Airports Authority of India
Information Technology Division
Safdarjung Airport, New Delhi – 110 003

TENDER DOCUMENT

Development, Hosting and Maintenance of Digital Sky Platform for Ministry of Civil Aviation

TENDER NO.: IT-11042/1/2018-DIRECTORATE OF IT

Tender ID: 2018_AAI_15726_1

Date: 26-09-2018
Contents

1 SECTION I: Notice Inviting Tender 3
2 SECTION II: General Information And Guidelines 11
3 SECTION III: General Terms & Conditions Of The Contract 20
4 SECTION IV: Special Conditions of the Contract 29
5 Section V: Scope of Work 33
Annexure I: Acceptance Letter 34
Annexure II: Performance Bank Guarantee 35
Annexure IV: Force Majeure Format 37
Annexure V: Extension of time format 38
Annexure VI: NDA 40
Annexure VII: MAF 42
Annexure VIII: Undertaking letter 43
Annexure IX: Integrity Pact 44
Annexure X: Bank Guarantee format for EMD 50
Annexure XI: Format for Undertaking of Not being Blacklisted 52
Annexure XII: No Deviation Certificate 53
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Sno.</th>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AAI</td>
<td>Airport Authority of India</td>
</tr>
<tr>
<td>2</td>
<td>ACD</td>
<td>Automatic Call Distributor</td>
</tr>
<tr>
<td>3</td>
<td>ADC</td>
<td>Air Defence Clearance</td>
</tr>
<tr>
<td>4</td>
<td>AES</td>
<td>Advanced Encryption Standards</td>
</tr>
<tr>
<td>5</td>
<td>AFTN</td>
<td>Aeronautical Fixed Telecommunication Network</td>
</tr>
<tr>
<td>6</td>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>7</td>
<td>AMC</td>
<td>Annual maintenance Contract Charges</td>
</tr>
<tr>
<td>8</td>
<td>AMC/ATS</td>
<td>Annual Maintenance Contract/ Annual Technical Service</td>
</tr>
<tr>
<td>9</td>
<td>AMSS</td>
<td>Aeronautical Message Switching Systems</td>
</tr>
<tr>
<td>10</td>
<td>ANI</td>
<td>Automatic Number Identification</td>
</tr>
<tr>
<td>11</td>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>12</td>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>13</td>
<td>ATCO</td>
<td>Air Traffic Controllers</td>
</tr>
<tr>
<td>14</td>
<td>ATR</td>
<td>Action Taken Reports</td>
</tr>
<tr>
<td>15</td>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>16</td>
<td>BFCP</td>
<td>Binary Floor Control Protocol</td>
</tr>
<tr>
<td>17</td>
<td>BI</td>
<td>Business Intelligence</td>
</tr>
<tr>
<td>18</td>
<td>BoM</td>
<td>Bill of Materials</td>
</tr>
<tr>
<td>19</td>
<td>BoQ</td>
<td>Bill of Quantity</td>
</tr>
<tr>
<td>20</td>
<td>BOOT/BOT/BOO</td>
<td>Build Own Operate Transfer/ Build Operate Transfer/ Build Own Operate</td>
</tr>
<tr>
<td>21</td>
<td>BPM</td>
<td>Business Process Management</td>
</tr>
<tr>
<td>22</td>
<td>BRD</td>
<td>Business Requirement Document</td>
</tr>
<tr>
<td>23</td>
<td>CA</td>
<td>Certifying Authority</td>
</tr>
<tr>
<td>24</td>
<td>CAG</td>
<td>Comptroller and Auditor General</td>
</tr>
<tr>
<td>25</td>
<td>CAME</td>
<td>Continuing Airworthiness Management Exposition</td>
</tr>
<tr>
<td>26</td>
<td>CAR</td>
<td>Civil Aviation Rules</td>
</tr>
<tr>
<td>27</td>
<td>CBEC</td>
<td>Central Board of Indirect Taxes and Customs</td>
</tr>
<tr>
<td>28</td>
<td>CCA</td>
<td>Controller of Certifying Authorities</td>
</tr>
<tr>
<td>29</td>
<td>CCB</td>
<td>Change Control Board</td>
</tr>
<tr>
<td>30</td>
<td>CCN</td>
<td>Change Control Notice</td>
</tr>
<tr>
<td>31</td>
<td>CERT-IN</td>
<td>Computer Emergency Response Team - India</td>
</tr>
<tr>
<td>32</td>
<td>CHQ</td>
<td>Corporate Headquarters</td>
</tr>
<tr>
<td>33</td>
<td>CI</td>
<td>Configuration Items</td>
</tr>
<tr>
<td>34</td>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>35</td>
<td>CIN</td>
<td>Corporate Identification Number</td>
</tr>
<tr>
<td>36</td>
<td>CLI</td>
<td>Caller Line Identification</td>
</tr>
<tr>
<td>37</td>
<td>CMDB</td>
<td>Configuration Management Data Base</td>
</tr>
<tr>
<td>38</td>
<td>CNS/ATM</td>
<td>Communication, Navigation and Surveillance/Air Traffic Management</td>
</tr>
<tr>
<td>39</td>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technologies</td>
</tr>
<tr>
<td>40</td>
<td>COTS</td>
<td>Commercial-off-the-Shelf</td>
</tr>
<tr>
<td>41</td>
<td>CPP</td>
<td>Central Public Procurement</td>
</tr>
<tr>
<td>42</td>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>43</td>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>44</td>
<td>CSE</td>
<td>Customer Service Executives</td>
</tr>
<tr>
<td>45</td>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>Sno.</td>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>46</td>
<td>CV</td>
<td>Curriculum Vitae</td>
</tr>
<tr>
<td>47</td>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>48</td>
<td>DC</td>
<td>Data Centre</td>
</tr>
<tr>
<td>49</td>
<td>DDOS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>50</td>
<td>DeitY</td>
<td>Department of Electronics and Information Technology</td>
</tr>
<tr>
<td>51</td>
<td>DFD</td>
<td>Data Flow Diagram</td>
</tr>
<tr>
<td>52</td>
<td>DGCA</td>
<td>Directorate General of Civil Aviation</td>
</tr>
<tr>
<td>53</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>54</td>
<td>DMZ</td>
<td>De-Militarized Zone</td>
</tr>
<tr>
<td>55</td>
<td>DNIS</td>
<td>Dialed Number Identification Sequence</td>
</tr>
<tr>
<td>56</td>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>57</td>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>58</td>
<td>DRC</td>
<td>Data Recovery Centre</td>
</tr>
<tr>
<td>59</td>
<td>DSC</td>
<td>Digital Signature Certificates</td>
</tr>
<tr>
<td>60</td>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>61</td>
<td>DSP</td>
<td>Digital Sky Service Provider</td>
</tr>
<tr>
<td>62</td>
<td>DTMF</td>
<td>Dual-Tone Multi-Frequency</td>
</tr>
<tr>
<td>63</td>
<td>eGCA</td>
<td>e-Governance of Civil Aviation</td>
</tr>
<tr>
<td>64</td>
<td>EIM</td>
<td>External Independent Monitor</td>
</tr>
<tr>
<td>65</td>
<td>EITM</td>
<td>Enterprise Information Technology Management</td>
</tr>
<tr>
<td>66</td>
<td>eKYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>67</td>
<td>EMD</td>
<td>Earnest Money Deposit</td>
</tr>
<tr>
<td>68</td>
<td>ESB</td>
<td>Enterprise Service Bus</td>
</tr>
<tr>
<td>69</td>
<td>FIC</td>
<td>Flight Information Centre</td>
</tr>
<tr>
<td>70</td>
<td>FRS</td>
<td>Functional Requirement Specification</td>
</tr>
<tr>
<td>71</td>
<td>FTE</td>
<td>Full-time equivalent</td>
</tr>
<tr>
<td>72</td>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>73</td>
<td>GCC</td>
<td>Government Community Cloud</td>
</tr>
<tr>
<td>74</td>
<td>GCS</td>
<td>Ground Control Station</td>
</tr>
<tr>
<td>75</td>
<td>GIGW</td>
<td>Guidelines for Indian Government Websites</td>
</tr>
<tr>
<td>76</td>
<td>GIS</td>
<td>Geographic Information System</td>
</tr>
<tr>
<td>77</td>
<td>GRM</td>
<td>Grievance Redressal Module</td>
</tr>
<tr>
<td>78</td>
<td>GSTN</td>
<td>Goods &amp; Service Tax Network</td>
</tr>
<tr>
<td>79</td>
<td>GUI</td>
<td>Graphic User Interface</td>
</tr>
<tr>
<td>80</td>
<td>H/W</td>
<td>Hardware</td>
</tr>
<tr>
<td>81</td>
<td>HDFS</td>
<td>Hadoop Distributed File System</td>
</tr>
<tr>
<td>82</td>
<td>HEX</td>
<td>Hexadecimal</td>
</tr>
<tr>
<td>83</td>
<td>HLD</td>
<td>High Level Design</td>
</tr>
<tr>
<td>84</td>
<td>HMAC</td>
<td>Hash-based message authentication</td>
</tr>
<tr>
<td>85</td>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>86</td>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>87</td>
<td>HTTPS</td>
<td>Hyper Text Transfer Protocol Secure</td>
</tr>
<tr>
<td>88</td>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>89</td>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>90</td>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>91</td>
<td>IDE</td>
<td>Integrated development environment</td>
</tr>
<tr>
<td>92</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>Sno.</td>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>93</td>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>94</td>
<td>IEM</td>
<td>Independent External Monitor</td>
</tr>
<tr>
<td>95</td>
<td>IOPS</td>
<td>Input/output operations per second</td>
</tr>
<tr>
<td>96</td>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>97</td>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>98</td>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>99</td>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>100</td>
<td>ITIL</td>
<td>Information technology Infrastructure library</td>
</tr>
<tr>
<td>101</td>
<td>ITSM</td>
<td>IT Service Management</td>
</tr>
<tr>
<td>102</td>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>103</td>
<td>IVRS</td>
<td>Interactive Voice Response System</td>
</tr>
<tr>
<td>104</td>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>105</td>
<td>JV</td>
<td>Joint Venture</td>
</tr>
<tr>
<td>106</td>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>107</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>108</td>
<td>LLD</td>
<td>Low Level Design</td>
</tr>
<tr>
<td>109</td>
<td>MAF</td>
<td>Manufacturer's Authorization Form</td>
</tr>
<tr>
<td>110</td>
<td>MCA</td>
<td>Ministry of Corporate Affairs</td>
</tr>
<tr>
<td>111</td>
<td>MEITY</td>
<td>Ministry of Electronics and Information Technology</td>
</tr>
<tr>
<td>112</td>
<td>MET</td>
<td>Meteorological Office</td>
</tr>
<tr>
<td>113</td>
<td>MHA</td>
<td>Ministry of Home Affairs</td>
</tr>
<tr>
<td>114</td>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>115</td>
<td>MoCA</td>
<td>Ministry of Civil Aviation</td>
</tr>
<tr>
<td>116</td>
<td>MPLS</td>
<td>Multi-Protocol label Switching</td>
</tr>
<tr>
<td>117</td>
<td>MSA</td>
<td>Master Services Agreement</td>
</tr>
<tr>
<td>118</td>
<td>MSDG</td>
<td>Mobile e-Governance Service Delivery Gateway</td>
</tr>
<tr>
<td>119</td>
<td>MSME</td>
<td>Micro, Small &amp; Medium Enterprises</td>
</tr>
<tr>
<td>120</td>
<td>MSP</td>
<td>Managed Service Provider</td>
</tr>
<tr>
<td>121</td>
<td>MVC</td>
<td>Model-View-Controller</td>
</tr>
<tr>
<td>122</td>
<td>NDA</td>
<td>Non Disclosure Agreement</td>
</tr>
<tr>
<td>123</td>
<td>NFS</td>
<td>Network File System</td>
</tr>
<tr>
<td>124</td>
<td>NIC</td>
<td>National Informatics Centre</td>
</tr>
<tr>
<td>125</td>
<td>NICNET</td>
<td>National Informatics Centre Network</td>
</tr>
<tr>
<td>126</td>
<td>NIT</td>
<td>Notice Inviting Tender</td>
</tr>
<tr>
<td>127</td>
<td>NOC</td>
<td>No Objection Certificate</td>
</tr>
<tr>
<td>128</td>
<td>NOCAS</td>
<td>No Objection Certificate Application System</td>
</tr>
<tr>
<td>129</td>
<td>NOTAM</td>
<td>Notice to Airmen</td>
</tr>
<tr>
<td>130</td>
<td>NPNT</td>
<td>No Permission No Takeoff</td>
</tr>
<tr>
<td>131</td>
<td>NSDG</td>
<td>National e-Governance Service Delivery Gateway</td>
</tr>
<tr>
<td>132</td>
<td>NSIC</td>
<td>National Small Industries Corporation</td>
</tr>
<tr>
<td>133</td>
<td>O&amp;M</td>
<td>Operation &amp; Maintenance</td>
</tr>
<tr>
<td>134</td>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>135</td>
<td>ORM</td>
<td>Object-relational mapping</td>
</tr>
<tr>
<td>136</td>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>137</td>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>138</td>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>139</td>
<td>PBG</td>
<td>Performance Bank Guarantee</td>
</tr>
<tr>
<td>Sno.</td>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>140</td>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>141</td>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>142</td>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>143</td>
<td>PKCS</td>
<td>Public Key Cryptographic Standards</td>
</tr>
<tr>
<td>144</td>
<td>PKI</td>
<td>Public key infrastructure</td>
</tr>
<tr>
<td>145</td>
<td>PM</td>
<td>Project Management</td>
</tr>
<tr>
<td>146</td>
<td>PMU</td>
<td>Project Management Unit</td>
</tr>
<tr>
<td>147</td>
<td>PODS</td>
<td>Pipeline Open Data Standard</td>
</tr>
<tr>
<td>148</td>
<td>POJO</td>
<td>plain old Java objects</td>
</tr>
<tr>
<td>149</td>
<td>PPL</td>
<td>Private Pilot License</td>
</tr>
<tr>
<td>150</td>
<td>QR</td>
<td>Quality Requirement</td>
</tr>
<tr>
<td>151</td>
<td>RCA</td>
<td>Root Cause Analysis</td>
</tr>
<tr>
<td>152</td>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>153</td>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>154</td>
<td>RFM</td>
<td>Registered Flight Modules</td>
</tr>
<tr>
<td>155</td>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>156</td>
<td>RPAS</td>
<td>Remotely Piloted Aircraft System(s)</td>
</tr>
<tr>
<td>157</td>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>158</td>
<td>RTCP</td>
<td>Real-time Transport Control Protocol</td>
</tr>
<tr>
<td>159</td>
<td>RTM</td>
<td>Requirement Traceability Matrix</td>
</tr>
<tr>
<td>160</td>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>161</td>
<td>RTP</td>
<td>Real-time Transport Protocol</td>
</tr>
<tr>
<td>162</td>
<td>RTS</td>
<td>Requirements Traceability Matrix</td>
</tr>
<tr>
<td>163</td>
<td>S/W</td>
<td>Software</td>
</tr>
<tr>
<td>164</td>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>165</td>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>166</td>
<td>SDK</td>
<td>Software developer's kit</td>
</tr>
<tr>
<td>167</td>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>168</td>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>169</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>170</td>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>171</td>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>172</td>
<td>SOA</td>
<td>Service-oriented architecture</td>
</tr>
<tr>
<td>173</td>
<td>SOE</td>
<td>Service Oriented Enterprise</td>
</tr>
<tr>
<td>174</td>
<td>SOP</td>
<td>Standard Operating Procedures</td>
</tr>
<tr>
<td>175</td>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>176</td>
<td>SRS</td>
<td>Software Requirement Specification</td>
</tr>
<tr>
<td>177</td>
<td>SRTP</td>
<td>Secure Real-time Transport Protocol</td>
</tr>
<tr>
<td>178</td>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>179</td>
<td>SSDG</td>
<td>State e-Governance Service Delivery Gateway</td>
</tr>
<tr>
<td>180</td>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>181</td>
<td>STQC</td>
<td>Standardization Testing and Quality Certification</td>
</tr>
<tr>
<td>182</td>
<td>TOGAF</td>
<td>The Open Group Architecture Framework</td>
</tr>
<tr>
<td>183</td>
<td>TPA</td>
<td>Third Party Auditor</td>
</tr>
<tr>
<td>184</td>
<td>TRAI</td>
<td>Telecom Regulatory Authority of India</td>
</tr>
<tr>
<td>185</td>
<td>UA</td>
<td>Unmanned Aircraft</td>
</tr>
<tr>
<td>186</td>
<td>UAS</td>
<td>Unmanned Aircraft Systems</td>
</tr>
<tr>
<td>Sno.</td>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>187</td>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>188</td>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>189</td>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>190</td>
<td>UID</td>
<td>Unique Identification</td>
</tr>
<tr>
<td>191</td>
<td>UIN</td>
<td>Unique Identification Number</td>
</tr>
<tr>
<td>192</td>
<td>UUID</td>
<td>Universal Unique Identifier</td>
</tr>
<tr>
<td>193</td>
<td>UX/UI</td>
<td>User Experience/ User Interface</td>
</tr>
<tr>
<td>194</td>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>195</td>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>196</td>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>197</td>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>198</td>
<td>W3C</td>
<td>World Wide Web Consortium</td>
</tr>
<tr>
<td>199</td>
<td>WBS</td>
<td>Work Breakdown Structure</td>
</tr>
<tr>
<td>200</td>
<td>WSRP</td>
<td>Web Services for Remote Portlets</td>
</tr>
</tbody>
</table>
1 SECTION I: Notice Inviting Tender

