure that the level of physical security is appropriate to the value of the system hardware and software and the sensitivity of the data it processes.

**Los Alamos County
Computer Security Policy
Appendix B**

**SENSITIVE UNCLASSIFIED INFORMATION
SUMMARY SHEET**

DEFINITION:

As defined in the National Telecommunications and Information Systems Security Policy, NTISSP #2, sensitive unclassified information is:

Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or Federal government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U. S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided the U. S. Government by its citizens. Information found within the ADP system and its associated telecommunications system clearly falls into this category.

SENSITIVE unclassified information:

- That which requires discretionary protection due to statutory or regulatory restrictions
- Legal information
- Privacy Act information; personnel data, personal identifying information, payroll
- Caveat marked documents; Official Use Only or other headings/footings
- UCNI (Unclassified Controlled Nuclear Information)
- Proprietary Data; privileged information
- Technical Scientific data
- Limited Access information
- Other information denoted as needing protection

Appendix C: ITD Supported Applications

IT Support –

IT Support is available through the automated knowledge base or by submitting a request to IT in the Right Now Technology (RNT) tracking system.

Requests are entered into RNT by submitting a request through the link to RNT on the intranet, sending an email to IT Request, which creates a request in RNT, or by calling 662-8090 for emergency situations during work hours.

The knowledge base is available to employees 24x7. To get into the RNT system from the intranet, open Internet Explorer, click on IT Support and search the answers. There are over 20,000 answers in the IT knowledge base relating to the Applications used throughout Los Alamos County. If you are unable to find your answer in the automated help, you can submit a request from that site by clicking on the Ask IT or IT Requests button and submitting a request. By using your account and password, you can login and monitor your request as it progresses.

Emergency Support –

Call out support for emergency IT situations is available 24x7 by calling 662-8222 and asking them to page the IT person on call. This may result in a charge back to the Department. 24x7 automated support is always available by going to the intranet and clicking on IT Support and searching answers. There are over 20,000 answers in the IT knowledge base. End users can also submit a request by clicking on the Ask IT or IT Requests button and submitting a request. They can login and monitor their request as it progresses.

ITD Supported Hardware

1. **Approved hardware purchases.** Departments with budget approval can request a standard client PC from the Warehouse. If the department has special requirements or needs a notebook, they can place a written work request to IT explaining the requirements and asking for a special quote. IT will provide the quote to the department and the department will be able to order the computer through Procurement. Once the computer is ordered, either from the Warehouse or by Procurement, the manager of the person receiving the computer (or a person to whom that manager has delegated that authority in writing to IT) needs to fill out a computer request on the intranet.
2. **Approved portable device purchases.** IT will keep a list of currently supported Phone/PDA/Hand-held devices supported by IT on the intranet. If a department purchases a device that is not on that list, it will not be supported unless the following steps are taken:
 - Review by IT to ensure that device can be supported
 - Purchase by the Department of specific device for IT so that support can be provided

- Purchase by the Department of any software required to provide support for the portable device
3. **Client Hardware replacement policy.** Hardware will be purchased with a three year warranty for hardware support. Hardware will be supported by IT in conjunction with the vendor for up to four years after the hardware was purchased, as long as it is in good functioning order. If the computer fails between the three and four year time frame, the department will be asked to replace the hardware with a new unit. Replacement of hardware every four years is not an optional budget item and computers older than four years of age are subject to being removed from the network in order to maintain network security and operability.

ITD Supported Applications

Supported Applications-

Definitions from webopedia.com:

Application - A program or group of programs designed for end users. Software can be divided into two general classes: systems software and applications software. Systems software consists of low-level programs that interact with the computer at a very basic level. This includes operating systems, compilers, and utilities for managing computer resources.

In contrast, applications software (also called end-user programs) includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems software because it is unable to run without the operating system and system utilities.

End User - The final or ultimate user of a computer system. The end user is the individual who uses the product after it has been fully developed and marketed. The term is useful because it distinguishes two classes of users, users who require a bug -free and finished product (end users), and users who may use the same product for development purposes. The term end user usually implies an individual with a relatively low level of computer expertise. Unless you are a programmer or engineer, you are almost certainly an end user.

Client - The client part of a client-server architecture. Typically, a client is an application that runs on a personal computer or workstation and (usually) relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

On the client side, IT fulfills the following duties for supported applications:

- provides support for the installation of software, both systems and applications

- ensures the supported applications are compatible with supported operating systems and other supported programs
- works with the vendor to resolve problems
- retains installation media
- provides information on costs to allow departments to budget and purchase hardware and/or software to allow them to maintain compliant levels to meet supported vendor specifications for client machines and applications
- installs current levels on hardware, operating systems and application software in compliance with the Application vendors specifications

On the server side, IT fulfills the following duties for supported applications:

- provides support for the installation of applications,
- ensures the supported applications are compatible with supported operating systems and other supported programs
- works with the vendor to resolve problems.
- retains installation media,
- backs up application components on the server
- maintains current levels on hardware, operating systems and application software in compliance with the Application vendors specifications
- work with vendor and end users to get costs for departments to upgrade server side application components for budget purposes as needed
- budgets and pays for software maintenance for applications that are used centrally
- Understand and maintain interfaces to share data between applications
- Determine and maintain single data source for use throughout the County
- Outsource support to vendors based upon cost, staff and support requirements

End Users have the following responsibilities for supported applications:

- Backup data that is not stored on network drives
- Pay for licenses for individual productivity programs
- Pay for client access licenses as needed
- Pay for support for applications that are used in one department
- Work with vendor/IT staff as necessary to resolve problems within applications
- Notify IT when problems occur through approved mechanism
- Maintain inventory and control of department owned hardware and software most of which is available through reports that the department can run from the County inventory/stores order systems
- Keep machines and operating systems updated via replacement when the machine reaches four years from the date of purchase
- Ensure that the application licenses have been purchased and kept at supported levels for licenses purchased and/or maintained by the departments

- Submit interdepartmental requests and bring IT projects before management oversight committee for approval/resources
- Designate departmental project manager for projects
- Maintain appropriate departmental resources with expertise in the use of the application
- Keep up-to-date with enhancements to applications and coordinate the installation of these features with IT

ITD Permitted Applications and Hardware

Permitted Applications-

Permitted applications are applications for which IT does not provide direct support, but are on the County network with IT's knowledge and approval. These applications generally are supported by the vendor with Department/Division staff coordinating the support. Permitted applications are reviewed on a case by case basis. On occasion, a permitted application may cause conflicts with supported applications. In those cases, the permitted applications will be removed from the machine on which they are causing problems and the Department/Division may allocate a separate machine to run the permitted application.

Permitted Hardware Devices-

Permitted hardware devices are devices for which IT does not provide direct support, but are on the County network with IT's knowledge and approval. These devices generally are supported by the vendor with Department/Division staff coordinating the support. Permitted devices are reviewed on a case by case basis. On occasion, a permitted device may cause conflicts with supported devices or applications. In those cases, the permitted device will be removed.

A list of supported applications and devices will be provided by ITD.