REQUEST FOR PROPOSALS

RFP NO. 19-01

DRS MAINFRAME REHOSTING SERVICES

ADDENDUM 1

QUESTIONS AND ANSWERS

May 9, 2019
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>REFERENCE</th>
<th>DRS RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  How will answers to questions be transmitted to Bidders?</td>
<td>RFP, Section 2.3.3</td>
<td>This document, which includes all of the questions submitted by vendors prior to the deadline and DRS’ responses, is available as an addendum to the RFP on the DRS website and on the state’s WEBS system. A copy will also be emailed directly to each bidder that submitted a Letter of Intent to Propose.</td>
</tr>
<tr>
<td>2  Digital Submission table: what is the difference between 19-01&lt;bidder name&gt;10JRP.xlsx &amp; 19-01&lt;bidder name&gt;15JRP.xlsx?</td>
<td>RFP, Section 2.4.1</td>
<td>They are the same document. DRS will amend the RFP to correct the error.</td>
</tr>
<tr>
<td>3  Is DRS envisioning an on-prem or cloud based destination for this</td>
<td>Exhibit B – Scope of Services, Section 1.1</td>
<td>See Question 4</td>
</tr>
<tr>
<td>4  Describe your desired landing zone.</td>
<td>Exhibit B – Scope of Services, Section 1.1</td>
<td>DRS’ preferred target infrastructure/platform is cloud. The Vendor will provide a hosting recommendation as described in Exhibit B – Scope of Services, Section 2.3.3 Server Hosting Analysis and Recommendation.</td>
</tr>
<tr>
<td>5  Could you provide details on your distributed architecture</td>
<td>Exhibit B – Scope of Services Section 1.1</td>
<td>The target environment will be Adabas and Natural deployed in Linux, connected to .NET C# applications via Entire-X and Web-Services, using VT emulation for UI.</td>
</tr>
<tr>
<td>6  Do any of the mainframe applications connect to the non-mainframe</td>
<td>Exhibit B – Scope of Services, Section 3.1 Phase 1</td>
<td>Yes, the DRS mainframe applications do connect to non-mainframe applications. They do so through EntireX or Natural’s web-service protocol (Natural’s REQUEST DOCUMENT statement).</td>
</tr>
<tr>
<td>7  Does the state want to retain the JCL like environment or convert the</td>
<td>Exhibit B – Scope of Services, Section 3.2 Phase 2</td>
<td>For the duration of this project, DRS prefers a JCL Emulator.</td>
</tr>
<tr>
<td>Question</td>
<td>Exhibit</td>
<td>Answer</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>8 Will user stories, test cases, and test scenarios will be provided by DRS to Bidders? How many test cases do you currently have for batch and for online?</td>
<td>Exhibit B – Scope of Services, Section 2.5.1</td>
<td>Bidders will not receive any user stories, test cases or test scenarios at this stage of the procurement. DRS has defined the following areas for testing. Each area may have both online and batch testing needs: - Review Member Screens - Process Member Audits - Optional Bills - Withdrawals - Restores - System/Plan Transfers - Legal Orders - Benefit Estimates - Retirement Benefit Calculations - Retirement Benefit Re-calculations - Disability - Death Process - Retiree Return to Work - ERA / eServices - Accounting Services: Disbursement Activities - Trust Accounting - Accounts Receivable - Employer Audit - COLAs - Annual Tax Reporting - Age 70.5 Annual Notification - Age 95+ letter process The chosen Contractor will participate as described in detail in Exhibit B – Scope of Services, Section 2.5.1.</td>
</tr>
<tr>
<td>9 Have performance metrics already been captured by DRS? If so, can those be provided to Bidders?</td>
<td>Exhibit B – Scope of Services, Section 7</td>
<td>See response to Question 78</td>
</tr>
<tr>
<td>10 Will it be possible to receive copies of the code (without data) in order to do parsing offsite?</td>
<td></td>
<td>Yes, if: - The requirements in Exhibit C - Sample Contract, Attachment 1 Security Requirements are met, and - The offsite work is approved by DRS.</td>
</tr>
<tr>
<td>11 What are the DRS policies for behavior? Can copies of these policies be provided to Bidders?</td>
<td>Exhibit C – Sample Contract, Section 5.2.4</td>
<td>See Attachment 1 at the end of this document</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>12</strong> What are the options for providing bidder’s access to DRS systems? <strong>Bidder clarification:</strong> What are the options for providing bidder’s access to DRS’ source code? Will the winning bidder have access to the existing test/non-production system during the project for purposes of verifying test cases and capturing test results for comparison?</td>
<td>Exhibit C – Sample Contract, Section 5.2.6 DRS will grant log-in accounts to non-production environments and the successful bidder will have access to source code in these environments. Only DRS owned equipment will be allowed to connect to the DRS network. See Exhibit C – Sample Contract, Attachment 1 SECURITY REQUIREMENTS d. v.</td>
<td></td>
</tr>
<tr>
<td><strong>13</strong> What are DRS’ procedures for this termination clause?</td>
<td>Exhibit C – Sample Contract, Section 8.7.1 At the time of contract termination, DRS will identify any specific requirements to ensure effective transition or project closure.</td>
<td></td>
</tr>
<tr>
<td><strong>14</strong> This does not address handling of any costs associated with any direct or third party licenses, which would be for the account of DRS. Please confirm this understanding.</td>
<td>Exhibit C – Sample Contract, Section 6.1.9 The proposal should include the costs for third party utilities and other software to be provided by the Vendor, with those licenses to become the property of DRS. See Exhibit C – Sample Contract, Section 6.1.9.</td>
<td></td>
</tr>
<tr>
<td><strong>15</strong> Does DRS have specific acceptance criteria for each milestone, or will those be developed with the Contractor during Assessment?</td>
<td>Exhibit C – Sample Contract, Section 10.1 Specific acceptance criteria will be developed with the Contractor during Phase 1 - Planning and documented 2.2.12 Phase Exit Plan described in the Exhibit B – Scope of Services.</td>
<td></td>
</tr>
<tr>
<td><strong>16</strong> What is your acceptance criteria for subcontractors?</td>
<td>Exhibit C – Sample Contract, Section 21.14 For details about subcontractors see Exhibit C - Sample Contract, Section 21.14. DRS will evaluate subcontractor requests based on their experience, qualifications, role, and any other factor DRS deems important.</td>
<td></td>
</tr>
<tr>
<td><strong>17</strong> Can you describe your remote access options to the DRS environment?</td>
<td>Exhibit C – Sample Contract, Attachment 1 RSA SSL VPN (Service provided by WaTech)</td>
<td></td>
</tr>
<tr>
<td><strong>18</strong> Can Bidders include additional milestones for payment?</td>
<td>Exhibit C – Sample Contract, Attachment 3 Yes, bidders can propose additional payment milestones for consideration.</td>
<td></td>
</tr>
<tr>
<td><strong>19</strong> What tools are currently being used for ETL?</td>
<td>Exhibit G – Technical Requirements Axway is the Secure-File-Transfer product; Natural programs extract some files; Adabas tools extract some files. Software AG’s Replicator product may be used to transport database content across platforms.</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Description</td>
<td>Exhibit</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>20</td>
<td>Can you elaborate on EOS and Securitre?</td>
<td>Exhibit G – Technical Requirements, ID 1</td>
</tr>
<tr>
<td>21</td>
<td>Which security software is being used on the open platform today at DRS?</td>
<td>Exhibit G – Technical Requirements, ID 1</td>
</tr>
<tr>
<td>22</td>
<td>Which technology (i.e., CITRIX, F5) is currently used to safely connect outside users to DRS applications?</td>
<td>Exhibit G – Technical Requirements, ID 5</td>
</tr>
<tr>
<td>23</td>
<td>Please expand on the current use of stateless and stateful transactions.</td>
<td>Exhibit G – Technical Requirements, ID 14</td>
</tr>
<tr>
<td>24</td>
<td>Please expand on the current DRS usage of intermediate storage in the Natural applications.</td>
<td>Exhibit G – Technical Requirements, ID 45</td>
</tr>
<tr>
<td>25</td>
<td>Please expand on the current usage of the multiple authentication methods in the Natural systems.</td>
<td>Exhibit G – Technical Requirements, ID 52</td>
</tr>
<tr>
<td>26</td>
<td>Can you elaborate on the requirements regarding the solution logs and monitors application usage activity?</td>
<td>Exhibit G – Technical Requirements, ID 63</td>
</tr>
<tr>
<td>27</td>
<td>Please expand on where in the DRS systems interactive help for technicians applies.</td>
<td>Exhibit G – Technical Requirements, ID 87</td>
</tr>
<tr>
<td>28</td>
<td>Please expand on where in the DRS systems interactive help for technicians applies.</td>
<td>Exhibit G – Technical Requirements, ID 98</td>
</tr>
<tr>
<td>29</td>
<td>The solution provides a scratch pad. Where in the system is this functionality needed? Please expand on its uses.</td>
<td>Exhibit G – Technical Requirements, ID 101</td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td>Exhibit</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>30</td>
<td>The solution provides automatic copy of highlighted text. Where in the system is this functionality needed? Please expand on its uses.</td>
<td>G –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical Requirements, ID 102</td>
</tr>
<tr>
<td>31</td>
<td>Are the points made regarding the Natural systems or the mainframe emulator? Which emulator is currently used by DRS?</td>
<td>G –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical Requirements, Usability</td>
</tr>
<tr>
<td>32</td>
<td>What is the requirement for onsite staffing?</td>
<td>H –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Joint Resource Plan</td>
</tr>
<tr>
<td>33</td>
<td>How many Assembler modules need to be converted?</td>
<td>I –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current Technical Profile</td>
</tr>
<tr>
<td>34</td>
<td>What is the total Lines of Code count and breakdown?</td>
<td>I –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current Technical Profile</td>
</tr>
<tr>
<td>35</td>
<td>What is the number of JCLs to be converted?</td>
<td>I –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current Technical Profile</td>
</tr>
<tr>
<td>36</td>
<td>Please provide diagrams of the existing infrastructure, mainframe and open systems environment, and application architecture.</td>
<td>I –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current Technical Profile</td>
</tr>
</tbody>
</table>
Response to Question 36 (continued)

If possible, please provide an Adarep output of the existing Adabas files.