E- Tenders from eligible bidders are invited by Executive Director (IT) on behalf of Chairman, Airports Authority of India (AAI) for the works as detailed below:

1. Details of works: Development, Hosting and Maintenance of Digital Sky Platform for Ministry of Civil Aviation

2. Total Estimated Cost: Rs. 46.22 Crores

3. Earnest Money Deposit (EMD): Rs. 71,22,000/-

4. Eligibility Criteria: Refer ‘Tender Document 3 - Qualification and Selection Criteria’

5. The tender processing fee shall be Rs 5,900/- (Rupees Five thousand nine hundred only) and will be non-refundable. Tender processing fee shall be paid to AAI, offline through Demand Draft in favor of “Airports Authority Of India, New Delhi”.

6. This tender is invited through the electronic tendering process and can be purchased offline & downloaded from the Central Public Procurement Portal with URL address http://etenders.gov.in/eprocure/app. A copy of the tender is also available on AAI website www.aai.aero. Please note that the submission of the tender is only through the e-Procurement portal http://etenders.gov.in. The tenders will not be accepted in any other form. Further it may be noted that tenders which are duly submitted on e-Procurement portal shall only be final and tenders just saved without submission / publish will not be available to the evaluation committee. Bidders are requested to go through the e-Procurement portal for guidelines, procedures & system requirements. In case of any technical difficulty, bidders may contact on the following help desk numbers & email ids.
(Help Desk Services)

- Any Queries relating to the process of online bid submission or queries relating to CPP portal Technical Assistance, please call the Helpdesk, on following Telephone Numbers Tel: +91-120-4200462, +91-120-4001002, +91-8826246593. & Email Address: support-eproc@nic.in.
- Before submitting queries related to system, bidders are requested to follow the instructions given in e-procurement portal and get their computer system configured according to the recommended settings for the e-procurement portal.
- In order to facilitate the Vendors / Bidders, the AAI Help desk services shall be available on all working days (except Sunday) between 0800-2000 hours and shall assist users related to the use of the CPP e-Procurement portal. • The below mentioned help desk numbers are intended only for queries related to the ease of use on e-procurement portal. However AAI shall not be responsible for any reason to bidders for not submitting the bids in the e-procurement portal.

7. In case of any Technical issues faced, the escalation matrix is available on the AAI website.

Note: The above mentioned help desk numbers are intended only for queries related to the issues on e-procurement portal and help needed on the operation of the portal. For queries related to the tenders published, bidders are advised to contact concerned Bid Manager of AAI.

*The Helpdesk services shall remain closed on all Govt. Gazetted Holidays.

8. The critical dates for this tender are as given below.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Activity</th>
<th>Date</th>
<th>Time in IST</th>
</tr>
</thead>
<tbody>
<tr>
<td>i.</td>
<td>Download of Tender Document and payment of tender fee from e-tender portal</td>
<td>27-Sept-18 to 31-Oct-18</td>
<td>0930 hrs</td>
</tr>
<tr>
<td>ii.</td>
<td>Submission of queries by bidders</td>
<td>27-Sept-18 to 05-Oct-18</td>
<td>1430hrs</td>
</tr>
<tr>
<td>iii.</td>
<td>Pre-bid meeting</td>
<td>10-Oct-18 to 11-Oct-18</td>
<td>1100 hrs</td>
</tr>
<tr>
<td>iv.</td>
<td>Uploading of replies of queries received up to 05-10-18 at 1430 hours on procurement portal</td>
<td>17-Oct-18 to be intimated later</td>
<td></td>
</tr>
<tr>
<td>v.</td>
<td>Online Submission of Bids (all the envelopes) on e-tender portal</td>
<td>18-Oct-18 to 02-Nov-18</td>
<td>1500hrs</td>
</tr>
<tr>
<td>vi.</td>
<td>Submission of Physical Documents</td>
<td>02-Nov-18</td>
<td>1500hrs</td>
</tr>
<tr>
<td>vii.</td>
<td>Opening of Eligibility Cum Technical Bids</td>
<td>To be intimated later</td>
<td></td>
</tr>
<tr>
<td>viii.</td>
<td>Opening of financial Bids</td>
<td>-</td>
<td>To be intimated later</td>
</tr>
</tbody>
</table>
9. **Clarifications/queries:** Bidder shall submit all pre-bid queries on or before the prescribed date and time (refer fact sheet), online in the following format in Microsoft Excel File, titled – Pre Bid Queries Digital Sky <Bidder’s Name>:

**For any clarifications, bidder may contact:**

**Mr. Ashok Dudee**
DGM (I.T.), CHQ
Airports Authority of India
Mob: 9716815676
Off: 011-24632950, Extn: 3524
Email: ashokdudee@aai.aero

**Sheet 1: Bidder’s Information**

<table>
<thead>
<tr>
<th>Information Sought</th>
<th>Details provided by the bidder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (Authorized Signatory)</td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact Number</td>
<td></td>
</tr>
<tr>
<td>e-Mail ID</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Please paste the table above in email body as well*

**Sheet 2: Clarification Requested**

<table>
<thead>
<tr>
<th>#</th>
<th>RFP Volume No.</th>
<th>Page No.</th>
<th>Section Name</th>
<th>Section No.</th>
<th>Statement as per RFP</th>
<th>Query by bidder</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note 1: Queries submitted in any other format will be rejected at the sole discretion of AAI.*

*Note 2: Queries for all separate documents should be in separate sheets of the excel file*

*Note 3: There shall be no merging of cells that should be undertaken for purpose of submissions.*
Note 4: It is required that proper spell checks are undertaken and proper formats are followed.

