Loudoun County, Virginia
REQUEST FOR PROPOSAL (RFP)

RFP RFQ 539782
APPENDIX H
Loudoun County Technical Standards

The following provides the County’s established technical standards to provide a high-level understanding of the technical environment across existing systems, platforms and interfaces. The Offerors should leverage and understand the environment while preparing proposals.

Technology Environment
The Department of Information Technology (“DIT”) provides information, office automation, and communications systems and services to all the departments of Loudoun County government. DIT support staff is responsible for maintaining the hardware, software, and network resources required to operate Loudoun County’s technology infrastructure.

Server Platforms
The County utilizes Intel-based Microsoft Windows 2012 and 2016 servers. The County has standardized on VMware ESXi hypervisor on Dell servers with Intel Xeon processors. The majority of servers are virtual and all future server hosts should be virtualized. The County uses Veeam Enterprise Backup for backups of all major Windows and Unix servers and applications. The County leverages VMware Horizon 7 to support GIS and other virtual applications. An IBM Z114 2818-I03 Enterprise Mainframe Server houses the County’s legacy application for Land Records (LMIS).

Database Management Systems
The County prefers two (2) different database products: Oracle and Microsoft SQL Server 2016 or higher.

Programming Languages
The County’s application systems utilize several different computer programming languages. The “legacy” applications were developed utilizing COBOL. Non-Financial applications are being re-written out of COBOL using VB.NET. Financial applications will utilize Oracle OAF and Java.
Network Services
TCP/IP is the predominant protocol utilized to communicate with Loudoun County servers. The County makes every effort to utilize browser-based access for all systems. IBM DB2 Connect, IBM Host on Demand, and IBM Wintegrate are the primary communications packages used on the IBM platforms. The County network is currently Microsoft-based Active Directory. A combination of O365 services and applications along with limited on-premise Microsoft Exchange servers provide the County’s email system. Remote access to the County networks is supported via SSL and IPsec VPN.

Personal Computers
County personal computer workstations consist of both networked and stand-alone PCs. The current standards are Dell models 5050 for desktops and models 5580, 7280, 7480 for laptops. Microsoft Windows 7 Enterprise 64 bit operating system and Microsoft Office Suite 2013 are standard on each system. Approximately 10% of the desktops are virtualized under a VMware environment.

Telecommunication
The County currently utilizes a combination of VoIP and analog networks utilizing SIP and H323 protocols supported by a Avaya PBX system. A majority of County facilities use Avaya One Cloud hosted telephony services with some locations remaining on the legacy Communication Manager 6.3.7 call management system.

Internet/Intranet
The County’s preferred Web and Intranet applications platform is Microsoft Internet Information Services on Windows 2019 virtual server. Other popular Unix-based operating system platforms (Red Hat Linux, Sun Solaris) and web platforms (Apache) are supported on Dell, or Sun hardware, respectively. The County’s z114 Enterprise Server is used for hosting data for Intranet and Internet based applications. Web servers are typically reversed-proxied, using F5 systems, in a DMZ.

Remote Access, Mobile Devices and Equipment Standards:
As Loudoun County integrates its service delivery, employees have become increasingly mobile as they deliver more services in the field. Loudoun County has a requirement to be able to use mobile devices (to include laptops, tablets, iPads and Smartphones) to work online anywhere they are delivering services using either a laptop or tablet PC. Loudoun County currently utilizes Global Protect and NetMotion for employee VPN access.. In addition, whenever a computer network connection is established between a County computer and another computer at a location outside an official Loudoun County office, and whenever this connection transmits or is likely to transmit sensitive information, the link shall be encrypted.

Security
The County is seeking a robust security component that will enable staff to assign access rights through a user friendly interface and to give rights across program areas as well as locations. The County is seeking flexibility in modifying security by individual in a live environment. The County is moving towards an integrated service provider model and the security must support this multi-role staffing pattern. However, access to all components of
the proposed New System shall be granted only to authorized users. The County must have the ability to reset all user passwords and maintain passwords for the New System.

Security Profiles - Users of the New System shall be limited to specific functions through user "profiles" that are maintained by a System Administrator. At a minimum, conditional access capabilities such as password protection must be included. Access rights shall be based on "need to know" criteria, with the ability to limit access for updates, as well as for data retrieval.

Authorized users of the proposed New System must be identified by a User ID and Password or another means for authentication that provides equivalent or better security.

The software must support https (TLS 1.1 or higher) for all traffic and not cache any information locally on any device used to access the New System.

Cloud Hosting Standards:

Cloud hosting must be SOC 2 compliant. SOC 2 compliance as part of the AICPA Service Organization control (SOC) reporting platform. In an effort to dramatically revamp reporting on service organizations (and to align with the growing trend of globally accepted accounting principles), the American Institute of Certified Public Accountants (AICPA) launched the SOC reporting platform, for which there are three (3) reporting options: SOC 1, SOC 2, and SOC 3. SOC 2 compliance is conducted in accordance with AT 101. SOC 2 compliance is designed for the growing number of technology and cloud computing entities that are becoming very common in the world of service organizations. Service providers are required to provide Loudoun County DIT with their SOC2 Type 1 and Type 2 reports on an annual basis.

ISO/IEC 27017 is a code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO 27017 is an extension of ISO 27002. ISO 27017 generally focuses on the protection of information in the cloud services. Service providers are required to provide Loudoun County DIT with any ISO 270xx certification reports for review on an annual basis.