Exhibit I – Current Technical Profile

See response below:

Response to Question 37 (continued): Here is the prod Adarep (general layout):

```
08:18:08          ***** A D A B A S BASIC SERVICES *****       2019-05-03
DBID Prod - Display General DB-Layout - PDRG012

Database Name . ......  ..... DRS-PROD
Database Number ......    ... nnn
Database Version ... ...... 8.4
Database Load Date . . ...... 2019-02-10 15:04:45
Timezone ........ ........ (no default defined)
System Files ............ 170 , 16 , 0 , 0 , 0 , 0 , 0
Maximum Number of Files .. 2000
Number of Files Loaded ... 117
Highest File Loaded ...... 239
Size of RABN ............ 4 Bytes
Current Log Tape Number .. 90
Delta Save Facility ...... Inactive
Recovery Aid Facility .... Inactive
Universal Encoding Sup. .. Inactive

IDEviceI      Total Number of I Extents in Block I DD-Names I
I Type I Blocks / Cyle. I From To I I
---------I-------------------I -------------------I I
I I I I I I
ASSO I 8393 I 5945388 33030 I 1 5945388 I DDASSOR1 I
I I I I I I
DATA I 8393 I 3304618 110154 I 1 3304618 I DDDATAR1 I
I I I I I I
WORK I 8393 I 10498 350 I 1 10498 I I
```
Here is the QA Adarep (general layout):

08:21:16  ***** A D A B A S  BASIC SERVICES *****  2019-05-03

DBID QA  - Display General DB-Layout -  PDRG012

Database Name .......... DRS-QUAL
Database Number .......... nnn
Database Version .......... 8.4
Database Load Date ...... 2019-02-10 13:23:22
Timezone ............... (no default defined)
System Files ............ 5 , 4 , 0 , 0 , 0 , 0 , 0
Maximum Number of Files .. 2000
Number of Files Loaded ... 122
Highest File Loaded ...... 1100

Size of RABN ............ 4 Bytes
Current Log Tape Number .. 87
Delta Save Facility ...... Inactive
Recovery Aid Facility .... Inactive
Universal Encoding Sup. .. Inactive

<table>
<thead>
<tr>
<th>IDeviceI</th>
<th>Total Number of I Extents in Block</th>
<th>I DD-Names I</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Type I Blocks / Cyls. I From To I I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASSO I 8393 I 582828 3238 I 1 582828 I DDASSOR1 I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA I 8393 I 200278 6676 I 1 200278 I DDDATAR1 I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WORK I 8393 I 2998 100 I 1 2998 I DDWORKR1 I</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Here is the DEV/test Adarep:

08:23:35  ***** A D A B A S  BASIC SERVICES *****  2019-05-03

DBID DEV  - Display General DB-Layout -  PDRG012

Database Name .......... DRS-TEST
Database Number .......... nnn
Database Version .......... 8.4
Database Load Date ...... 2019-02-10 13:39:28
Timezone ............... (no default defined)
System Files ............ 5 , 4 , 0 , 0 , 0 , 0 , 0
Maximum Number of Files .. 2000
Number of Files Loaded ... 128
Highest File Loaded ...... 1100

Size of RABN ............ 4 Bytes
Current Log Tape Number .. 87
Delta Save Facility ...... Inactive
Replication Facility ..... Yes
Recovery Aid Facility .... Inactive
Universal Encoding Sup. .. Inactive

<table>
<thead>
<tr>
<th>IDeviceI</th>
<th>Total Number of I Extents in Block</th>
<th>I DD-Names I</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Type I Blocks / Cyls. I From To I I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASSO I 8393 I 539988 3000 I 1 539988 I DDASSOR1 I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA I 8393 I 149998 5000 I 1 149998 I DDDATAR1 I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WORK I 8393 I 2998 100 I 1 2998 I DDWORKR1 I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Exhibit Reference</td>
<td>Answer</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Can you provide a list of all SAG software and their versions currently in use at DRS? Similarly, please provide a list of all none SAG products and their versions currently used at DRS | Exhibit I – Current Technical Profile, Section 2                                      | **Owned by Mainframe Service Provider:**  
- Natural version 8.2.7.5  
- Adabas version 8.4.2.0  
- Adabas Online System version 8.4.2.0  
- Adabas Replication Facility version 3.5.4.0  
- EntireX Communicator version 9.10.0.0  
- Natural Development Facility version 8.2.3.0  
- Natural Optimizer Compiler version 8.2.7.0  
- Natural Security version 8.2.7.5  
- Predict version 8.3.1.0  
**Owned by DRS:**  
- NaturalOne version 10.1  
- Adabas SQL Gateway (Connx) version 12.00.16047 |
| You state that there are 561 partitioned data sets. What are they used for? | Exhibit I – Current Technical Profile, Section 3                                      | Endevor, CA7, EOS (utilities). Most are associated with individual programmers. Eighty partitioned data sets will be moved forward, the rest will be left. |
| Regarding the 379 VSAM files, how many, if any, will be part of the rehosting scope? | Exhibit I – Current Technical Profile, Section 3                                      | None.                                                                                           |
| Will it be required to migrate the databases of all 7 environments as is? | Exhibit I – Current Technical Profile, Section 3 Adabas databases                    | Yes.                                                                                           |
| In the summary of the Natural program entities you don't mention maps. Are they counted under objects? | Exhibit I – Current Technical Profile, Section 3                                      | Yes, they are under objects.                                                                    |
| There is no mention of Natural entities in the development environment. Are these to be rehosted? If so, please state their quantities. | Exhibit I – Current Technical Profile, Section 3                                      | Yes. The numbers presented for the production environment are the base number for all the other environments. |
| Can you provide a LIST COUNT * of the entities from the Natural libraries? | Exhibit I – Current Technical Profile, Section 3                                      | Available Summary LIST COUNT information is provided in Exhibit I – Current Technical Profile, Section 3. And here is a more detailed list: |
45. It states that there are 3 Adabas databases with the same number of Adabas files: Production, Tahiti, and Fiji. Are the latter two DRPs and contain copies of the production DB?

Exhibit I – Current technical profile, Section 3, Summary of Current Adabas/Natural Environment

Yes, but with greatly reduced record sets.

46. Amongst the mainframe systems to be rehosted, are there any systems that are isolated from interaction with the other mainframe systems?

Exhibit I – Current technical profile, Section 4

No

47. Please elaborate on any online interfaces between the applications to be rehosted and those already existing on the open platform.