Note 5: Non-adherence to the above instruction may result in rejection of the pre-bid queries.

2 SECTION II: General Information And Guidelines

A. INTRODUCTION

1. DEFINITIONS

1.1 “AAI / The Buyer” means the Airports Authority of India.

1.2 "The Bidder / Vendor" means the individual or firm or Company who participates in this tender and submits its bid.

1.3 “Project Manager AAI” means the AAI executive responsible for signing all documents from AAI side and shall coordinate all the activities of the project with the bidder / contractor.

1.4 “The Supplier / Contractor“ means the individual or firm taking up the work as defined under the Notice Inviting Tender.

1.5 "The Works Order" means the order placed for the supply, installation, testing & commissioning of systems / works by the Buyer on the Contractor signed by the Buyer including all attachments and appendices thereto and all documents incorporated by reference therein.

1.6 "The Purchase Order / Supply Order" means the order placed for the supply of items by the Buyer on the Supplier signed by the Buyer including all attachments and appendices thereto and all documents incorporated by reference therein.

1.7 “The Contract” means the agreement signed between the Buyer and the Contractor as per the terms and conditions contained in the Works Order / Purchase Order.

1.8 "The Contract Price" means the price payable to the Contractor under the Works Order / Purchase Order for the full and proper performance of its contractual obligations.

1.9 “Non-responsive Bid” means a bid, which is not submitted as per the instructions to the bidders or Earnest Money Deposit has not been attached, or the required data has not been provided with the Bid or intentional errors have been committed in the Bid.

2. ELIGIBILITY BID CRITERIA
Refer *Tender Document 3 - Qualification and Selection Criteria*

3. **COST OF BIDDING**

   3.1 The Bidder shall bear all costs associated with the preparation and submission of the bid. The Buyer, will in no case, be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

4. **BID DOCUMENTS**

   4.1 The Bidder is expected to examine all instructions, forms, terms and specifications in the Bid Documents. Failure to furnish all information required as per the Bid Documents or submission of bids not substantially responsive to the Bid Documents in every respect will be at the bidder's risk and shall result in rejection of the bid.

5. **AMENDMENTS TO BID DOCUMENTS**

   5.1 At any time, prior to the date of submission of bids, the AAI may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the bid documents by amendments.

   5.2 The amendments shall be communicated to all prospective bidders as corrigendum on the portal and these amendments will be binding on them.

B. **PREPARATION OF BIDS**

Refer *Tender Document 3 - Qualification and Selection Criteria*

6. **DOCUMENTS COMPRISING THE BID**

   The bid prepared by the bidder shall be in three parts to be submitted as per defined procedure in *Tender Document 3 - Qualification and Selection Criteria* and additional below instruction:

   6.1 Payment of tender fee through Demand Draft in favor of “AIRPORTS AUTHORITY OF INDIA” payable at New Delhi in accordance with Clause 12 under Section I of the tender.

7. **BID PRICES**

   7.1 The bidder shall fill the commercials as per the follows:

   7.1.1 Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. The Financial Bid shows the bill of material for all items with scheduled quantities. Bidders are required to download the BoQ file, open it and complete the unprotected cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BoQ file is found to be modified by the bidder, the bid will be rejected. **It may be noted that only duly submitted bids shall be evaluated and bids just saved but not submitted shall not be part of the evaluation process.**
7.1.2 The tendered rate should be inclusive of any taxes, duties, cess, fee and charges levied under any statute including SGST Act / CGST Act and “Good and Service Tax” (Compensation to the states for loss of revenue and after taking into account input credits).

Note: Payment of taxes such as GST shall be made as per actuals at prevailing rates during payments to the bidder.

7.1.3 An undertaking from the bidder shall be submitted that they are registered under GST and compliant of GST provision.

7.1.4 In case of noncompliance of GST provisions and blockage of any input credit, the bidder shall be responsible to indemnify AAI.

7.1.5 The bidder shall indicate all taxes such as GST separately in the BOQ of Financial Bid Form.

7.1.6 The Unit rate shall be inclusive of packing & forwarding charges if any.

7.1.7 The Unit Rate (Inclusive of all taxes) shall be used for calculating the total amount in the Financial Bid.

7.1.8 In the event of any ambiguity, the Unit Rate given in the Financial Bid shall be taken as the correct basis for calculating all other data. In the event of any Errors or Ambiguity in Unit Rates itself the Financial Bid of the bidder shall be rejected.

7.1.9 The prices quoted by the bidder shall remain firm on the date of submission of the Bid and shall not be subject to variation on any account. A bid submitted with an adjustable price quotation will be treated as non-responsive and rejected.

7.2 The bidder shall quote only one price for each item of same specification against the nomenclature shown in Financial Bid/BOQ.

7.3 The bidder shall quote as per price schedule given in Financial Bid/BOQ for all the items as per specifications in Appendix.

7.4 Each Bidder should submit only one product for each item. Offering products of more than one brand or multiple models of the same brand against one item shall make the technical / financial bid of the vendor invalid and such offers shall be rejected at technical / financial stage wherever such defaults are noticed.

7.5 Post offer discount, if any, offered by the bidders shall not be considered. Bidders’ planning to offer discount shall therefore modify their offers suitably while quoting and shall quote clearly net price taking into account discount, free supply etc. However, such discounts from the firm declared as bid winner on the basis of post bid negotiations if any shall be considered and such negotiated offers when agreed by AAI & the bidder shall form a part of the financial Bid.

8. DOCUMENTS ESTABLISHING ITEMS CONFORMITY TO BID DOCUMENTS:
8.1 The bidder shall furnish, as part of his bid, documents establishing the conformity of his bid to the Bid document of all Items and services, which he proposes to supply under the Contract. Submission shall be as follows:

8.1.1 The documentary evidence of the Items and services in conformity to the Bid Documents shall be in the form of literature, drawings and data that the Bidder shall furnish. These shall be attached as Annexure.

8.1.2 Bidder must attach required technical brochures/literatures/data sheets for all the products asked in the tender to ensure that compliance to all the specifications given in the tender document can be verified. Non-availability of specifications (as mentioned in the tender document) in the brochure/literature will be treated as non-compliance and no clarifications may be asked in this regard. If bidder fails to submit the required brochures/literatures along with the tender document, it shall be treated as non-compliance and may lead to outright rejection of bid submitted by bidder. No clarifications in this regard may be sought from the bidder and evaluation committee will be the final authority on the same.

8.1.3 The supporting documents downloaded from websites shall have the complete URL of the page in the header or footer.

8.1.4 Each specifications sought shall be marked or highlighted in the attached brochures / literatures / data sheets. The brochures / literatures / data sheets shall be superscripted with the Item Number and shall be arranged sequentially. The supporting documents shall carry all the required specifications and same shall be marked.

8.1.5 The proposal shall be duly supported by technical literature, equipment brochures & other related reports / documents from the OEM and supported by the documentary evidence that demonstrate compliance to the requirements of the RFP. Proposals that do not provide documentary evidence for complying to the requirement to the RFP shall be considered as non-responsive and may result in rejection on technical grounds.

8.1.6 Bidder to submit letter indicating that the products offered by the bidder is available in the market and will be supplied without any change in specifications & model during the currency of the contract. In case of End of Life of offered product, alternate model with equivalent or better specifications shall be acceptable with prior approval from AAI.

8.1.7 The product/configuration offered by the bidder must be standard and proven. Bidder shall submit a list of clients/locations where similar product/configuration is available. AAI, if so desire, may visit these locations to verify that all the specifications and operational requirements are met as mentioned in the tender document. Any non-compliance observed during such visits shall lead to rejection of bid.

9. PERIOD OF VALIDITY OF TENDER (BID)

9.1 The offered Bid shall remain valid for a minimum of 180 days from the last date of submission of bid. The bidder shall not be entitled, to revoke or cancel the offer or to vary any term thereof, during the said period of validity without the consent in writing of AAI. In case of the bidder revoking or canceling the offer or varying any term in regard thereof,
the bidder’s earnest money deposit shall be forfeited.

9.2 If there is any delay in finalization due to unforeseen factors, all the bidders shall be asked to extend the validity for an appropriate period, specifying a date by which tender is expected to be finalized. However, the tender process shall not be vitiated if any tenderer declines to extend the offer as requested for. In case award of contract is not finalized within 150 days, AAI shall request the bidders to extend the validity of bid and EMD. If bidder does not extend bid & EMD then their bid shall not be considered for further evaluation and EMD shall be refunded.

10. FORMATS AND SIGNING OF BID:

10.1 The e-Bid shall be digitally signed by the bidder at e-tendering portal duly authorized to bind the bidder to the contract. Written power-of-attorney accompanying the bid shall indicate the letter of authorization. The person or persons signing the e-bid shall sign the bid, except for printed literature. The e-bid submitted shall be in properly in readable form and encrypted as per e-tendering portal requirements. Standard Printed terms and conditions of the company other than the NIT conditions shall not be considered.

C. SUBMISSION OF BID DOCUMENTS:

11. SEALING AND MARKING OF BIDS:

11.1 The bidders shall digitally sign & encrypt their bid and submit the bid on-line at CPP procurement portal.

11.2 If all the envelopes are not digitally signed & encrypted the buyer shall not accept such open bids for evaluation purpose and treated as non responsive. Such bid shall be liable to be rejected.

12. SUBMISSION OF BIDS:

12.1 The buyer shall receive the bids online through e-tender portal only not later than that the schedule date specified in the NIT/portal.

12.2 The AAI may, at its discretion extend this deadline for the submission of the bids by amending the bid documents in accordance with Clause 5 in which case all rights and obligations of the AAI and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

12.3 The bidder shall submit his bid offer online at e-tender portal only. Digitally signed tender document downloaded from e-tender portal shall be considered. No separate documents shall be valid. Only relevant attachments, if any other than the tender document, shall be listed out for reference.

12.4 For all documents listed below, the physical copy shall be submitted before the deadline for submission of the bid:

1. Tender Fees
2. EMD
3. Acceptance Letter
4. Integrity Pact

13. LATE BIDS :

13.1 Any bid uploaded after the deadline, the portal system shall not permit uploading of bids after the schedule time of submission.

14. CORRECTIONS / MODIFICATIONS AND WITHDRAWAL OF BIDS :

14.1 The bidder may correct, modify his digitally signed bid after submission prior to the deadline, through provisions of e-tendering portal.

14.2 Subject to Clause 16, no bid shall be modified subsequent to the deadline for submission of bids.

E BID OPENING AND EVALUATION:

15. OPENING OF BIDS:

15.1 The Buyer shall open Bids on-line through e-portal as per schedule or as per intimation of Bid Opening Date &Time to bidders. Bidders or his authorized representatives who choose to attend on the opening date and time may do so if desired. The Bidder's representatives, who are present, shall sign the tender opening register. The bidder shall submit authority letter to this effect before they are allowed to participate in bid opening.

15.2 Maximum of two well-informed representatives of each eligible bidder shall only be allowed to attend the opening of the bids.

