ARRC RFP #19-45-207439 - Appendix B: Technical Requirements

Requirements for All Respondents	Meets	Does not Meet	Comments

1. Policy Requirements
    a. ARRC policy dictates that all contractors accessing ARRC's computer resources will comply with our security policies (available upon request).
    b. ARRC policy requires all software used or installed must be legally licensed.
    c. ARRC policy is to encrypt data from ARRC databases in flight as well as at rest.			

Requirements for On Premise Solutions	Meets	Does not Meet	Comments

1. Uses one of the following database systems:
    a. SQL Server 2016, 2017
    b. IBMi DB2 Version 7.3			

2. Uses one of the following drivers for data access
    a. Microsoft ODBC Driver 17 for SQL Server *preferred
    b. Microsoft ODBC Driver 13.1 for SQL Server
    c. Microsoft OLEDB Driver for SQL Server (MSOLEDBSQL, not SQLOLEDB)
    d. SQL Server Native Client
    e. iSeries Access ODBC Driver			

3. Client installation can be packaged for delivery by automated endpoint management system.			
4. Client installation can be made silent for remote delivery.			
5. Integration of Security			
6. Is the security integrated with our internal Active Directory for authentication?			
7. Does the application use groups to assign rights?			

8. How does the application implement minimum required permissions?			
9. Secure in storage, in transmission, and minimum display of PII 10. Is ARRC data encrypted in storage? 11. Is ARRC data encrypted in backup? 12. Is ARRC data encrypted in flight?			
13. Below is a list of ARRC Infrastructure standard supported software. Please list below any new components that your system would be require ARRC to install or support.			

Requirements for Hosted or SAAS Solutions	Meets	Does not Meet	Comments

1. API exposed for interfaces uses one or more of the following technologies:
    a. REST *preferred
    b. SOAP
    c. JSON *preferred
    d. XML			

2. Solution has a reporting tool for custom report development and data access			
3. Authentication integrates with our current AD infrastructure			
4. Does the application use SAML or other well known protocols to implement federated security?			
5. Does the application use groups to assign rights?			
6. Does the application implement minimum required permissions?			

7. Data security
    e. Is ARRC data encrypted in storage?
    f. Is ARRC data encrypted in backup?
    g. Is ARRC data encrypted in flight?			

8. Does your policy include a signed non-disclosure agreement in force for ARRC data?			
9. Describe is the Backup and Disaster Recovery Plan for ARRCs data?			

10. How has the company attempted to limit excessive data leakage (limit the amount of data presented or reported on?)
11. How highly available is the system?
12. Describe your breach notification and response process.
13. Have you notified anyone of a breach in the past?
14. How will the application be protected from Command and Control or keystroke recording for ARRC data?
15. Can the workstations that run the remote software be audited on connection? Is there a way to get the list of workstations if not on ARRC property?
16. Below is a list of ARRC Infrastructure standard supported software. Please list below any new components that your system would be require ARRC to install or support.

The ARRC infrastructure currently supports the following. Proposed systems that would integrate without the addition of new components are preferred:

Operating Systems
- Windows 10 (1709 current baseline, 1809 in testing, 1909 might be next baseline)
- Windows Server 2012R2, 2016, or 2019 (prefer 19, then 12R2, then 16)
- Linux (RHEL/CentOS 7, Ubuntu 16/18 LTS, others on request, limited though)
- Other (IBM iSeries on POWER7 and POWER9)

Database Systems
- SQL Server 2016, 2017
- IBMi DB2 Version 7.3

ARRC RFP #19-45-207439 - Appendix B: Technical Requirements

Core Systems supported on-premise

- Redundant DNS for internal DNS supporting akrr.local and others
- Redundant DHCP for most corporate subnets
- Redundant Active Directory (no current federation internal nor external)
- Group Policy Management for least privilege, policy enforcement for Windows
- Ivanti Endpoint Management (LANDESK) for provisioning, software distribution, patching
- Ivanti Antivirus (Bitdefender)
- Ivanti Mobile Device Management (MDM) for Android/iOS devices
- Barracuda SPAM Gateway (for email protection)
- iPrism Web Proxy (for outbound web protection)
- Exchange for Email
- SAN for block-level storage
- NAS for file-level storage, secondary storage, and soon off-site storage
- Veeam Backup and Restore for data protection
- Veeam ONE for some system monitoring
- PRTG for most system monitoring
- HPE OneView for some system monitoring
- vSphere Enterprise Plus virtualization with vCenter Centralized Management
- MS Certification Services for internal digital certificates
- IIS and Apache on Windows, Apache on Linux

Core Systems supported off-premise/cloud

- Entrust for internet-facing digital certificates
- Network Solutions for internet-facing DNS supporting akrr.com and others

Core Applications on all Desktops

- Office 2016 Pro
- Firefox
- Chrome
- Internet Explorer (where required)
- Edge (Both legacy and new) are NOT supported
- Adobe Acrobat Reader