Exhibit I – Current technical profile, Section 4

All online interfaces are constructed using Entire-X and Natural Web service for the online interfaces.
<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>The RFP States that “The Bidder must have a minimum of five years’ experience migrating IBM legacy applications off mainframe technology into Linux server environments. Bidder must have migrated Adabas/Natural within a minimum of three projects. We assume that this requirement encompasses the entire bidder team (both prime and sub) experience. Can DRS confirm?</td>
<td>RFP – Section 1.6, Minimum Qualifications</td>
<td>The primary Bidder must meet all minimum qualifications.</td>
</tr>
<tr>
<td>49</td>
<td>Architecture, services, and information security design will use STANDARD NO. 141.10 Securing Information Technology Assets as guidance. Is the proposed architecture subject to any other compliance regulations – e.g., IRS/SSA 1075, HIPAA?</td>
<td>Exhibit B – Scope of Services, Section 1.1 Item 10</td>
<td>No, DRS is not subject to other compliance regulations.</td>
</tr>
<tr>
<td>50</td>
<td>The RFP states “The resulting Project Schedule will be maintained in Microsoft Project by DRS during the Project Term and will be updated in joint status meetings.” Please confirm that once the schedule is built who will “maintain” it, DRS or the contractor?</td>
<td>Exhibit B – Scope of Services, Section 1.1 Phase 1 – Planning Deliverable ID 2.2.2 Project Schedule</td>
<td>DRS will maintain the project schedule.</td>
</tr>
<tr>
<td>51</td>
<td>The RFP states that the “Contractor will gather both functional and non-functional business and technical requirements in accordance with the Requirements Management Plan.” Since this is a migration from the mainframe to Linux could DRS provide examples of what “other” type of requirements could be gathered outside of the basic migration such as SOA requirements? Is this deliverable for the future modernizations post go live?</td>
<td>Exhibit B – Scope of Services, Section 3.2 Phase 2 – Analysis and Detailed Systems Review/Inventory Deliverable ID 2.3.4 Gather Requirements</td>
<td>SOA analysis will be done after the mainframe migration (“post go live”). However, print management, Data migration needs (packed data, signed decimal, etc.), transference of CA7 run-schedules, RACF security profiles, Current software-management (n2O), etc, will need requirements and analysis.</td>
</tr>
<tr>
<td>52</td>
<td>In Exhibit B Scope of Services Section 3.5 Phase 5 Deployment lists 2.6.2 UAT Readiness Report and in Exhibit E, Questionnaire Section 1 item F numbers (ii) UAT Readiness Report and (Viii) list a Test Readiness Report. Please clarify if these are the same deliverable. If they are not the same, please clarify how they are different.</td>
<td>Exhibit B – Scope of Services, Section 3.5 Phase 5 – Deployment</td>
<td>They are the same deliverable. DRS will amend Exhibit E Questionnaire to correct the error.</td>
</tr>
<tr>
<td>53</td>
<td>In Exhibit B Scope of Services Section 3.5 Phase 5 Deployment lists 2.6.4 UAT Results Report and in Exhibit E, Questionnaire Section 1 item F numbers (ix) list a User and System Acceptance Test Report. Please clarify if these are the same deliverable. If they are not the same, please clarify how they are different.</td>
<td>Exhibit B – Scope of Services, Section 3.5 Phase 5 – Deployment&lt;br&gt;Exhibit E – Questionnaire, Section 1 Item F</td>
<td>They are the same deliverable. DRS will amend Exhibit E Questionnaire to correct the error.</td>
</tr>
<tr>
<td>54</td>
<td>The RFP states “The post-implementation support during the Stabilization Period will consist of technical and end-user support.” Please clarify “end-user support”.</td>
<td>Exhibit B – Scope of Services, Section 3.6 Phase 6 – Stabilization and Closeout</td>
<td>In this context, end user refers to the IT team testing and supporting these applications and emulator support for business team members.</td>
</tr>
<tr>
<td>55</td>
<td>The RFP states that DRS will have an external Quality Assurance and IV&amp;V vendor. Has that vendor been selected? If so which vendor?</td>
<td>Exhibit B – Scope of Services, Section 4.2 External Quality Assurance and IV&amp;V Responsibilities</td>
<td>The external Quality Assurance and IV&amp;V vendor has not been selected at this time.</td>
</tr>
<tr>
<td>56</td>
<td>The RFP states “In a separate double-sided document, no more than 60 pages in length, describe your proposed Solution.” Please clarify does this mean 30 double sided (which results in 60 pages) or is this 60-double sided (which results in 120 pages)?</td>
<td>Exhibit E – Questionnaire, Section 1</td>
<td>Sixty pages of content. Either 60 pages single-sided or 30 pages double-sided are acceptable.</td>
</tr>
<tr>
<td>57</td>
<td>The RFP states “adherence to various industry integration standards”. Is that in relation to data integration standards such as XML or JSON or system Integration standards such as ITIL?</td>
<td>Exhibit E – Questionnaire, Section 2, Item i</td>
<td>Integration standards include all security considerations, data transfer considerations, protocols, XML/JSON, methodology (e.g. SOAP/REST), RPC considerations, etc.</td>
</tr>
<tr>
<td>Question</td>
<td>Exhibit</td>
<td>Answer</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>58 This exhibit does not include a place for Hardware or Hosting costs. We assume that hardware and hosting is determined in Phase 2 activities, therefore should not be included in this bid. Please confirm.</td>
<td>Exhibit F – Fee Proposal</td>
<td>Hardware and hosting costs are not included. The hosting environment will be determined in Phase 2 and documented in Scope of Services document 2.3.3 Server Hosting Analysis and Recommendation. DRS will procure the hosting environment separately from this procurement.</td>
<td></td>
</tr>
<tr>
<td>59 If the software licensing and maintenance cost is dependent on hosting such as cloud licensing versus on-prem or core licensing how should that be reflected?</td>
<td>Exhibit F – Fee Proposal</td>
<td>If the cost of software licensing and maintenance is dependent on the hosting method, clearly state the assumptions about hosting along with the cost proposed. If a solution could be offered either cloud or on-prem provide both costs for consideration.</td>
<td></td>
</tr>
<tr>
<td>60 Does DRS have the mechanism to purchase third party products that are being proposed or should those be included in the Fee Proposal?</td>
<td>Exhibit F – Fee Proposal</td>
<td>Third party product fees should be included in the Fee Proposal.</td>
<td></td>
</tr>
<tr>
<td>61 Do the existing DRS Natural applications provide for spell check functionality? If so, how is this being accomplished?</td>
<td>Exhibit G – Technical Requirements, Usability, ID 98</td>
<td>No, this is done by the Reflections emulator.</td>
<td></td>
</tr>
<tr>
<td>62 Do the existing DRS Natural applications provide for scratch pad functionality? If so, how is this being accomplished?</td>
<td>Exhibit G – Technical Requirements, Usability, ID 101</td>
<td>No, it is done through the Reflections emulator.</td>
<td></td>
</tr>
<tr>
<td>63 Which usability requirements are specific to only the code development interface?</td>
<td>Exhibit G – Technical Requirements, Usability</td>
<td>Interactive help is specific to only the code development interface.</td>
<td></td>
</tr>
<tr>
<td>64 Which usability requirements are specific to the end-user interface? As the applications are to be re-hosted as-is, are all end-user usability requirements available in the existing DRS applications?</td>
<td>Exhibit G – Technical Requirements, Usability</td>
<td>This is focused on the business end user. All of this functionality is currently available through the Reflections emulator.</td>
<td></td>
</tr>
<tr>
<td>65 What is the total number of concurrent Adabas/Natural users?</td>
<td>Exhibit I – Current Technical Profile, Section 1 Introduction</td>
<td>DRS’ Adabas/Natural environment includes 353 sessions.</td>
<td></td>
</tr>
<tr>
<td>Q &amp; A</td>
<td>The RFP states that the applications are &quot;Software AG’s Natural Language (~98%), Assembler&quot;. We would like to confirm that the 2% Assembler will be deprecated prior to migration and only Natural application code is part of this migration scope. Please confirm.</td>
<td>Exhibit I – Current Technical Profile, Section 2 Summary of Current Technology Environment</td>
<td>Yes, that is correct.</td>
</tr>
<tr>
<td>66</td>
<td>Are Adabas User Exits in use? If so, please provide a list of them and if any have been customized for use at DRS.</td>
<td>Exhibit I – Current Technical Profile, Section 2 Summary of Current Technology Environment</td>
<td>Only one Adabas User Exit is currently in use. However, that user exit will not be migrated.</td>
</tr>
<tr>
<td>67</td>
<td>Regarding the reference to product &quot;ADASTRIL&quot;, is this a typo which should reference the Treehouse product ADASTRIP?</td>
<td>Exhibit I – Current Technical Profile, Section 2 Summary of Current Technology Environment</td>
<td>Both are Treehouse products. Neither will be migrated into Linux.</td>
</tr>
<tr>
<td>Page</td>
<td>Questions and Answers</td>
<td>Exhibit I – Current Technical Profile, Section 2 Summary of Current Technology Environment</td>
<td>Exhibit I – Current Technical Profile, Section 3 Summary of Current Adabas Natural Environment</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>69</td>
<td>Please provide more information on the use of these utilities in the current mainframe environment and how it affects the integration requirements: Expediter Finalist Endevor Icetool ADASTRIL Fileaid Secure File Transfer (SFT) TRCENGIN Overlay Generation Language (OGL), DFSMS DataMiner Endevor</td>
<td>Here is more information regarding these specific utilities.  - <strong>Expediter</strong> is a debugging tool. Will not be ported/migrated.  - <strong>Finalist</strong> is an address formatting tool. Will need some replacement for this functionality.  - <strong>Endevor</strong> is source code management for JCL and COBOL, and will not be ported/migrated. Will use an open system source management toolset.  - <strong>Icetool</strong> is a dataset utility; expected Linux tools will replace the Icetool functions.  - <strong>ADASTRIL</strong> is a ETL tool, and will not be ported/migrated  - <strong>SFT</strong> is external to mainframe but will need to be available to Linux for file transfers.  - <strong>OGL</strong> is an IBM mainframe zOS function for forms printing, and will require alternative solution(s).  - <strong>DFSMS</strong> is IBM mainframe Systems-Managed-Storage (part of zOS). Expect to use some Linux based file management toolset as replacement.  - <strong>TRCENGIN</strong> is an execution trace facility from CA.  - <strong>DataMiner</strong> is a dataset utility; expecting Linux based data management toolset as substitute.</td>
<td>This was the result of Natural’s LIST COUNT command in the production environment at the time the RFP was composed.</td>
</tr>
<tr>
<td>70</td>
<td>Please confirm the total number of Natural modules to be re-hosted, including Natural maps. DRSMIONL Online 2,377 DRSMIBAT Batch 3,389 DRSCMONL Common 386 Total number of Natural modules: 6,945</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Addendum 1 – Questions and Answers*
*RFP 19-01, Mainframe Rehosting Services*
*Page 15 of 52*
<table>
<thead>
<tr>
<th>Qn</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 71 | **How many datasets are permanent and contain the following Natural data field types as part of the data?**  
  Date (D), Time (T), Packed Numeric (P), Binary (B), Integer (I), Floating (F), Attribute Control (C) or Logical (L)  
  Bidder clarification: Permanent datasets are application datasets that contain special values. To rephrase - are there any sequential or interim batch datasets that need to be migrated, that contain packed numeric/decimal or other fields that would not convert from EBCDIC to ASCII when being transferred with a standard file transfer? If so, how many and what is the volume? | Exhibit I – Current Technical Profile, Section 3 Summary of Current Adabas Natural Environment  
  DRS currently has TPA interface files that contain packed data. DRS is working to convert those files now and anticipates having this complete before a Vendor begins their work. |
| 72 | **How many Natural modules contain NATRJE job submissions?** | Exhibit I – Current Technical Profile, Section 3 Summary of Current Adabas Natural Environment  
  We use a central reusable subroutine to submit RJE from online sessions. |
| 73 | **How many JCL members (including steps) and PROCS (including steps) need to be re-hosted?** | Exhibit I – Current Technical Profile, Section 3 Summary of Current Adabas Natural Environment  
  Approximately 1,045 JCL modules to convert. The step count is 26,125. No PROCES. |
| 74 | **Do your applications make use of Adabas alphanumeric data field redefines using any of the following Natural data types in the redefinition: Date (D), Time (T), Packed Numeric (P), Binary (B), Integer (I), Floating (F), Attribute Control (C) or Logical (L)? Are you able to identify them for conversion purposes?** | Exhibit I – Current Technical Profile, Section 4 Applications  
  Yes, DRS applications make use of Adabas alphanumeric data field redefines. Yes DRS is able to identify them for conversion purposes. |
<table>
<thead>
<tr>
<th>Question</th>
<th>Source</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>With regards to Employer Information System (EIS), since it is slated for replacement by ERA in 2020, does this application still need to be included and estimated in the re-hosting effort?</td>
<td>Exhibit I – Current Technical Profile, Section 4 Applications</td>
<td>No</td>
</tr>
<tr>
<td>Can DRS confirm that the conversion of VSAM files and associated Natural code for the Employer Information System (EIS) will be completed before the re-hosting or at a minimum completed by the DRS application teams?</td>
<td>Exhibit I – Current Technical Profile, Section 4 Applications</td>
<td>Yes</td>
</tr>
<tr>
<td>What methods of communication are used for interfaces utilizing EntireX? For example, Natural RPC, Natural ACI, XML RPC/Web Services, other? For each method, is the communication incoming to DRS, outgoing from DRS or both?</td>
<td>Exhibit I – Current Technical Profile, Section 6 IT Systems External Interfaces</td>
<td>Natural RPC incoming to MF; Natural webservice outgoing from MF.</td>
</tr>
<tr>
<td>Question</td>
<td>Reference</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| What methodology will be used to determine the averages for Performance Standard listed in section 7 PERFORMANCE STANDARDS of Scope of Services? | Exhibit B – Scope of Services, Section 7 Performance Standards | **Average Batch Processing Time:** Duration of time between start and end of batch job execution recorded in system log divided by the number of records processed, averaged across a set of selected batch jobs.  