15.3 Representative whose bid is not submitted/ rejected cannot attend the tender opening.

16. CLARIFICATION / CONFIRMATION OF COMPLIANCE OF BIDS

16.1 The general eligibility criteria shall be evaluated during preliminary stage and the vendors who have not submitted requisite documents shall be asked through AAI e-tendering portal or by email to substantiate their claims with documentary evidence before a given date failing which their bids shall not be considered further for detailed evaluation.

16.2 It may be noted that enquires / clarifications shall be responded only through e-tendering Portal. All such queries shall be entertained which are received on or before last date/time for submission of queries. AAI response will be uploaded through e-tendering portal. Written responses and no verbal / telephonic enquiry shall be entertained during the tender process

17. EVALUATIONS AND COMPARISON OF SUBSTANTIALLY RESPONSIVE BIDS:

Refer Tender Document 3 - Qualification and Selection Criteria

18 CONTACTING THE BUYER :

18.1 Canvassing in any form in connection with the tenders is strictly prohibited and the tenders submitted by the contractors who resort to canvassing are liable for rejection.
Such rejected tenders will not be returned.

18.2 No bidder shall try to influence directly or through external source, the Buyer on any matter relating to its bid, from the time of publication of NIT till the time the contract is awarded.

18.3 Any effort by a bidder to influence the Buyer in the bid evaluation, bid comparison or contract award decisions shall result in the rejection of the bid, and such actions will be considered as bad performance for future Projects.

19. AWARD OF CONTRACT:

19.1. The acceptance of the tender will be intimated to the successful bidder by AAI, either by fax or by Letter, e-mail, e-tender portal.

19.2. AAI shall be the sole judge in the matter of award of contract and decision of AAI shall be final and binding.

20. RIGHT TO ACCEPT OR REJECT THE TENDERS:

20.1. The right to accept the tender in full or in part/parts will rest with AAI. However, AAI does not bind itself to accept the lowest tender and reserves to it-self the authority to reject any or all the tenders received without assigning any reason whatsoever.

20.2. Tenders not accompanied with prescribed information or are incomplete in any respect, and/or not meeting prescribed conditions, shall be considered non-responsive and are liable to be rejected.

20.3. The Buyer reserves the right to accept or reject any bid or a part of the bid or to annul the bidding process and reject all bids, at any time prior to award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds for the Buyer’s action.

20.4. Pursuant to Clause 20.3 the documentation submitted by bidder shall not be returned unless the bidder explicitly states this request at the time of submission of the tender. AAI also reserves the right at its sole discretion not to award any order under the tender called. AAI shall not pay any costs incurred in the preparation and submission of any tender.

20.5. If the bidder gives wrong information in his Tender, AAI reserves the right to reject such tender at any stage or to cancel the contract, if awarded, and forfeit the Earnest Money.

20.6. Tenders that are not accompanied with Earnest Money Deposit (EMD) shall be rejected outright.

20.7. Should any bidder personnel involved in the project have a relation or relations employed in AAI in the capacity of an officer or the authority inviting tender, the same shall be informed by the bidder. In the event of failure to inform and in a situation where it is established that the relation or relations employed in AAI has/have tried to influence the tender proceedings then AAI at its sole discretion may reject the tender or cancel the contract and forfeit the Earnest Money.
20.8. The requirements indicated in this NIT are the minimum and bids of the firms not complying with these minimum requirements or having deviations equivalents to the minimum requirements shall be liable to be rejected. However, higher than the minimum requirements shall be technically acceptable without any additional financial implication.

20.9. Any correspondence after the opening of the bid, from the bidder, regarding the bid unless specifically sought by AAI shall not be considered. Such post bid offers/clarifications may be liable for action as per clause 16 above.

21. ISSUE OF WORKS ORDER:

21.1. The acceptance of the tender will be intimated to the successful bidder by AAI, either by fax or by letter, e-mail or through e-tender portal.

21.2. The issue of a Works Order / Purchase Order shall constitute the intention of Buyer to enter into the contract with the bidder.

21.3. Acceptance of the Works order / Purchase Order will be deemed as effective from the date of issue of Works Order / Purchase Order. All formalities of submission of the Contract Performance Bank Guarantee in pursuant to clause 6 of section-III of NIT in the format attached Annexure II and signing of the contract shall be completed within 30 days of the issue of Work Order.

21.4. AAI shall be the sole judge in the matter of award of contract and decision of AAI shall be final and binding.

22. SIGNING OF THE INTEGRITY PACT

22.1. Integrity Pact Programme: Signing of Integrity Pact (Annexure) is mandatory for every bidder participating in this tender and the contractor who is awarded the work. The Pact signed on each page by the person authorized by bidder/sub-contractor/associate to sign the bid for submission or the person authorized to sign the contract on behalf of successful bidder shall be submitted by the bidder in PQQ along with the agreement by the Vendor.

22.2. All sub-contractors/associates whose contribution in the project is Rs. 0.50 Crores (Rupees Zero point Five Crores) or above shall sign Integrity Pact with the Authority after the work is awarded to the successful bidder. All bidder shall inform their sub-contractors/associates accordingly.

22.3. The Independent External Monitor (IEM) for this work shall be Sh. M. P. Juneja & Dr. Anup K. Pujari. All correspondences to him regarding implementation of Integrity Pact, shall be addressed Sh. M. P. Juneja c/o Chairman, Airports Authority of India, Rajiv Gandhi Bhawan, Safdarjung Airport, New Delhi–110003 & Dr. Anup K. Pujari IAS (Retd). E-mail id of IEMs are mp_juneja@yahoo.com & anup@nic.in respectively.

22.4. Integrity Pact shall be signed on plain papers by bidder, later which shall be signed by contract signing authority of AAI.

22.5. PROFORMA FOR UNDERTAKING: bidder firm shall submit an undertaking stating its firm or its partners or its Directors are not currently black listed or any case is pending
or any complaint regarding irregularities is pending in India by any Indian State/Central Governments Departments or Public Sector Undertaking of India as per Annexure.

23. **SIGNING OF CONTRACT:**

23.1. The issue of Works Order / Purchase Order shall constitute the award of contract on the bidder. The signing of the Contract shall be completed within 30 days of the acceptance of the Work Order / Purchase Order.

24. **ANNULMENT OF AWARD :**

24.1. Failure of the successful bidder to comply with the requirement of Clause 22 shall constitute sufficient ground for the annulment of the award and forfeiture of the EMD in which event the Buyer may make the award to any other bidder at his discretion or call for new bids.

25. **QUALITY ASSURANCE REQUIREMENTS :**

25.1. The supplier shall submit copies of Valid Certificates to ensure that all works comply with standards specified in the QRs.

26. **TRANSFER OF TENDER DOCUMENT :**

26.1. Transfer of Tender Documents by one bidder to another is not permissible. Similarly transfer of tenders submitted by one bidder in the name of another vendor is not permissible.

27. **CONTRACT MONITORING :**

27.1. The buyer shall hold regular contract monitoring meetings after the award of the contract to monitor the performance of the contract

27.2. First such meeting shall be hold within one week of award of the contract. The date and time of such meeting shall be intimated to the contractor / supplier by fax / post. The date and time of subsequent meetings shall be decided and recorded in previous meetings.

27.3. The proceedings of each meeting shall be recorded and action as required towards successful completion of the project shall be initiated promptly by both AAI and the contractor. Project review meetings shall be with reference to mile stones and contract performance analysis.

27.4. Buyer shall communicate the readiness of the site(s) to the vendor & when the buyer is ready with the installation plans.
3 SECTION III: General Terms & Conditions Of The Contract

1. Purpose & Scope

1.1 This document sets out the terms & conditions be met in connection with the provision of the RFP to AAI for the work as per details given in the notice inviting Tender with Scope of work and specifications.

1.2 This tender document includes details like quantity, delivery, installation, commissioning (including Operating system & other software for the items as tendered for) & support services for maintenance, etc.

1.3 The hardware & software supplied against this tender must include all the modules, sub modules and items required for installation, smooth performance and crash recovery of the system such as installation kit, CDs, software manuals, hardware sub-systems etc.

2. Compliance:

2.1 The unconditional acceptance of all the terms & conditions of the NIT has to be submitted through a letter. The format of the letter is attached at Annexure-I.

2.2 The submission of the tender will imply acceptance of all the tender condition by the bidder laid in tender document including all the Annexure(s) & Appendices to the tender document.

2.3 The compliance to the terms & conditions should be supported by authenticated documentation wherever required.

2.4 The submission of unconditional acceptance as described above is essential for the tender evaluation. The failure to submit the unconditional acceptance statement in the said format shall result in his tender being rejected.

3. Language and Currency :

3.1 The bidder shall quote the rates in English language and international numerals. The rates shall be in whole numbers. The rates shall be written in both figures as well as in words. In case of disparity in figures & words, the rate in words will be considered. In the event of the order being awarded, the language of all services, manuals, instructions, technical documentation etc. provided for under this contract will be English. The bidders should quote only in Indian Rupees and the bids in currencies other than Indian rupees shall not be accepted.


4.1 Standard printed conditions of the bidder to the offer, other than the conditions specified here, will not be acceptable.

4.2 For the purpose of the tender, the metric system of units shall be used.
4.3 All entries in the tender shall either be typed or be in ink. Erasers shall render such tenders liable to summarily rejection. The bidder shall duly attest all corrections, cancellation and insertions.

4.4 Bidder's offers shall be with reference to section and clause numbers given in the tender Appendix.

5. **Earnest Money**:

5.1 The Earnest Money Deposit (EMD) (valid up to 6 months from last date of submission of tender) in the form of Demand Draft or Bank Guarantee from Nationalized/Scheduled Banks for an amount of Rs ____________ shall be submitted. Scanned copy of the EMD and tender fee shall be submitted in the along with the bid document. The bidder required to submit the original Tender Fee and EMD documents to Bid Manager, AAI before opening of the First Cover otherwise the bids will be rejected outright.

Bank Guarantee Format provided in **Annexure X** shall be used in case EMD is being submitted as Bank Guarantee.

5.2 The EMD of the unsuccessful bidders of First Cover shall be discharged / returned after the completion of the evaluation process.

5.3 The EMD of the bidders other than the lowest bidder shall be discharged / returned promptly, after evaluation of financial bids.

5.4 The EMD of the successful bidder will be returned after the bidder provides the performance guarantee, as required in para 6 of this section of the tender document.

5.5 The EMD amount shall be forfeited in the following events:

5.5.1 If the successful bidder fails to enter into a contract with AAI within 30 calendar days after the receipt of the purchase order / work order as specified under clause 23 of section-II.

5.5.2 If the successful bidder fails to submit the performance guarantee as stipulated in para 6 of this section within 30 calendar days after the receipt of the purchase order / work order.

5.5.3 In the event of not accepting the conditions of the contract even after agreeing to do so and submitting the letter of un-conditional acceptance of terms as per letter in Annexure-I.

5.6 No interest or any other expenses, whatsoever, will be payable by AAI on the EMD in any manner.

6. **Performance Bank Guarantee**.