**Average Interactive On-line Response Time:** Duration of time between submitting and receiving a response for an on-line screen submission, averaged across a set of selected on-line transactions.  

**Average Middleware Response Time:** Duration of time between start and received time recorded in system logs, averaged across a set of selected calls from web Applications to pre/post migrated Applications.  

**Average Time Database Request Spends in the Queue:** Length of time a request is in database queue before being processed, averaged across a set of selected database calls.  

**Average Time a Database Call Takes to Execute:** Duration of time the database takes to process a database call, averaged across a set of selected database calls. |
| Do the existing (in scope) applications, code and data meet security policies and standards (e.g., WA State Enterprise Security Policy 141, standard 141.10 and DRS policy ITS 3) mentioned in the RFP (e.g., Exhibit B Scope of Services and Exhibit C Sample Contract)? | Exhibit B – Scope of Services  
Exhibit C – Sample Contract | Yes, to the degree possible. Mainframe cannot be fully compliant (for example, 8 character ID and Password limitation). Desire is for Linux to resolve these limitations so that full compliance is achieved. |
| Will DRS consider alternative approaches to managing the project? | Exhibit B – Scope of Services | Not at this time. |
| Will DRS consider waivers for minimum qualifications? | RFP | No. |
VENDOR QUESTIONS AND ANSWERS

ATTACHMENT 1
DRS POLICIES
<table>
<thead>
<tr>
<th>DRS Policy Number</th>
<th>DRS Policy Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRS-ASD-OS-9</td>
<td>Lost or Stolen Property</td>
</tr>
<tr>
<td>DRS-GENL-4</td>
<td>Using Social Media</td>
</tr>
<tr>
<td>DRS-HR-1</td>
<td>Understanding Ethics in Public Service</td>
</tr>
<tr>
<td>DRS-HR-2</td>
<td>Preventing Workplace Harassment</td>
</tr>
<tr>
<td>DRS-HR-3</td>
<td>Reporting Improper Governmental Action (Whistleblower)</td>
</tr>
<tr>
<td>DRS-HR-4</td>
<td>Maintaining an Alcohol and Drug-Free Workplace</td>
</tr>
<tr>
<td>DRS-HR-6</td>
<td>Maintaining a Smoke-Free Environment</td>
</tr>
<tr>
<td>DRS-ASD-OS-1</td>
<td>Establishing and Controlling Access to DRS Facilities</td>
</tr>
<tr>
<td>DRS-HR-S&amp;H-1</td>
<td>Preventing Violence in the Workplace</td>
</tr>
<tr>
<td>DRS-ISD-1</td>
<td>Using Electronic Communication Systems</td>
</tr>
<tr>
<td>DRS-ISD-3</td>
<td>Providing Information Technology Security</td>
</tr>
<tr>
<td>DRS-ISD-ITS-3</td>
<td>Using Wireless Communication Devices to Conduct DRS Business</td>
</tr>
<tr>
<td>DRS-IT-4</td>
<td>Controlling Information Technology Access</td>
</tr>
</tbody>
</table>
DRS-ASD-OS-9

LOST OR STOLEN PROPERTY

This policy is in accordance with the State Administrative & Accounting Manual, published by the Office of Financial Management (SAAM 30.40.80), and applies to all employees of the Department of Retirement Systems.

1. Employees Are Responsible for All Equipment in Their Immediate Areas

   Employees are responsible for immediately reporting lost or stolen state property.

2. Employees Are Responsible for Completing a Property Disposal Request Form

   When state property is determined to be lost or stolen, completion of a Property Disposal Request form is required.
This policy applies to all Department of Retirement Systems (DRS) Team Members.

1. **Purpose And Justification**

Social media tools are a powerful method of communication and are used by millions of individuals and groups to share information and connect with others. DRS will use social media tools and channels when appropriate to enhance communication and engagement with customers, partners, stakeholders and others to support its mission, key goals and core processes.

This policy describes how the agency will use social media and gives DRS Team Members information regarding permitted use of social media while at work.

**DEFINITIONS:**

**Social Media** – is an umbrella term encompassing various activities that integrate technology, social interaction and content creation. There are numerous forms of social media, such as blogs, wikis, photo and video sharing, podcasts, social networking, ideation, bookmarking, discussion boards, gamification, and virtual worlds. Examples of social media include, but are not limited to, Facebook, LinkedIn, Twitter, Blogger, YouTube, Flickr, Instagram, Reddit, SnapChat and Wikipedia.

**Content** – consists of text, articles, photographs, videos, applications, infographics, links, graphic elements, messages and comments.

2. **Management Of DRS Social Media Accounts**

The DRS Communications Team, at the direction of the Communications Director or designee(s), is responsible for establishing and supervising all social media accounts for the agency. These accounts are considered agency tools. DRS-sponsored social media accounts may only be established with approval from the Communications Director.

The DRS Communications Team, at the direction of the Communications Director or designee(s), shall establish, monitor and administer policies or procedures for appropriate conduct, content, security, and records retention on all social media accounts for the agency.

The management of content on DRS-sponsored social media accounts is limited to the DRS Communications Team. Only Communications Team Members are authorized to log on to and/or post, edit or remove content on DRS-sponsored social media accounts. DRS Team Members may not, as an agency representative, originate posts on agency social media platforms, nor may they respond to messages or comments transmitted to DRS via agency social media platforms.
The DRS Communications Team will monitor all content posted to agency social media platforms by outside sources. DRS reserves the right to delete content from and block access to agency social media platforms in instances where activity is in violation of agency policies.

3. **Team Member Access To Social Media**

DRS Team Members may use social media only for business (work-related) purposes. Business purposes are defined as furthering specific job responsibilities, viewing agency-managed social media, or professional networking. Reasonable use in this manner is permitted, so long as it is in accordance with DRS-HR-1 Understanding Ethics In Public Service and DRS-ISD-1 Using Electronic Communication Systems.

No Team Member may use state resources, including but not limited to work time, computers and software programs, for personal use of social media. There is no *de minimis* personal use of social media allowed.

Social media shall not be used to transmit information or knowingly connect to sites for an unlawful or prohibited purpose, including, but not limited to, the following examples:

- Discrimination on the basis of sex, race, creed, color, gender, religion, age, marital status, national origin, sensory, mental, or physical disability, sexual orientation or veteran status
- Sexual harassment or sites containing sexual content
- Transmission of obscene materials
- Infringement on any copyright
- Expression of any campaign, political or religious beliefs
- The conduct of a personal, outside business, or other financial benefit or gain

4. **Privacy**

The Internet is an unsecured publicly accessible network. Team members should have no expectation of privacy in the use of Internet resources, including social media. Team members should also be aware that using social media for business purposes may result in their social media account being subject to public records and disclosure requirements. Social media shall not be used to distribute privileged or confidential material.
UNDERSTANDING ETHICS IN PUBLIC SERVICE

This policy applies to all Department of Retirement Systems (DRS) team members.

DEFINITIONS:

**Family member** – A team member’s spouse, registered domestic partner, child, stepchild, foster child, grandchild, parent, grandparent, sibling, aunt, uncle, niece, nephew, cousin, and relatives by marriage or former marriage.

**Honorarium** – Money or something of economic value that is offered to a team member for providing a speech, appearance, article or other similar item or activity in connection with his or her official duties.

**Hosted reception** – A social function involving a diverse group of people, some of whom are regulated and/or provide goods and services to the agency and others who are not, that does not involve a sit-down meal.

**Household members** – Persons who reside in the same home who have reciprocal duties to and do provide financial support for one another. Does not include persons sharing the same house when the living style is that of a dormitory or other type of shared dwelling.

**Person** – For purposes of this policy, a person is defined as any individual, partnership, association, corporation, firm, institution or other entity, whether or not operated for profit.