6.1 The successful bidder shall furnish the Contract Performance Bank Guarantee as specified in the tender within 30 days of acceptance of purchase/work order. The value of Performance Bank Guarantee shall be 10% of the total project cost for contract period from the issue of purchase order that is Five years 8 months. This has to be done in a fixed period of time as per
terms and conditions of the tender to avoid any delay in execution of work. In case of delay in execution of work the bidder shall be required to proportionately extend the PBG. In case successful bidder fails to submit the PBG within stipulated period, interest @ 12% p.a. on performance Guarantee amount would be levied (non-refundable) for delayed period of submission and shall be deducted from EMD or First running Bill in case, successful bidder fails to submit performance bank guarantee within 30 days, AAI reserve the right to forfeit EMD and cancel the order. In case successful bidder fails to submit performance bank guarantee within 60 days, AAI reserves the right to forfeit EMD and cancel the order.

6.2 The performance guarantee amount shall be payable to AAI without any condition whatsoever and the guarantee shall be irrevocable.

6.3 The performance guarantee shall be deemed to govern the following guarantees from the successful bidder, in addition to other provisions of the guarantee:

6.3.1 The Hardware / Software supplied under the contract shall be free from all defects / bugs and upon written notice from AAI, the successful bidder shall fully remedy, free of expenses to AAI, all such defects / bug as developed under the normal use of the said hardware / software within the period of guarantee/Warranty.

6.3.2 The performance guarantee is intended to secure the performance of the entire system. However, it is not to be construed as limiting the damages stipulated in any other clause.

6.4 The performance guarantee will be returned to the successful bidder at the end of the period of liability without interest.

6.5 The bidder as per operation, installation, maintenance manuals and performance guarantee tests supplied by the successful bidder, will do the loading, installation, testing & commissioning of systems. The successful bidder will be fully responsible for the guaranteed performance of the supplied systems under warranty & AMC period. In case of any problem after commissioning and during guarantee/AMC period the successful bidder will depute required resources to AAI's site as per SLA to remove all defects at contractor's cost.

6.6 A fine of an agreed amount calculated as per the Service Level Agreement (SLA) subject to a maximum value equal to 10% of the Annual Maintenance Cost. The acceptance of valid reasons for non-compliance to 6.5 above shall rest with ED (IT) and his decision with regard to imposition of the fine shall be final. The fine shall be recovered from the Bank Guarantee or shall be recovered from Quarterly payment of AMC as the case may be.

7. Correspondence:

7.1 All correspondence would be directly with the bidder and correspondence through agents will not be entertained.

8. Testing and Inspection:

8.1 The acceptance testing of the system to be developed and deployed under this project shall be as per the Section-V.
8.2 The testing & inspection as per above clauses in any way does not relieve the Contractor from any Warranty or other obligations under this contract.

9. **Extension of Time**

9.1 This work is urgent and hence the completion period as per contract shall be adhered to strictly. However, in-case of extraordinary situations which may delay the completion of the project, the contractor shall apply for extension in time as per format contained in Annexure-V.

9.2 AAI at its sole discretion may extend the time period for completion of the work without any prejudice to operate the penalty clauses provided for in the Tender Document. Such extension of time and the circumstances leading to the extension of time shall be communicated in writing to the contractor.

10. **Compensation for Delay**

10.1 Time is the essence of the Contract.

10.2 If the successful bidder fails to complete the supply / work within time fixed under the contract, he shall pay to the AAI without prejudice to any other rights or remedy as may be available to the purchaser, an agreed compensation amount calculated @ 1% of the total value of the uncompleted portion of the work per week or part thereof subject to a maximum value equal to the 10% of Total Contract value. If the project is delayed by 8 weeks, AAI reserves the right to cancel the contract. In case of cancellation of the contract the developed source code and documents shall be property of AAI.

10.3 The amount of compensation for delay and waiver of compensation for delay in case of justified reasons shall be decided at the discretion of Accepting Authority and the same shall be final and binding on the contractor. Time taken by AAI and local statutory authorities for approval of drawings, design, estimate etc, force majeure reasons and any other reasons beyond control of the contractor shall be considered as justified reasons. The amount of compensation may be adjusted or set off against any sum payable to the contractor under this or any other contract with AAI.

11. Blank

12. **Force Majeure**

12.1 AAI shall grant an extension of time limit set for the completion of the work / repair in case the timely completion of the work is delayed by force majeure beyond the contractors control, subject to what is stated in the following sub paragraphs and to the procedures detailed there in being followed. Force Majeure is defined as an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, flood, storms etc.), acts of states, the direct and indirect consequences of wars (declared or un-declared), hostilities, national emergencies, civil commotion and strikes (only those which exceed a duration of ten continuous days) at successful Bidder’s factory. The successful bidder’s right to an extension of the time limit for completion of the work in above-mentioned cases is subject to the following procedures.

12.2 That within 10 days after the occurrence of a case of force Majeure, the bidder informs the AAI in writing about the occurrence of Force Majeure Condition (as per Annexure-IV to the...
tender document) and that the Bidder considers himself entitled to an extension of the time limit. The contractor shall submit the application for extension of time as attached in Annexure.

12.3 That the contractor produces evidence of the date of occurrence and the duration of the force majeure in an adequate manner by means of documents drawn up by responsible authorities.

12.4 That the contractor proves that the said conditions have actually been interfered with the carrying out of the contract.

12.5 That the contractor proves that the delay occurred is not due to his own action or lack of action.

12.6 Apart from the extension of the time limit, force majeure does not entitle the successful bidder to any relaxation or to any compensation of damage or loss suffered.

13. Patents, Successful bidder's Liability & Compliance of Regulations

13.1 Successful bidder shall protect and fully indemnify the AAI from any claims for infringement of patents, copyright, trademark, license violation

13.2 Successful bidder shall be responsible for compliance with all requirements under the laws and shall protect and indemnify completely the AAI from any claims/penalties arising out of any infringements and indemnify completely the AAI from any claims/penalties arising out of any infringements.

13.3 All the software licenses shall be in the name of AAI or its nominated body. All the system upgrades/patches shall be provided free of cost during the contract period, which includes support period with latest updates.

14. Settlement of Disputes :

14.1 If a dispute of any kind whatsoever arises between the AAI/MoCA and the Contractor in connection with, or arising out of the Contract or the execution of the works, whether during the execution of the Works or after their completion and whether before or after repudiation or after termination of the contract, including any disagreement by either party with any action, inaction, opinion, instruction, determination, certificate or valuation of the Project Manager or his nominee, the matter in dispute shall, in first place be referred to the ED (IT), AAI. He shall activate the dispute resolution mechanism to resolve the dispute in question. Any party may invoke arbitration clause, if dispute in question is not settled by the Dispute resolution mechanism

14.2 Unless the Contract has already been repudiated or terminated or frustrated the Contractor shall in every case, continue to proceed with the works with all due diligence and the Contractor and AAI shall give effect forthwith to every decision of the Project Manager or his nominee unless and until the same shall be revised, as hereinafter provided, by the Dispute Resolution Mechanism or in an Arbitral Award.

15. Arbitration and Law :
15.1 Except where otherwise provided for in the contract, all questions and disputes relating to the provisions of this contract shall be settled under the Rules of Indian Arbitration and Conciliation (Amendment) Act, 2015, within thirty (30) days (or such longer period as may be mutually agreed upon from the date that either party notifies in writing that such dispute or disagreement exists. The single Arbitrator for settlement of any dispute with regard to this contract shall be appointed by the Chairman AAI on mutual agreement of both parties. The venue of Arbitration shall be New Delhi, India. The arbitration resolution shall be final and binding upon the parties and judgment may be entered thereon, upon the application of either party, by any court having jurisdiction.

15.2 Indian laws shall govern this contract.

16. TERMINATION FOR DEFAULT & RISK PURCHASE:

16.1 The AAI may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Contractor, terminate this Contract in whole or in part in any or the following events.

16.2 If the Contractor fails to deliver any or all of the Items within the time period(s) specified in the Contract or any extension thereof granted by the AAI pursuant to Clause 9 of Section - III.

16.3 If the Contractor fails to perform any other obligation(s) under Contract.

16.4 If the Contractor, in either of the above circumstances, does not remedy his failure within a period of 30 days (or such longer period as AAI may authorize in writing) after receipt of the default notice from AAI.

16.5 As a penalty to the Contractor the AAI shall en-cash Contract Performance Bank Guarantee. The AAI in such case shall pay for the assessed value of the executed work that can be used. No payment shall be made for the efforts put in by the Contractor in case the same are of no value to AAI. The balance unfinished work of the project will be got done by fresh tendering on Contractor’s risk and that extra expenditure will be recovered.

17. TERMINATION FOR INSOLVENCY:

17.1 The AAI may at any time terminate the Contract by giving written notice to the supplier, without compensation to the Contractor, if the Contractor becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right or action or remedy which has accrued or will accrue thereafter to AAI. In the event of termination for penalty to the contractor Clause 16.5 shall be applicable.

18. SET OFF:

19. Deviation in Quantity:
19.1 AAI reserves the right to change the quantity or part thereof to be supplied by +/-50% of the tendered quantity (for site specific measurable length) but within the overall deviation limit of 30% of the contract value.

19.2 AAI also reserves the right to purchase Extra item, Substitute items as per site requirements upto the overall limit of 30% of the contract value.

19.3 The overall deviation, Extra item or the substitute items taken together shall not exceed 30% of the contract value unless until it is mutually agreed by both the parties and a specific order is placed on the vendor in this regard.

20. Limitation of Liability

20.1 Subject to Clause 20.4 below, Implementation Agency i.e bidder (the "Indemnifying Party") undertakes to indemnify, hold harmless the Purchaser (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys’ fees), fines, penalties, taxes or damages (Collectively “Loss”) on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party’s negligence or willful default in performance or non-performance under this Agreement.

20.2 If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

20.3 Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by
a) Indemnified Party’s misuse or modification of the Service;
b) Indemnified Party’s failure to use corrections or enhancements made available by the Indemnifying Party;
c) Indemnified Party’s use of the Service in combination with any product or information not owned or developed by Indemnifying Party;

However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either
i. Procure the right for Indemnified Party to continue using it
ii. Replace it with a noninfringing equivalent
iii. Modify it to make it noninfringing.

The foregoing remedies constitute Indemnified Party’s sole and exclusive remedies and Indemnifying Party’s entire liability with respect to infringement.

20.4. The indemnities set out in Clause 20 shall be subject to the following conditions:

(i) the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
(ii) the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense;

(iii) if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this Article, the Indemnifying Party may participate in such Defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses;

(iv) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;

(v) all settlements of claims subject to indemnification under this Clause will:
   a. be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and
   b. include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;

(vi) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings;

(vii) the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;

(viii) in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and

(ix) if a Party makes a claim under the indemnity set out under Clause 20.1 above in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

20.5 The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the indemnification obligations set out in Clause 20 and breach of Clause 21 (Non-Disclosure Agreement).

20.6 In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third party claims (other than those set-forth in Clause 20.1) even if it has been advised of their possible existence.

20.7 The allocations of liability in this Section 20 represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each
Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

21. Non-Disclosure Agreement:

Bidder shall submit Non Disclosure Agreement (NDA) as per Annexure on Rs. 100/- non judicial stamp paper in original. This is required to be submitted by the bidder for not sharing the source code etc. to others.
4 SECTION IV: Special Conditions of the Contract

1. Standards

1.1. All designs, codes, developing platforms, developing techniques and workmanship shall be in accordance with the highest accepted industry standards for this type of work.

1.2. The bidder shall also state, where applicable, the National or other International standard(s) to which the whole, or any specific part, of the system, software, or training complies.