**Personal benefit or gain** – The use of a state resource, available to an individual only because he or she is a state employee, to benefit him or her personally, to personally benefit another person, and/or avoid a personal cost or expense. Examples include, but are not limited to:

- Using the state SCAN system to make a personal long-distance call
- Using hotel/motel reward points earned during official travel for personal travel (if the employee participated in the selection of the hotel/motel used during official travel)
- Receiving a government rate for a hotel while not on official business (unless the rate is offered to all government employees, whether or not they are on official business)
- Using a state computer to shop online
- Posting information to advertise another person’s business
- Using a state copy machine to make copies of personal documents for the team member or another person that are not related to DRS business
- Using state e-mail to send or receive information regarding personal interests (e.g., home remodel, car repairs, utility issues, etc.)

**Regulatory agency** – Any state board, commission, department or officer authorized by law to conduct adjudicative proceedings, issue permits or licenses, or to control or affect interests of identified persons.
**State resources** – Includes, but is not limited to: work time, computers, software programs (including e-mail and Internet), SCAN, telephones, employees, copiers, fax machines, office supplies, furniture, postage, vehicles, publications, and facilities.

1. **Purpose Of Policy Is Defined**

As public employees, all team members are expected to demonstrate the highest standard of fairness, honesty, and compliance with both the spirit and the letter of the law in the performance of their job duties. It is the responsibility of every team member to understand their obligations regarding ethical behavior and to conduct themselves in a fair, impartial, and ethical manner.

2. **Specific Actions Are Restricted**

2a. **Conflicts Of Interest** *(RCW 42.52.020)*

A team member may not use his or her job to gain special privileges, financial benefits or other advantages for themselves, their family members or their friends.

To eliminate even the perception of a conflict of interest, a team member cannot provide service or perform any functions involving changing of data, processing of information, or conducting business transactions for family members, household members, or individuals with whom he or she has a significant personal relationship.

No team member will perform any transaction involving his or her own personnel information (with the exception of updates allowed through a self-service option available to all state employees), agency record or retirement account, no matter how insignificant the transaction may seem.

2b. **Use of State Resources for Personal Benefit and/or Gain** *(RCW 42.52.160)*

No team member may use state resources under his or her control, direction, or in his or her official custody for personal benefit or gain or to benefit another person. The *de minimis* standard regarding the use of state resources does not apply when those resources are used to benefit a team member personally, to personally benefit another person, and/or to avoid a personal cost or expense.

2c. **Acceptance of Gifts** *(RCW 42.52.140)*

A team member may not ask for, receive or agree to receive anything of value – either directly or indirectly – for doing his or her job or if it could be perceived to influence or reward his or her vote, judgment, action, or inaction. Additionally, a team member may not accept compensation from or participate in a business relationship with a person or vendor that is regulated by, has a contract with or is seeking to provide goods and services to the agency.

*Food and Beverage* (EEO Advisory Opinions 96-02 and 96-06)
A team member is free to accept unsolicited token beverage items, such as water, coffee, tea or juice while performing official duties, provided the unsolicited items are generally made available by the business, free of charge, to its own employees, customers, and visitors.

At no time may a team member accept gifts of food or beverage from persons or vendors who are engaged in regulatory or contractual matters with the agency or are seeking to provide goods and services to the agency.

In certain circumstances, a team member may accept a gift of food and/or beverage. These circumstances are limited to:

- Food and/or beverage received as part of training paid for by the agency
- Infrequent offers of food and/or beverage as part of the ordinary course of a meal where attendance is related to the performance of official duties (provided the donor is not engaged in regulatory or contractual matters with the agency)
- Food and/or beverage provided as part of a hosted reception

2d. Acceptance Of Honoraria (RCW 42.52.130)

Unless specifically authorized by the Director or designee, a team member cannot accept an honorarium for a speech or article given in connection with his or her official DRS duties.

2e. Political Activities (RCW 42.52.180)

No team member may use state resources, either directly or indirectly, for the purpose of assisting a campaign for election of a person to an office, for the promotion of or opposition to a ballot proposition, or to view or discuss his or her own political beliefs. Any team member with the authority to direct, control, or influence the actions of other team members may not knowingly acquiesce to the use of state resources to carry out political activities.

2f. Transactions with the State (RCW 42.52.040)

Except in the course of official duties, a team member may not assist another person, whether compensated or not, in a transaction with the state in which he or she participated.

No team member, even in his or her official DRS capacity, may participate in a transaction with a person or entity with which he or she is also an employee, member, or in which he or she owns a beneficial interest.

2g. Employment After Public Service (RCW 42.52.080)

No former DRS team member may accept an offer of employment or receive compensation from an employer if:

- he or she knows or has reason to believe that the offer was intended, completely or in part, directly or indirectly, to influence the performance of his or her job duties
the circumstances would lead a reasonable person to believe the offer was made or compensation given for the purpose of influencing the performance or non-performance of his or her job duties during his or her state employment

2.g.1. One-Year Restriction

A former DRS team member may not accept employment or compensation from an employer within one year of termination of state employment if all three of the following conditions are present:

- The DRS team member, during the two years immediately preceding termination of state employment, negotiated or administered contracts for the state and/or agency with that employer or was in a position to make discretionary decisions regarding the negotiation or administration of such contracts
- The contract(s) had a total value in excess of $10,000
- The duties which the former DRS team member would be required to perform for the new employer would include fulfilling or implementing those same contracts

2.g.2. Two-Year Restriction

For the two-year period following his or her termination of state employment, a former DRS team member cannot have a beneficial interest, either direct or indirect, in a contract which was expressly authorized or funded by specific legislative or executive branch action in which he or she participated.

DRS will not willingly or knowingly do business with a former state employee who is or has been in violation of this policy or if doing so would cause either of the parties to be in violation of Chapter 42.52 RCW.

3. Limited Use Of Team Member Time And Agency Resources May Be Authorized By The Director (WAC 292-110-020(2)(b)(i))

The DRS Director may authorize the limited use of team members’ time and agency resources to support, promote, or solicit for charitable activities, including but not limited to: Adopt-A-Family and Combined Fund Drive.

4. Disclosure Of Confidential Information Is Explained

No team member may disclose confidential information to any person not entitled to or authorized to receive it or for his or her personal benefit or gain or to benefit another person.

A team member may not accept employment or engage in a business or professional activity that he or she reasonably expects would cause him or her to make an unauthorized disclosure of confidential information accessible to him or her due to employment with DRS.

A team member may not intentionally conceal a record if he or she knew it was required to be released under Chapter 42.52 RCW, had a personal obligation to release it and failed to do so.
5. **Issues Are Reported**

If a team member becomes aware of a potential violation of any portion of this policy, he or she will promptly report it to his or her team leader or the Human Resources & Office Services Director or designee (see DRS-HR-1.1 *Reporting Potential Policy Violations*). All reports will be immediately investigated by the Human Resources & Office Services Director or designee and findings reported to the Director or designee.

A team member also has the right to file a complaint with the Executive Ethics Board ([RCW 42.52.410](https://app.leg.wa.gov/RC/RCW/42.52.410)).

6. **Training Will Be Provided**

All new DRS team members will be made aware of this policy during New Employee Orientation. This policy and procedure will be available on the DRS intranet for team members, volunteers, and contractors. It will also be made available to the public upon request.
This policy applies to all Department of Retirement Systems (DRS) team members.

DRS is committed to providing all individuals with a working environment free from harassment, intimidation, and discrimination. Harassment is considered misconduct, undermining the integrity of the employment or contract relationship and is detrimental to the individual(s) to whom it occurs, debilitating morale, and interfering with the work productivity of its victim(s) and co-worker(s). Harassment of any individual, as defined below, is prohibited and will not be tolerated in the workplace.

1. **Workplace Harassment Is Defined**

1.a. Harassment

Unlawful, unwelcome, or unprofessional conduct toward or about an individual based on their age, color, creed, disability, marital or familial status, national origin, political activity, race, religion, sex, sexual orientation or genetic information constitutes harassment if it unreasonably interferes with an individual’s work performance or creates an intimidating, hostile or offensive work environment.

1.b. Sexual Harassment

Behavior that is sexual in nature, which is unwelcome and personally offensive to the recipient of the action. Sexual harassment is defined and prohibited by state and federal anti-discrimination laws where:

- Submission to such conduct is made, either explicitly or implicitly, a term or condition of an individual’s employment
- Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual (quid pro quo)
- Such conduct has the purpose or effect of unreasonably interfering with an individual’s work performance or creating an intimidating, hostile or offensive working environment

2. **Harassing Behavior Is Prohibited**

Prohibited behavior includes but is not limited to:

- Unwelcome touching, including hugs, shoulder rubs, or repeatedly brushing against someone
- Blocking or impeding someone’s movement
- Dirty jokes, sexually suggestive comments, pictures, cartoons, diagrams or objects, obscene gestures or sexual innuendo
- Unwelcome staring, leering, winking or suggestive looks
- Excessive unwanted attention, such as flowers, personal letters and notes, or compliments
- Unwelcome and repeated requests for sexual favors or social contact, whistling and catcalls
- Rumors
- Jokes, teasing, name-calling, pranks, or otherwise inappropriate behavior that reflects bias
Individuals who believe they are being subjected to harassing behavior are encouraged to notify the person, either verbally or in writing, that their conduct is unwelcome.

3. **Reporting Incidents Of Workplace Harassment Is Required**

Any individual who observes, becomes aware of, or who has been or is being subjected to workplace harassment must promptly report the behavior to their team leader or the Human Resources & Office Services Director/designee immediately.

Individuals who believe they have been or are being subjected to harassment in the workplace also have the right to file a complaint with the Washington State Human Rights Commission or the federal Equal Employment Opportunity Commission.

4. **Team Leaders’ Responsibilities Are Defined**

Every team leader must take reasonable steps to prevent harassment from occurring in the workplace. This includes, but is not limited to:

- Promoting and encouraging a working environment that is free from harassment and discrimination
- Modeling the behavior expected of team members
- Ensuring his or her team members are aware of this policy and the procedure for reporting allegations of workplace harassment
- Take prompt action to stop inappropriate behavior

Should a team leader become aware of alleged workplace harassment, he or she must promptly notify the Human Resources Director/designee.

5. **Investigations Are Conducted By the Human Resources Director/Designee**

All reports of workplace harassment will be promptly investigated by the Human Resources Director/designee. Prompt, remedial action will be taken to address unlawful behavior.

Investigative procedures may vary depending on the nature and extent of the reported behavior and the context in which the alleged behavior occurred.

6. **Team Members Will Cooperate in All Phases Of The Investigative Process**

In order to properly investigate a complaint of workplace harassment, DRS team members will cooperate with the Human Resources Director/designee in all phases of the investigative process.

7. **Confidentiality Is Maintained To The Fullest Extent Possible**

Although a guarantee of confidentiality or anonymity cannot be made, discretion will be exercised in all aspects of the reporting and investigative process. Information about the complainant and respondent
and the incidents giving rise to the complaint will be revealed only as investigatory and disciplinary processes require.

8. **Non-Disclosure Agreements Are Prohibited**

No individual will be required, as a condition of employment, to sign a non-disclosure agreement, waiver, or other documentation that would prevent him or her from disclosing sexual harassment or sexual assault, whether it occurs in the workplace or at work-related events coordinated by or through DRS, between team members, between the agency and a team member, off the employment premises.

9. **Retaliation Against Individuals For Reporting Workplace Harassment Will Not Be Tolerated**

No individual should be discriminated or retaliated against for reporting workplace harassment or for providing information as part of an investigative process. The agency will take prompt, appropriate corrective or disciplinary action for acts of retaliation, up to and including dismissal from employment.

10. **Awareness Training Is Required**

All new team members will be made aware of this policy and the procedure for reporting allegations of workplace harassment during New Employee Orientation. Contractors and volunteers with DRS will be made aware of the policy and the requirement for compliance. This policy and procedure will be available on the DRS intranet and will also be made available to the public upon request.

DRS will provide training for all team members on workplace harassment awareness and prevention. New team members will complete training within the first six months of employment. Refresher training for team members and team leaders will be provided in accordance with state requirements.
DRS-HR-3
REPORTING IMPROPER GOVERNMENTAL ACTION (WHISTLEBLOWER)

This policy applies to all Department of Retirement Systems (DRS) employees.

DEFINITIONS

Good faith – A state government employee providing the information or report of improper governmental action has a reasonable basis in fact for reporting and providing the information, is not knowingly reporting malicious, false or frivolous information, is not providing information with a reckless disregard for the truth, is not knowingly omitting relevant information, and is acting in good faith.

Gross mismanagement – The exercise of management responsibilities in a manner grossly deviating from the standard of care or competence that a reasonable person would observe in the same situation.

Gross waste of funds – To spend, use funds, or to allow funds to be used without valuable result in a manner grossly deviating from the standard of care or competence that a reasonable person would observe in the same situation.

Improper governmental action – Any action by a state government employee undertaken in the performance of his or her official duties which:

1. Is a gross waste of public funds or resources;
2. Is in violation of federal or state law or rule, if the violation is not merely technical or of a minimum nature;
3. Is of substantial and specific danger to the public health or safety;
4. Is gross mismanagement; or
5. Prevents the dissemination of scientific opinion or alters technical findings without scientifically valid justification, unless state law or a common law privilege prohibits disclosure.

Improper governmental action does not include personnel actions for which other remedies exist, any action which may be taken under chapter 41.06 RCW, or other disciplinary action except as provided in chapter 42.40.030 RCW.

Use of official authority or influence – Includes threatening, taking, directing others to take, recommending, processing or approving any personnel action such as an appointment, promotion, transfer, assignment (including but not limited to duties and office location), reassignment, reinstatement, restoration, reemployment, performance evaluation, determining any material changes in pay, provision...

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 32 of 52
of training or benefits, tolerance of a hostile work environment, or any adverse action under chapter 41.06 RCW, or other disciplinary action.

Public official – The attorney general’s designee or designees; the director of DRS; the DRS human resources manager; or the executive ethics board.
**Whistleblower** – A state government employee who:

1. In good faith, reports an allegation of improper governmental action to the auditor or other public official, initiating an investigation; or
2. Is perceived by the employer, whether they did or did not, as reporting alleged improper governmental action to the auditor or other public official or providing information in connection with an investigation; or
3. In good faith identifies rules warranting review or provides information to the rules review committee, or is perceived to have done so but has not.

1. **Allegations of Improper Governmental Action Are Reported**

   Any state government employee may report an assertion of improper governmental action through the Whistleblower Program or to a public official. The written report must be received within one year of the occurrence of the asserted action. A public official receiving an assertion of improper governmental action must report it to the State Auditor’s Office within 15 calendar days of receipt.

   The written report should include:

   - A detailed description of the improper governmental action(s);
   - The name(s) of the employee(s) involved;
   - The agency, division, date and location where the action(s) occurred;
   - If known, the specific law or regulation that has been violated;
   - Any other details, such as witnesses, documents and evidence, to assist the State Auditor in conducting an investigation; and
   - The whistleblower’s name, home address, and phone number (optional).

   State law requires the identity or identifying characteristics of the whistleblower be kept confidential at all times, unless the person consents to disclosure by written waiver or by acknowledging his or her identity as a witness who provides information in an investigation.

2. **State Auditor’s Office Determines Scope of Investigation**

3. **Workplace Reprisal or Retaliatory Action Is Prohibited**

   Workplace reprisal or retaliatory action against an employee who, in good faith, reports or provides information during an investigation into an allegation of an improper governmental action is strictly prohibited.
No employee may use his or her official authority or influence to intimidate, threaten, coerce, command or influence the right of an individual to disclose allegations of an improper governmental action to the State Auditor.

4. Summary of Whistleblower Act Is Provided to Staff

Human Resources will provide every new DRS employee that is first entering public employment with a written summary of the Whistleblower Act and a copy of this policy. Notification of the procedures and protections of the Whistleblower Act will be provided to all DRS employees on an annual basis.
DRS-HR-4
MAINTAINING AN ALCOHOL AND DRUG-FREE WORKPLACE

This policy applies to all Department of Retirement Systems (DRS) team members.

DEFINITIONS

Alcohol – Any beverage or substance as defined in RCW 66.04.

Drugs – All controlled substances that are illegal under either state or federal law, as well as unlawful use of prescription medications (see RCW 69.41, RCW 69.50 and RCW 69.51A).

Prescription medications – Any drug required by state law or regulation of the State Board of Pharmacy to be dispensed only by prescription or restricted to use by practitioners as defined in RCW 69.41.

1. DRS is Committed to Maintaining an Alcohol and Drug-Free Workplace

DRS is committed to providing all team members with a safe and healthful work environment free from the presence, use and effects of alcohol and drugs. DRS will not tolerate the unlawful use, possession, solicitation, purchase, transport, delivery, dispensing, distribution, manufacture or sale of drugs or alcohol by any team member while in a state vehicle, on agency premises or while on official state business.

2. Team Members Must Be Fit for Duty

All team members are required to report for work in a condition fit to perform their duties, unimpaired by any current or recent use of alcohol and/or drugs. During working hours, team members shall not use, consume or be under the influence of alcohol and/or drugs that may impair their job performance.

A team leader who believes a team member is impaired by drugs and/or alcohol or has engaged in prohibited activities must immediately relieve the team member of his or her job duties and notify the HR and Office Services Director or designee and the appropriate chain-of-command. Any team member who has reason to believe another team member is impaired by drugs and/or alcohol or has engaged in prohibited activities on the job must notify his or her team leader or the HR and Office Services Director/designee immediately.

3. Use of Medication May Require Team Leader Notification

Any team member who is taking physician-prescribed or over-the-counter medication that has a likelihood of affecting job safety or performance must notify his or her team leader immediately. The notification shall include the fact that he or she is taking medication and the side effects of that medication.

4. Referral to Employee Assistance Program May Be Offered

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 36 of 52
Except in the case of drug delivery, solicitation or sale, a team member with a drug and/or alcohol problem will be referred to the Employee Assistance Program (EAP). A referral to the EAP will not impede the agency’s ability to take appropriate action against any team member who violates this policy.
This policy applies to all Department of Retirement Systems (DRS) employees.

**DEFINITION**

Smoking – For purposes of this policy, the term “smoking” refers to the inhaling, exhaling, burning and/or chewing of tobacco-related products and/or equipment, including but not limited to: cigarettes, cigars, pipes, electronic cigarettes, chewing tobacco, and snuff.

1. **Smoking Is Prohibited in All DRS Facilities**

   There is no smoking in any building owned, leased, rented or controlled by DRS.

2. **Smoking Is Prohibited in All State Vehicles**

3. **Smoking Is Limited to Established Breaks and Lunch Periods in Designated Outside Areas**

   Smoking is not allowed in close proximity to any entryway, air intake, or other opening that may allow airflow directly into the building.

4. **Reimbursement May Be Available to DRS Employees Who Participate in a Smoking Cessation Program**

   A DRS employee may receive reimbursement of up to $75 for costs associated with participation in a smoking cessation program. Reimbursement is limited to a one-time basis per employee. Proof of attendance or participation must be provided to receive reimbursement. Reimbursement is not available for persons working under a personal or purchased services contract or persons performing volunteer work for DRS.
establishing and controlling access to drs facilities

this policy applies to all department of retirement systems' (drs) team members and individuals who require access to drs facilities.