1.3. The requirements given in this document are firm and no deviation of any kind is acceptable.

2. Time Schedule

2.1. The work as per the Notice Inviting Tender shall be completed within (As per Scope of Work Documents) days of placement of firm order from AAI or as per the schedule submitted by the bidder whichever is less.

2.2. Time - The Essence of Contract

2.2.1. The time and date of completion of the works as contained in the supplier’s proposal and as agreed to contractually after modifications, if any, shall be final and binding upon the supplier. It must be understood that the supplier has made the proposal after fully considering all such factors which may have any bearing on the time schedule of the contract, and no extension in the schedule whatsoever shall be permitted on these accounts by AAI.

2.2.2. The bidder is expected to submit the project plan within 1 week of award of the contract and shall stick to the plan. The contract execution shall be monitored initially on weekly basis and subsequently on daily basis.

2.2.3. The Design, Development/Integration, and Implementation of Digital Sky Portal and Mobile Apps timelines are indicated in Scope of Work Documents

3. Delay & Non-Conformance

3.1. In case of the above time scheduled including levy of compensation for late delivery of systems as contained in Section-III and Scope of Work of the tender document not being adhered to, AAI has the right to cancel the order wholly or in part thereof without any liability to cancellation charges and procure the goods / software elsewhere in which case the successful bidder shall make good the difference in the cost of goods procured elsewhere and price set forth in the order with the successful bidder.

4. Payment terms

4.1. No mobilization advance shall be paid.
4.2. The payment shall be made progressively on completion of each milestone as detailed in Tender Document 2. The payments shall be released to the Contractor on submission of documents as below for each completed milestone.

   4.2.1. Bills (Invoices) in duplicate
   4.2.2. Delivery Challan in original
   4.2.3. Original receipt from the Consignee for completion of work
   4.2.4. Original Test/Inspection certificate from Consignee as applicable
   4.2.5. SAT completion certificate as applicable.
   4.2.6. Payment for Annual maintenance Contract Charges (AMC) shall be made quarterly on quoted annual cost for each year on the basis of SLA performance.

5. **Guarantee / Warranty**

5.1. Complete Hardware, Software, Apps, Interfaces & Accessories shall be guaranteed against all defects/bugs and for a satisfactory performance, as per all the listed features, for the duration of contract from the date of supply/Go-live.

5.2. The bidder shall attend at his own expense and get the defect/bugs removed in the systems as detected by AAI during the period of warranty/AMC Support.

5.3. The Bidder hereby represents and warrants that (i) the Services/Products as supplied, installed, tested and accepted; (ii) use of the Services/Products in accordance with the Contract; and (iii) copying of the Software and Documentation provided to the Employer in accordance with the Contract do not and will not infringe any Intellectual Property Rights registered in India held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Employer to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Bidder shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for Project execution.

6. **Substitution & Wrong Supplies**

6.1. Unauthorized/Pirated substitution or materials delivered in error of wrong description or quality or supplied in excess quantity or old versions shall be returned to the successful bidder at his cost and risk.

7. **Dispatch of Documents**

7.1. Pre-receipted Bills in triplicate at each stage of payment.
7.2. Copy of the Delivery Challan.
7.3. Copy of the Inspection report as applicable.
7.4. Duly certified Installation / Commissioning Certificate/Certified SLA with the bills.
7.5. Any other Document

8. **Up gradation**
8.1. The successful bidder shall guarantee the long-term availability of Upgraded versions of hardware / software to the buyer for the full life of the system. The successful bidder must ensure that before outdating the current versions/systems or availability of the upgraded versions/systems covered under the contract, successful bidder shall ensure deployment of the next upgraded version/system. Installation of software Updates/upgrades and Patches to be covered under warranty/AMC period.

8.2. In case additional effort are required for the web portal and mobile apps development, the rates shall be charged on pro-rata basis


9.1. The bidder shall supply/prepare complete set of technical/ operations and maintenance manuals (as applicable) along with the delivery. The cost of such manuals supplied will be included in the cost of the system.

10. Change of Model: As per the Section II.

11. Sample Testing - Clause not applicable

12. Training

12.1 Bidder to provide training as per Scope of Work of this tender document.

13. INTELLECTUAL PROPERTY RIGHTS

13.1. Airports Authority of India shall be the sole owner of the web-portal, mobile Apps and system developed under this project. Airports Authority of India shall have the sole and exclusive rights over source code, design and all related documents to market this product commercially. AAI may however on its own discretion take the help of vendor in facilitating in this effort.

13.2. All intellectual property rights owned by the vendor shall belong to the vendor that owned such rights immediately prior to the Effective Date (pre-existing rights) or developed independently of this agreement. Such pre-existing rights will include all rights to improvements, enhancements and other additions to any of selected vendors pre-existing work, proprietary methodologies or tools, without regard to whether these were developed during the performance of the Agreement. Subject to the foregoing, AAI will also have rights to use and copy all intellectual property rights, process, specifications, reports and other document, drawings, manuals etc. provided or used by the vendors / subcontractors as part of the Scope of Works under this Agreement for the purpose of this Agreement on non-exclusive, non-transferable, perpetual, royalty-free license to use basis. No part or portion of such pre-existing work shall be unbundled or separated from the particular Work Product/Deliverable or used as a stand-alone product or development tool.

14. Submission of Acceptance Testing procedure

14.1 It will be the responsibility of the vendor to submit the system test procedure for conducting the post installation site acceptance testing. The procedure submitted by the vendor should be drafted in line with the standard practices followed in the industry.
and should be in accordance with the test procedures & practices specified by the OEM/Govt. Agencies. The acceptance test procedure on approval by AAI shall become the document for acceptance of the software / equipment after installation at the site. The draft copy of system test procedure should be made available to AAI before 15 days of the schedule site acceptance date / UAT.

15. Project Schedule & Monitoring

15.1 The vendor shall plan various activities and submit the execution schedule within one week of award of the work. The execution schedule should clearly indicate all activities and the time required for completion of each activity taking the total project time as specified in para 2 above. Parallel activities and the dependent activities for each activity may be required to be specified in the schedule. The vendor would be required to submit the bar chart for all the activities along with the schedule. The project shall be closely monitored with respect to this schedule. The project review & coordination meetings shall be held once in 15 days with respect to this schedule. Apart from the regular monitoring meeting at CHQ the physical progress of the work shall be monitored from time to time as agreed between both the parties in the progress review meetings. Any slippage from the schedule in completion of one activity and resultant delay / impact on the overall completion schedule shall be reviewed in each review meeting and the vendor would be required to take corrective actions to bring back the project on schedule.

16. Concessions to the MSME registered with NSIC, shall be applicable as per the directives of Govt. of India.

17. Purchase preference to Central Public Sector Undertaking shall be applicable as per the directives of Govt. of India prevalent on the date of acceptance.

18. Purchase preference to domestically manufactured electronics goods shall be applicable as per policy issued by Department of Electronics and Information Technology (DeitY).

19. The vendor should deploy well trained personnel at the site. AAI shall not be responsible for any incident or accident of any order happening at the site due to any negligence of the personnel deployed by the bidder. The bidder shall absolve AAI against all such claims.
5 Section V: Scope of Work

Please refer the following documents for details:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tender Document 2 - Scope of Work</td>
</tr>
<tr>
<td>2.</td>
<td>Scope of Work - Appendix 1 - Development of Digital Sky Pilot Phase</td>
</tr>
<tr>
<td>3.</td>
<td>Scope of Work - Appendix 2 - Technology Standards</td>
</tr>
<tr>
<td>5.</td>
<td>Scope of Work - Appendix 4 - Functional Requirements for Digital Sky</td>
</tr>
<tr>
<td>7.</td>
<td>Scope of Work - Appendix 6 - Digital Sky - Cloud Service</td>
</tr>
<tr>
<td>8.</td>
<td>Scope of Work - Appendix 7 - Digital Sky Help Desk Solution</td>
</tr>
<tr>
<td>9.</td>
<td>Scope of Work - Appendix 8 - Solution Architecture</td>
</tr>
<tr>
<td>10.</td>
<td>Scope of Work - Appendix 9 - Service Level Agreement (SLA)</td>
</tr>
</tbody>
</table>

Additional documents as part of tender documents include:

1. Tender Document 1 - Digital Sky
2. Tender Document 3 - Qualification and Selection Criteria
Annexure I: Acceptance Letter

ACCEPTANCE LETTER

To,
General Manager (IT)
Airports Authority of India, CHQ
Safdarjung Airport,
New Delhi

Sub: Acceptance of Terms & Conditions of Tender

Name of Work:
Tender No.:

Dear Sir,

1. The tender document for the works mentioned above have been sold to me/us by Airports Authority of India and I / we hereby certify that I / we have read the entire terms and conditions of the tender document made available to me / us in the office of the General Manager (IT) , AAI, which shall form part of the contract agreement and I / we shall abide by the conditions / clauses contained therein.

2. I / We hereby unconditionally accept the tender conditions of AAI’s tender document in its entirety for the above works.

3. It is clarified that after unconditionally accepting the tender conditions in its entirety, it is not permissible to put any remarks / conditions (except unconditional rebates on quoted rates if any) in the tender enclosed in envelope "A", "B"& "C" and the same has been followed in the present case. In case any provisions of this tender are found violated after opening envelope "A","B"&"C". I / we agree that the tender shall be rejected and AAI shall without prejudice to any other right or remedy be at liberty to forfeit the full said earnest money absolutely.

4. That, I /We declare that I/we have not paid and will not pay any bribe to any officer of AAI for awarding this contract at any stage during its execution or at the time of payment of bills, and further if any officer of AAI ask for bribe /gratification, I will immediately report it to the appropriate authority of AAI.

I /We declare that I/we have received and read through all tender documents, corrigendum and clarifications uploaded by AAI on the the e-Procurement portal for the project.

Yours Faithfully,

(Signature of the Tenderer)

Date: ____________________

with rubber stamp
Annexure II: Performance Bank Guarantee

PROFORMA BANK GUARANTEE FOR CONTRACT PERFORMANCE
(To be stamped in accordance with Stamp Act)
(The non-judicial stamp paper should be in the name of issuing Bank)

Ref: ___________________ Bank Guarantee No: _______________
Date: ______________

To
AIRPORTS AUTHORITY OF INDIA
Rajiv Gandhi Bhavan,
Safdarjung Airport New Delhi

Dear Sirs,

In consideration of the Airports Authority of India (hereinafter referred to as the 'Owner', which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns) having awarded to M/s ----------- (hereinafter referred to as the 'Contractor', which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns), a contract. Bearing No. ----------- dated---------- valued at ----------- for ----------- and the contractor having (scope of contract) agreed to provide a Contract Performance of the entire Contract equivalent to ----------- -----(10 per cent) of the said value of the Contract to the Owner. We at ----------- (hereinafter referred to as the 'BANK', which expression shall, unless repugnant to the context or meaning thereof, include the successors, administrators, executors and assigns) do hereby guarantee and undertake to pay the Owner, on demand any and all money payable by the Contractor to the extent of ____________________ at any time upto __________(day/month/year) without any demur, reservation, contest, recourse or protest and/or without any reference to the Contractor. Any such demand made by the owner the Bank shall be conclusive and binding notwithstanding any difference between the owner and contractor or any dispute pending before any court, tribunal or any authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the Owner and further agrees that the guarantee herein contained shall continue to be enforceable till the Owner discharges this guarantee. The Owner shall have the fullest liberty, without affecting in any way the liability of the Bank under this guarantee, to postpone from time to time the exercise of any powers vested in then or of any right which they might have against the Contractor. And to exercise the same at any time in any manner, and either to enforce or to forebear to enforce any convenants, contained or implied, in the Contract between the Owner and the Contractor or any other course of or remedy or security available to the Owner. The Bank shall not be released of its obligations under these presents by any exercise by the Owner or by any other matters or thing whatsoever which under law would, but for this provision, have the affect of relieving the Bank. The Bank also agrees that the Owner at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Contractor and notwithstanding any security or other guarantee that the Owner may have in relation to the Contractors liabilities.