1. purpose of the policy is defined

safety and security of team members, member information, and agency systems and equipment are top priorities for the agency. this policy will help ensure that only individuals who have a business-related need will be granted access to a drs facility beyond the general reception area or outside standard access hours, and that individuals will be appropriately and easily identifiable to others while in the building.

2. need for id/access cards and building keys will be determined

all team members will be provided a photo id card that will allow them standard building access during the hours of 6:00 am to 6:00 pm. team members who have a business need for building access outside of these core hours may be granted extended access with team leader approval. access to non-standard areas (e.g., server room, tech support room, cash room, etc.) must be approved by the appropriate appointing authority.

building door keys will be assigned to: 1) leadership team members; 2) team members who are assigned an office; 3) administrative assistants supporting leadership team members; 4) central reception unit (cru); and 5) office services team members.

state auditors, contractors, temporary contract workers, vendors, and maintenance professionals (e.g., heating/cooling system, copy machine repair, etc.) will be issued temporary building access cards by the facilities manager for the duration of their work or assignment.

guests who will be going beyond the general reception area will be issued a temporary visitor badge after signing in at the reception desk. all guests must be escorted by a drs team member at all times.

3. issuance of id/access cards and building keys is closely controlled

the facilities manager or his/her designee will create and issue photo id cards, building access cards and building door keys. all information regarding the issuance of photo id/access cards and keys and the level of access provided will be maintained in the drs facilities security system and key log. all master and spare building keys will be secured by the facilities manager.

a team member or individual who has an id/access card or building key but leaves it at home must request a temporary one-day replacement.

4. id/access cards must be worn by individuals

addendum 1 – questions and answers

rfp 19-01, mainframe rehosting services

page 39 of 52
All team members and other individuals who have ID/access cards must wear them at all times and in a way that is readily visible to others while in a DRS facility.

5. **Lost Or Stolen ID/Access Cards And Keys Must Be Reported Immediately**

Any team member or individual who believes their ID/access card and/or building key has been misplaced, lost or stolen must report it immediately to the Facilities Manager/designee (see DRS-HR-OS-1.2 Reporting Lost, Stolen or Misplaced ID Cards and Keys).

An individual may be charged for replacement costs of lost or stolen cards and keys and, if deemed necessary, costs for changing locks on exterior building doors.

6. **Assigned ID/Access Cards And Building Keys Should Not Be Loaned Or Borrowed**

An ID/access card or building key must always remain in the possession of the team member or individual to whom it is issued. Assigned ID/access cards and building keys should not be borrowed by or loaned to anyone else for their use.

7. **Annual Review Will Be Performed**

Every year, the Facilities Manager/designee will conduct an audit of all issued building keys and notify the HR and Office Services Director if any keys are unaccounted for. A review of team members with non-standard access will also be conducted annually to verify the ongoing business need for continued extended access.

8. **Training Will Be Provided For Individuals With After-Hours Access**

All team members who are granted building access outside of the 6:00 AM to 6:00 PM standard will receive training on building security (e.g., disarming/rearming the building’s alarm, ensuring personal security while in the building, etc.) when they first receive extended access and annually thereafter. Participation in this training is required to maintain extended access.

9. **Extended Access May Be Suspended**

Team members with extended building access who fail to follow established procedures and/or repeatedly cause false alarms with the security system may have their extended access suspended until a review is conducted and refresher training completed.
DRS-HR-S&H-1
PREVENTING VIOLENCE IN THE WORKPLACE

This policy applies to all Department of Retirement Systems (DRS) team members.

DEFINITION

Dangerous Weapon - Any object in a person's possession apparently capable of producing bodily harm, in a manner, under circumstances, and at a time and place that either manifests an intent to intimidate and/or cause fear to other persons, threatens the life of other persons or warrants alarm for the safety of other persons.

Workplace – State office, facility, work site, vehicle or location where an employee conducts state business.

1. Purpose of Policy is Defined

DRS is committed to providing a safe working environment that is free from violence, threats and/or intimidation. Violent behavior is unacceptable in the workplace and will not be tolerated.

Violent behavior includes, but is not limited to:

- Intentional actions that cause physical harm or injury to another person;
- Written or verbal comments or threats, whether direct or implied, that create a reasonable belief of an intent to inflict physical harm to a person or property;
- Harassment or the display of violent or threatening behavior that may result in physical or emotional injury; and/or
- Conduct that arouses fear, hostility, or intimidation.

DRS is also committed to providing support and assistance for any team member who is or who has a family member who is a victim of domestic violence, sexual assault, or stalking.

2. Incidents of Violent Behavior Must Be Reported

Any team member who observes or is subjected to violent behavior in the workplace must report the incident to his or her supervisor or the Human Resources Manager/designee immediately.

If a team member has a personal protection order in place against another individual that prohibits contact in the workplace, the employee must inform the Human Resources
Manager/designee immediately. The protection order will be managed in a confidential manner and shared only with individuals who have a need to know (e.g., front desk reception, facilities, management).

A team member who is the victim of domestic violence, sexual assault or stalking is strongly encouraged to inform his or her supervisor or the Human Resources Manager/designee so security measures and a safety plan can be put in place.

3. Reports of Workplace Violence Will be investigated

All reports of workplace violence will be promptly investigated by the Human Resources Manager/designee. Prompt, remedial action will be taken to address unlawful behavior and/or to remove any threat of immediate danger.

Investigative procedures may vary depending on the nature and extent of the reported behavior and the context in which the alleged behavior occurred.

In order to properly investigate a complaint of workplace violence, DRS employees will cooperate with the Human Resources Manager/designee during all phases of the investigative process. No individual will be discriminated or retaliated against for reporting violent behavior or for providing information as part of an investigative process. The agency will take prompt, appropriate corrective or disciplinary action for acts of retaliation.

4. Support and Resources Will be Provided

The Human Resources Office will provide a list of available resources to victims and witnesses of workplace and/or domestic violence. Resources for employees who are perpetrators of domestic violence will also be provided.

DRS will ensure that reasonable efforts will be made, in accordance with applicable rules and statutes, for an employee who is, or who has a family member who is the victim of domestic violence, sexual assault or stalking, to make arrangements for obtaining medical treatment, counseling, legal assistance, to leave the area, or to create a safer situation for themselves and/or their family members. Efforts may include, but are not limited to, adjusting work schedules and/or granting the use of accrued paid leave or leave without pay. Verification may be required to support the use of leave.

5. Firearms Are Not Permitted on Agency Premises

Individuals are prohibited from carrying and/or possessing firearms or other dangerous weapons in any facility owned or leased by DRS. A facility is defined as the physical building and surrounding grounds, including the designated parking lot.
DRS-ISD-1

USING ELECTRONIC COMMUNICATION SYSTEMS

This policy applies to all Department of Retirement Systems (DRS) employees.

DRS employees are responsible for using agency electronic communication systems (ECS) resources in an ethical, lawful, responsible and non-discriminatory manner. As set forth in this policy, every DRS employee is responsible for communications generated, responded to, sent or posted under his or her network ID. Employees should have no expectation of privacy in the use of agency ECS.

DEFINITIONS

Agency electronic communication systems (ECS) – ECS include, but are not limited to, any electronic media that is used to generate, transmit, display, reproduce or store communications for business purposes. Such electronic media include, but are not limited to:
• personal computers;
• portable laptop computers;
• software;
• e-mail systems;
• telephones;
• voicemail systems;
• facsimile (fax) machines; and
• other electronic message systems which store and transmit communications, including the Internet and related resources.

De minimis use – Five minutes or less and infrequent, not every day.

Internet – Internet means the connection to and use of interconnected networks in the public and private domains to access the World Wide Web, e-mail, file transfer protocols, and other state network resources.

1. Permissible Use Is Outlined

In accordance with WAC 292-110-010, permissible use of ECS is defined as communications that are reasonably related to the conduct of official state business. Permissible use of ECS is broken into three categories:
• Business;
• Agency-approved activities; and
• Authorized, de minimis personal use.

A DRS employee may make de minimis personal use of ECS resources if the subject matter is not related to activities listed as prohibited in this policy and such use:

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 43 of 52
• Results in little or no cost to the state;
• Does not interfere with the performance of official duties;
• Is brief in duration and frequency;
• Does not distract from the conduct of state business; and
• Does not compromise the security of state information or software.
2. Prohibited Use Is Outlined

The use of agency ECS is prohibited:
- For the purpose of conducting outside business, private employment or other activities conducted for private financial gain;
- To support or promote the interests of or solicit for any outside organization, charity, or group unless provided for by law and authorized by the agency Director or designee;
- To assist a campaign for election of a person to office or the promotion of or opposition to a ballot proposition;
- To participate in or assist in an effort to lobby the state legislature or a state agency head;
- To promote personal political beliefs or religious affiliations;
- To engage in personal online bill paying activities; or
- To engage in any conduct that is prohibited by federal or state law or agency policy.

3. Form Must Be Completed

Every DRS employee will complete and sign the Use of the DRS Internet Access Acknowledgement form, documenting his or her understanding of appropriate and authorized use of agency ECS as described in this policy. The supervisor will ensure the policy has been reviewed with the employee and all questions have been answered satisfactorily.

4. Employees Responsible to Maintain Security

DRS will attempt to provide ECS that are secure for business purposes. However, all users should be aware that ECS are vulnerable to interception and to security violations. In an attempt to maintain security of data created, received, stored, etc., on ECS, all DRS employees are responsible to:

- Establish and protect confidential passwords and/or access codes that are used to gain access to ECS (e.g., network ID, e-mail, voicemail, screensaver);
- Access only messages intended for their review; and
- Notify the appropriate supervisor if they believe their password or access code has been compromised and immediately change the password/code.

Supervisors are responsible to ensure proper employee use of ECS. Supervisors may access any communication system used by an employee to carry out business functions and may request a log of activity if necessary.

5. Take Appropriate Precautions When Using Electronic Communication Systems

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 45 of 52
Employees need to take appropriate precautions before requesting or transmitting privileged information and messages. Disclosure of privileged information may occur unintentionally or inadvertently if an unauthorized user gains access to agency ECS. Disclosure may also occur when messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read the messages.

Employees should be aware that it is possible for those outside state government to identify them as visitors to an Internet site. Employees should always exercise conservative judgment in selecting the sites they visit when accessing information on the Internet.

When using Internet services, employees should be aware that certain electronic documents, which potentially include e-mail messages composed or transmitted on the DRS network or the Internet, may constitute public records. Public records must be retained in accordance with RCW and WAC requirements and may be disclosed to requesters.

6. **Downloading Software or Files via the Internet for Personal Use Is Prohibited**

   Downloading of business-related software or files must be arranged through the Help Desk.

7. **Information Is Stored According to Established Standards**

   DRS will maintain information stored on ECS in accordance with retention schedules approved by the Office of the Secretary of State and the agency.

   The ability to monitor employee use of ECS exists within the agency and at the Department of Information Services. Electronic access to an employee’s e-mail, computer hard drive, network files and/or Internet use may be authorized for Human Resources staff for investigatory purposes, as necessary. Additionally, the Internet is a public communications medium and can be monitored by anyone who chooses to monitor Internet traffic.

   DRS may restrict use of, or limit access to, the Internet using gateways and proxy servers, by group, or on an individual by individual basis.
1. **Purpose And Justification**

The agency depends upon Information Technology (IT) to fulfill its mission and goals. It is therefore necessary to establish policies, standards and procedures for securing IT.

This policy forms the Department of Retirement System (DRS) IT security program elements of compliance and accountability upon owners, stewards, custodians and users of IT services, applications, and systems; and enables monitoring of the confidentiality, integrity and availability of IT assets and services.

2. **DRS IT Security Program Ensures**

- Formal IT risk and security assessments are conducted; gaps are identified; mitigations are implemented, and protection of IT assets ensured;
- IT assets are physically secured and annually inventoried;
- Networks, servers and communication infrastructures are securely architected, configured, protected and maintained;
- IT usage is logged, monitored and reviewed to prevent misuse, unavailability, or loss;
- Access to DRS data and other IT assets and services is granted by privilege and authenticated through security controls which are monitored and managed by the Information Services Division (ISD) or a delegate (See definition); Access credentials are hardened appropriately to protect IT assets and services.
- Security awareness training is conducted before access is granted, and annually thereafter;
- Software, applications, and systems are securely architected, developed, transitioned, operated and maintained;
- Changes to production IT assets are authorized, planned, tested, documented, and communicated; Media is securely managed and disposed.
- An IT incident response (IR) plan is maintained and annually tested by team members who are trained and familiar with the IR plan;
- DRS IT security policies, standards, and procedures are reviewed and maintained.

3. **Authority For IT Security Is Established**

- The state Office of the Chief Information Officer (OCIO) sets the IT security strategic direction and policy for Washington state agencies.
- The Technology Services Board (TSB) is responsible for reviewing and approving IT security policy and standards which govern all Washington State agencies.
- The state Chief Information Security Officer (CISO) is responsible for conducting security design reviews of new or significantly upgraded IT infrastructure.
- DRS Human Resources (HR) Office:
  - Performs reference checks and background/criminal checks where appropriate;
  - Schedules and monitors security awareness training;
  - Consults, investigates and provides findings for policy violations.

_Sources:_

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 47 of 52
4. **Annual Confirmation Of DRS IT Security Compliance Required**

The agency director will confirm in writing[1] that DRS is in compliance with the OCIO IT security standards [OCIO Standard No. 141.10](#).

The annual security verification letter indicates review and acceptance of agency IT security policies, procedures, and practices as well as updates since the prior verification.

The agency will establish and maintain an IT security program to contain IT security policies, standards, and documentation in compliance with [OCIO Policy No. 141](#) and [OCIO Standard No. 141.10](#).

[1] OCIO 141.10, 1.5 Compliance, 5, 8; 1. Agency IT Security Program, 1.1 Documentation, 1-8

5. **IT Security Roles And Responsibilities Are Documented**

DRS Team leaders and members (i.e. Owners, stewards and custodians) with IT security responsibilities, impacting the agency IT security program, shall have those roles and responsibilities documented in their position descriptions (PDs).

The DRS Assistant Directors (AD) and DRS HR manager will ensure that team leaders periodically review and maintain team member PDs for these security roles and responsibilities.

6. **Exceptions Management Is Established**

Change requests or exceptions for non-compliance to Office of the Chief Information Officer (OCIO) policy or standards must be authorized by the DRS Director and the OCIO.

7. **Compliance To DRS IT Policies And Standards Is Enforced**

Non-compliance with this policy may lead to corrective measures such as mandatory retraining, suspension/revocation of access, or other sanctions.
This policy applies to all Department of Retirement Systems (DRS) employees.

DEFINITIONS

Appointing Authority – An individual authorized to appoint, transfer, layoff, reduce, dismiss, suspend or demote employees.

Wireless Communication Device (WCD) – a device that transmits voice and/or data via a wireless network or cellular carrier network and supports access to those services necessary to support the documented business need (e.g., hosted Shared Services E-Mail service). Examples of these devices include, but are not limited to, cell phones, smartphones, mobile broadband modems and tablet computers.

Stipend – for the purpose of this policy, a regular monthly payment to an employee towards defraying the cost of using a personally-owned WCD for business-related purposes.

1. Purpose of Policy Is Defined

DRS may authorize the use of WCDs by employees when the job duties of a position warrant their use. The agency may provide a WCD or pay an employee a stipend for the business use of a personally-owned WCD, based on business-related needs as outlined in this policy.

2. Use of Agency-Owned Or Personal WCD For Business Reasons Must Be Authorized

Justification of business need and authorization by the employee’s appointing authority must be documented for an employee to:

a) Use an agency-owned WCD; or
b) Receive a stipend for business use of a personal WCD

Authorization will be granted on a case-by-case basis.
An overtime-eligible employee who is authorized to use a WCD for business-related purposes must ensure he or she uses it only during his or her regularly scheduled work hours.

3. Stipend Program is Established

If an employee is authorized to use his or her personal WCD to conduct state business, he or she will receive one of the following stipends:

Addendum 1 – Questions and Answers
RFP 19-01, Mainframe Rehosting Services
Page 49 of 52
a) $10.00 per month for use of a voice service only; or  
b) $20.00 per month for use of a data service only; or  
c) $40.00 per month for use of combination voice and data service

The employee’s appointing authority will determine the appropriate stipend amount based on the authorized use. See the Wireless Communication Stipend Request Form. Only one stipend amount will be paid to an employee regardless of the number of personally-owned WCDs he or she uses to conduct the authorized state business.  
DRS reserves the right to adjust or terminate the stipend program at any time. DRS is not responsible for any costs incurred by the employee for his or her voice and/or data plan as a result of conducting state business.

4. Use of WCDs While Driving Is Strongly Discouraged

For employee safety, any use of a WCD while driving is strongly discouraged. Any employee who uses a WCD for business-related purposes while operating a motor vehicle must do so only in accordance with state law (RCW 46.61.667 and RCW 46.61.668).

5. Privacy Is Not Expected

Employees using an agency-owned WCD should not have an expectation of privacy in anything they create, store, send or receive via the WCD. All records contained within the WCD; including, but not limited to, phone calls, text messages, e-mails and internet access, are subject to public records request.

As with agency-owned WCDs, employees using a personally-owned WCD to conduct state business should not have an expectation of privacy for such activity on their device. DRS has the right to monitor any and all aspects of this activity.
1. **Purpose And Justification**

The agency depends upon Information Technology (IT) to fulfill its mission and goals. This policy ensures access to DRS IT assets and data is controlled and only granted for authorized DRS team members and users, in accordance with agency Leadership Team requirements and the Office of the Chief Information Officer's (OCIO) IT security policies and standards.

This policy, and its associated standards and procedures are a risk mitigation to ensure only authorized access to agency IT assets and data.

2. **Authority For Access Control Security Is Established**

- The state Office of the Chief Information Officer (OCIO) sets the IT security strategic direction and policy for Washington state agencies.
- The Technology Services Board (TSB) is responsible for reviewing and approving IT security policy and standards which govern all Washington State agencies.
- The office of the state Chief Information Security Officer (CISO/CSO) is responsible for conducting security design reviews of IT infrastructure.
- DRS Leadership Team establishes access control requirements for DRS IT assets and data, commensurate with the agency’s assessment of risk.
- The Information Services Division (ISD) ensures secure access of DRS IT assets and data with IT security controls implemented and maintained according to OCIO security policy and standards and DRS Leadership requirements.
- ISD IT stewards may allow security access controls to be monitored and managed by a delegate (see DEFINITIONS).

3. **Access Is Granted By Permission Only**

Access to DRS IT assets and data must only be granted by permission, through security controls established in the DRS Information Technology (IT) Service and Security standards and procedures.

Access will not be granted to individuals without current security awareness training. Individuals without current training may have access revoked until training is completed.

4. **Unauthorized Access To DRS IT Assets Is Prohibited**

Unauthorized access to DRS IT assets is prohibited and may result in:

- Mandatory retraining of security requirements and concepts
- Mandatory monitoring of IT resource usage

Addendum 1 – Questions and Answers

RFP 19-01, Mainframe Rehosting Services

Page 51 of 52
• Revocation of access permissions or
• Disciplinary action, up to and including termination of employment