Apart from other guarantees this Bank Guarantee explicitly provides for the following:
A) The Hardware / Software supplied under the contract shall be free from all defects / bugs and upon written notice from AAI, the successful bidder shall fully remedy, free of expenses to AAI, all such defects / bug as developed under the normal use of the said hardware / software within the period of guarantee/Warranty.

B) The performance guarantee is intended to secure the performance of the entire system. However, it is not to be construed as limiting the damages stipulated in any other clause.

Notwithstanding anything mentioned herein above our liability under this guarantee is restricted to Rs. ---------- and it shall remain in force upto and including ------------ and shall be extended from time to time for such period (not exceeding one year), as may be desired by M/s ----------- on whose behalf this guarantee has been given.

WITNESS

Dated this --------- day of ------- 2017 at ----

Signature ----------- Signature ----------

Name --------------- (Bank's Rubber Stamp)

Official address ----------- Name -------------

Designation with Bank Stamp

Attorney as per Power of

Attorney No. -----------

Date--------------------------
**Annexure IV: Force Majeure Format**

**FORMAT FOR INTIMATION OF FORCE MAJEURE OCCURRENCE**

To,
General Manager (IT)
Airports Authority of India, CHQ
Safdarjung Airport,
New Delhi

**Name of Work:** -  
**Tender No.:** -

**Subject:** Intimation regarding Force Majeure Case:

Sir,

**Pursuant to Clause No.12 Section III-** FORCE MAJEURE, it is for your kind information that a case of force majeure has since occurred. Details are given below:

<table>
<thead>
<tr>
<th>Date of occurrence</th>
<th>Detail of Incident</th>
<th>Activity affected</th>
<th>Likely Delay</th>
<th>Requested Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We are entitled to an extension in the date of completion as requested above. Bar Chart with revised schedule of activities is attached. Please approve the extension in the time. Evidence of the date of occurrence is also enclosed.

It is certified that performance of the Contract has been interfered with. It is also certified that the incident has not occurred due to our own action and that there has not been any lack of action by us in preventing the occurrence.

We are only claiming the extension in the date of completion of the activity (ies) and not claiming the loss incurred in the course of the incident.

Yours truly,

*(Project Manager)*

**Enclosures:**
1. Revised Bar Chart.
2. Evidence of the occurrence of the Force Majeure case (….. sheets)
Annexure V: Extension of time format

APPLICATION FOR EXTENSION OF TIME

Part-I

1. Name of the Contractor
2. Name of the work as given in the agreement
3. Agreement No.
4. Contract Amount
5. Date of Commencement of work as per agreement
6. Period allowed for completion of work as per agreement
7. Date of completion stipulated in agreement
8. Date of actual completion of work
9. Period for which extension is applied for.
10. Hindrances on account of which extension is applied for with dates on which hindrances occurred and the period for which these are likely to last.

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Name of Hindrance</th>
<th>Date of occurrence of hindrance</th>
<th>Date of over of hindrance</th>
<th>Period of hindrance</th>
<th>Overlapping Period</th>
<th>Net extension applied for</th>
<th>Remarks if any</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total period for which extension is now applied for on account of hindrances mentioned above.

11. Extension of time required for extra work.

12. Details of extra work and the amount involved:-
13. Total extension of time required for 10 & 11. Submitted to the Project Manager ____________________________.

Signature of Contractor
Dated

Part II
(For Official Use)

1. Date of receipt of application from ________________________________ Contractor for the work of ________________________________ in the office of the General Manager (IT) ________________________________.

2. Recommendations of the project Manager as to whether the reasons given by the contractor are correct and what extension, if any, is recommended by him. If he does not recommend the extension, reasons for rejection should be given.

Dated: ________________________________
Signature of the Installation In-charge

(To be filled in by the Project Manager)

1. Date of receipt in the Office:-

2. Project Manager’s remarks regarding hindrances mentioned by the contractor.

   (i) Serial No
   (ii) Nature of hindrance
   (iii) Date of occurrence of hindrance
   (iv) Period for which hindrance is likely to last
   (v) Extension of time applied for by the contractor
   (vi) Overlapping period, if any, giving reference to items which overlap
   (vii) Net period for which extension is recommended
   (viii) Remarks as to why the hindrance occurred and justification for extension recommended.

2. Project Manager’s Recommendations. The present progress of the work should be stated and whether the work is likely to be completed by the date up to which extension has been applied for. If extension of time is not recommended, what compensation is proposed to be levied under Clause 32 of the agreement.

Signature of Project Manager

Signature of Accepting Authority
Annexure VI: NDA

NON-DISCLOSURE AGREEMENT
(To be stamped in accordance with Stamp Act)

The Non-Disclosure Agreement (hereinafter called the “NDA”) is made on the [day] day of the month of [month], [year], between, Airports Authority of India, on the one hand, (hereinafter called the “Purchaser”) and, on the other hand, [Name of the bidder] (hereinafter called the “Bidder”) having its registered office at [Address].

WHEREAS
1. the “Purchaser” has issued a public notice inviting various organizations to propose for hiring services of an organization for provision of Information Technology Services (hereinafter called the “Project”) of the Purchaser;
2. the Bidder, having represented to the “Purchaser” that it is interested to bid for the proposed Project;
3. The Purchaser and the Bidder agree as follows:

In connection with the “Project”, the Purchaser agrees to provide to the Bidder a Detailed Document on the Project vide the tender document contained in different sections with Annexures. The Tender contains details and information of the Purchaser operations that are considered confidential.

The Bidder to whom this Information (Tender document) is disclosed shall:

1. hold such Information in confidence with the same degree of care with which the Bidder protects its own confidential and proprietary information;
2. restrict disclosure of the Information solely to its employees, agents and contractors with a need to know such Information and advise those persons of their obligations hereunder with respect to such Information;
3. use the Information only as needed for the purpose of bidding for the Project;
4. except for the purpose of bidding for the Project, not copy or otherwise duplicate such Information or knowingly allow anyone else to copy or otherwise duplicate such Information; and
5. Undertake to document the number of copies it makes Tender for “Development of Web Portal and Mobile Apps for AAI”.
6. on completion of the bidding process and in case unsuccessful, promptly return to the Purchaser, all Information in a tangible form or certify to the Purchaser that it has destroyed such Information.

The Bidder shall have no obligation to preserve the confidential or proprietary nature of any Information which:

1. was previously known to the Bidder free of any obligation to keep it confidential at the time of its disclosure as evidenced by the Bidder’s written records prepared prior to such disclosure; or
2. is or becomes publicly known through no wrongful act of the Bidder; or
3. is independently developed by an employee, agent or contractor of the Bidder not associated with the Project and who did not have any direct or indirect access to the Information.

4. Is required to be disclosed as per law or according to any legal process or administrative process of the government

The NDA shall apply to all Information relating to the Project disclosed by the Purchaser to the Bidder under the NDA.

Nothing contained in the NDA shall be construed as granting or conferring rights of license or otherwise, to the Bidder, in any of the Information.

The NDA shall benefit and be binding upon the Purchaser and the Bidder and their respective subsidiaries, affiliates, successors and assigns.

The NDA shall be governed by and construed in accordance with the Indian laws.

For and on behalf of the Bidder
(Signature)
(Name of the Authorized Signatory)
Date
Address
Location
Annexure VII: MAF

To,
The General Manager (IT)
Airports Authority of India,
Safdarjang Airport,
New Delhi

Subject: Manufacture Authorization Letter

Sir,

With reference to the Tender No. ___________ for, ___________we
__________________________ (Software Firms name) having our office in
__________________________ (Software Firms address), authorize
__________________________ (System Integrator name and address), our system Integrator
in India, to quote and supply to you the following Software product/Solution/License/Equipment:
1. ___________
2. ___________
3. ___________

We further certify that the products quoted are latest version of our standard product and our
standard OEM comprehensive support shall be available for next 5 years. We confirm that the
Warranty/Software Support for the products shall be to AAI irrespective of the involvement of
System Integrator. We also confirm that the products offered are currently available in the market
and shall not be end of life during the contract period.

Yours faithfully,

(Name)
(Name of the Manufacturers)

Note: This letter of authority should be on the letterhead of the manufacturer/Software OEM Firm
and should be signed by a person competent and having the power of attorney to bind the
manufacturer. It should be included by the Bidder in its bid.
Annexure VIII: Undertaking letter

Date: ____________
Place: ____________

To,
The General Manager (IT)
Airports Authority of India,
Safdarjung Airport,
New Delhi.

Subject: Undertaking Letter

Sir,

I hereby undertake that our firm ______________ (Company Name) or its partners or its directors are not currently black listed and no case or complaint is pending against its firm or its partners regarding irregularities, in India by any Indian State/Central Governments Departments or Public Sector Undertaking of India.

Yours faithfully,

(Name)
(Name of the Company)

Note: This letter of authority should be on the letterhead of the company and should be signed by a person competent and having the power of attorney.
Annexure IX: Integrity Pact

INTEGRITY PACT

This Pact made this …….day of……..between Airports Authority of India, a body corporate constituted by the Central Government under the Airports Authority of India Act, 1994 and having its Corporate Office at Rajiv Gandhi Bhawan, New Delhi, and offices at …………………………….in India, hereinafter called the Authority (which term shall unless excluded by or is repugnant to the context, be deemed to include its Chairman, or Member, Executive Directors, Airport Directors, Officers or any of them specified by the Chairman in this behalf, and shall also include its successors and assign) of the one part.

AND

……..represented by …………….of the other part, hereinafter called the “Bidder/Contractor” (which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the Bidder/Contractor)

WHEREAS the Authority intends to award, under laid down organizational procedures, tender/contract for ……………………………. The Authority, while discharging its functions on business principles, values proper compliance with all relevant laws and regulations, and the principles of natural justice, ethics, equity, fairness and transparency in its relations with the Bidders/Contractors;

WHEREAS the Authority is desirous to make its business mechanism more transparent, thus to ensure strict adherence of the aforesaid objectives/goals, the Authority hereby adopts the instrument developed by the renowned international non-governmental organization “Transparency International” (TI) headquartered in Berlin (Germany). The Authority will appoint an External Independent Monitor (EIM) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above;

AND WHEREAS the Bidder is submitting a tender to the Authority for ………………………………in response to the NIT (Notice Inviting Tender) dated…………/ Contractor is signing the contract for execution of……………………………

NOW, therefore, this indenture witnessed herewith:

SECTION 1. Commitment of the Authority

1.1. That the Authority commits itself to take all measures necessary to prevent corruption and to observe the following principles:

i. No employee of the Authority, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a Promise for or accept for him/her or third person, any material or immaterial benefit, which he/she is not legally entitled to.
ii. The Authority will, during the tender process treat all Bidders with equity and reason. The Authority will in particular, before and during the tender process, provide to all Bidders the same information and will not provide to any Bidder Confidential/additional information through which the Bidder could obtain an advantage in relation to the tender process or the contract execution.

iii. The Authority will take all measures to exclude all known prejudiced persons from the tender process.

1.2. That if the Authority receives information on the conduct of any of its employee which is a criminal offence under the relevant anti-corruption laws of India, or if there be a substantive suspicion in this regard, the Authority will inform its Vigilance Department to initiate appropriate action.

SECTION 2. Commitments of the Bidder/Contractor

2.1. That the Bidder/Contractor commits itself to take all measures necessary to prevent corruption. Further he commits himself to observe the following principles during his participation in the tender process and during the contract execution:

i. The Bidder/Contractor has not offered, promised or given and will not, directly or through any other person or firm, offer, promise or give to any of the Authority’s employees involved in the tender process or the execution of the contract or to any third person, any material or immaterial benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

ii. The Bidder/Contractor has not entered and will not enter with other bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

iii. The Bidder/Contractor has not committed and will not commit any offence under the relevant Anti-Corruption Laws of India. Further the Bidder/Contractor will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Authority as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

iv. The Bidder/Contractor will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

v. The Bidder/Contractor will inform the External Independent Monitor:

a) If he receives demand for an illegal/undue payment/benefit.

b) If he comes to know of any unethical or illegal payment/benefit.
c) If he makes any payment to any Authority’s associate(s).

vi. The Bidder(s)/Contractor(s) will not submit a frivolous/false/bogus complaint with malafide intention.

2.2. That the Bidder/Contractor will not instigate any person to commit offences mentioned in Clause 2.1 above or be an accessory to such offences.

SECTION 3. Disqualification from tender process and exclusion from future contracts

3.1. That if the Bidder(s)/Contractor, during tender process or before the award of the contract or during execution of the contract/work has committed a transgression in violation of section 2 or in any other form such as to put his reliability or credibility as Bidder(s)/Contractor into question, the Authority is entitled to disqualify him from the tender process or to terminate the contract for such reason.

3.2. That if the Bidder/Contractor against whom any action in terms of Section 3.1 above has already been taken in any other tender/contract process, again commits a transgression in violation of section 2 such as to put his reliability or credibility into question, the Authority is entitled also to debar the Bidder/Contractor from future tender/contract processes. The imposition and duration of the debarment will be determined by the severity of the transgression. The severity will be determined taking into consideration the circumstances of the case, in particular the number of transgression, the position of the transgressor within the company hierarchy of the bidder and the amount of the damage. The debarment will be imposed for a period minimum of six months and maximum of five years.

3.3. That the Bidder/Contractor accepts and undertakes to respect and uphold the Authority’s absolute right to resort to and impose such debarment and further accepts and undertakes not to challenge or question such debarment on any ground.

3.4. That if the Bidder/Contractor applies to the Authority for premature revocation of the debarment and proves to the satisfaction of the Authority that he has installed a suitable and effective corruption prevention system and also restored/recouped the damage, if any, caused by him, the Authority may, if thinks fit, revoke the debarment prematurely considering the facts and circumstances of the case, and the documents/evidence adduced by the Bidder/Contractor for first time default.

3.5. That a transgression is considered to have occurred if the Authority is fully satisfied with the available documents and evidence submitted along-with External Independent Monitor’s recommendations/suggestions that no reasonable doubt is possible in the matter.

SECTION 4. Previous transgression

4.1. That the Bidder/Contractor declares that no previous transgression occurred in the last five years with any other company in any country or with any other Public Sector Enterprise in India conforming to the TI approach that led to debarment/disqualification and could justify his exclusion from the tender process.
4.2. That if the Bidder/Contractor makes incorrect statement on the subject, he can be disqualified from the tender process or the contract, if already awarded can be terminated for such reason and he may be considered for debarment for future tender/contract processes.

SECTION 5. Compensation for damages

5.1. That if the Authority has disqualified/debarred the Bidder from the tender process prior to the award under section 3 or 4, the Authority is entitled to forfeit the earnest money deposited/bid security.

5.2. That if the Authority has terminated the contract under section 3 or 4, or if the Authority is entitled to terminate the contract under section 3 or 4, the Authority shall be entitled to demand and recover from the contractor damages equivalent to 5% of the contract value or the amount equivalent to security deposit or performance bank guarantee, whichever is higher.

5.3. That the Bidder/Contractor agrees and undertakes to pay the said amount without protest or demur subject only to condition that if the Bidder/Contractor can prove and establish to the satisfaction of the Authority that the disqualification/debarment of the bidder from the tender process or the termination of the contract after award of the contract has caused no damage to the Authority.

SECTION 6. Equal treatment of all Bidders/Contractors/Sub-contractors/ associates

6.1. That the Bidder/Contractor undertakes to get this Pact signed by the sub-contractor(s) and associate(s) whose value of the work contribution exceeds Rs. 5 (Five) Crores, and to submit the same to the Authority along with the tender document/contract before contract signing.

6.2. That sub-contractor(s)/associate(s) engaged by the Contractor, with the approval of the Authority after signing of the contract, and whose value of the work contribution exceeds Rs.5 (Five) Crores will be required to sign this Pact by the Contractor, and the same will be submitted to the Authority before doing/performing any act/function by such sub-contractor(s)/associate(s) in relation to the contract/work.

6.3 That the Authority will disqualify from the tender process all Bidder(s) who do not sign this Pact or violate its provisions or fails to get this Pact signed in terms of section 6.1 or 6.2 above.

6.4 That if the Contractor(s) does/does not sign this Pact or violate its provisions or fails to get this Pact signed in terms of section 6.1 or 6.2 above, Authority will terminate the contract and initiate appropriate action against such Contractor(s).

SECTION 7. Allegations against bidders/contractors/sub-contractors/ associates.

7.1. That if the Authority receives any information of conduct of a Bidder, Contractor or Sub-contractor, or of an employee or a representative or an associates of a Bidder, Contractor or Sub-contractor which constitutes corruption, or if the Authority has substantive suspicion in this regard, the Authority will inform the Vigilance Department for appropriate action.
SECTION 8. External Independent Monitor(s), number depending on the size of the contract to be decided by the Chairman of the Authority.

8.1. That the Authority will appoint competent and credible External Independent Monitor(s) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact. He will also enquire into any complaint alleging transgression of any provision of this Pact made by the Bidder, Contractor or Authority.

8.2. That the Monitor is not subject to any instructions by the representatives of the parties and would perform his functions neutrally and independently. He will report to the Chairperson of the Board of the Authority.

8.3. That the Bidder/Contractor accepts that the Monitor has the right to access without restriction to all project documentation of the Authority including that provided by the Bidder/Contractor. The Bidder/Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to subcontractors and associates. The Monitor is under obligation to treat the information and documents of the Authority and Bidder/Contractor/Sub-Contractors/ Associates with confidentiality.

8.4. That the Authority will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meetings could have an impact on the contractual relations between the Authority and the Contractor/Bidder. The parties offer to the Monitor the option to participate in such meetings.

8.5. That as soon as the Monitor notices, or believes to notice, a violation of this Pact, he will so inform the management of the Authority and request the management to discontinue or heal the violation, or to take other relevant action. The Monitor can in this regard submit his recommendations/ suggestions. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

8.6. That the Monitor will submit a written report to the Chairperson of the Board of the Authority within 2 weeks from the date of reference or intimation to him by the Authority and, should the occasion arise, submit proposals for correcting problematic situations.

8.7. That if the Monitor has reported to the Chairperson of the Board a substantiated suspicion of an offence under relevant Anti-Corruption Laws of India and the Chairperson has not, within reasonable time, taken visible action to proceed against such offence or reported it to the Vigilance Department, the Monitor may also transmit this information directly to the Central Vigilance Commissioner, Government of India.

8.8. The word ‘Monitor’ would include singular and plural.

9.1. That this Pact comes into force when both the parties have signed it. It expires for the Contractor 12 months after the final payment under the respective contract, and for all other Bidders 3 months after the contract is awarded.

9.2. That if any claim is made/lodged during this period, the same shall be binding and continue to be valid despite the lapse of this Pact as specified herein before, unless it is discharged/determined by Chairman of the Authority.

SECTION 10. Miscellaneous provisions.

10.1. That this Pact is subject to Indian Laws. Place of performance and jurisdiction is the Corporate Headquarter/the Regional Headquarter/offices of the Authority, as applicable.

10.2. That the changes and supplements as well as termination notices need to be made in writing.

10.3. That if the Contractor/Bidder is a partnership or a consortium, this Pact must be signed by all the partners and consortium members, or their authorized representatives.

10.4. That should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact remains valid. In this case the parties will strive to come to an Agreement to their original intentions.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For the Authority</td>
<td>For the Bidder/Contractor</td>
</tr>
<tr>
<td>Place 123456</td>
<td>Witness 1 : 123456</td>
</tr>
<tr>
<td>Date 123456</td>
<td>Witness 2 : 123456</td>
</tr>
</tbody>
</table>
Annexure X: Bank Guarantee format for EMD

BANK GUARANTEE FORMAT FOR EMD
(On Non-judicial stamp paper of Rs.100.00)

Bank Guarantee

The Chairman,
Airports Authority of India, CHQ, Rajiv Gandhi Bhawan,
Safdarjung Airport,
New Delhi 110 003, INDIA

Dear Sir,

We __________________ (full name of the banker) hereby refer to the tender for (“Name of the work as given in Schedule-A Sr. No. 1”) between the Airports Authority of India as purchaser and M/s ____________ (fill in the name of tenderer) as tenderer providing in substance for ……………..(name of work) as particularized in said tender, to which specific reference is made. Under the terms of said tender, the tenderer is required to provide a bank guarantee in a form acceptable to the purchaser for the amount of Rs………(amount in figures)(Rupees ………………………..) on account of EMD.

In view of the foregoing and pursuant to the terms of the said tender, which tender is referred to and made a part thereof as fully and to the same extent as if copied at length hereon, we hereby absolutely and unconditionally guarantee to the purchaser, performance of the terms and conditions of the said tender. The guarantee shall be construed as an absolute, unconditional and direct guarantee of the performance of the tender without regard to the validity, regularity or enforceability of any obligation of the parties to the tender.

The purchaser shall be entitled to enforce this guarantee without being obliged to resort initially to any other security or to any other remedy to enforce any of obligations herein guaranteed any may pursue any or all of its remedies at one or at different times. Upon default of the tender, we agree to pay to the purchaser on demand and without demur the sum of Rs………(amount in figures)(Rupees ………………………..) or any part thereof, upon presentation of a written statement by the purchaser that the amount of said demand represents damages due from the tenderer to the purchaser by virtue of breach of performance by the tenderer under the terms of the aforesaid tender. The determination of the fact of breach and the amount of damages sustained and or liability under the guarantee shall be in the sole discretion of the purchaser whose decision shall be conclusive and binding on the guarantor.

It is mutually agreed that the purchaser shall have the fullest liberty without affecting in any manner our obligation hereunder with or without our consent to vary any of the terms of the said tender or to extend the time for performance by the tenderer, from time to time any of the powers exercisable by the purchaser against the tender and either to forebear or on force any of the terms and conditions relating to the said tender and we shall not be relieved from our liability by reasons of any variation of any extension being granted to the tender or for any forbearance act or commission on the part of the purchaser or any indulgence by the purchaser to the tenderer or by any such matter or thing whatsoever which under the law relating to the sureties would but for this provision have effect of so relieving our obligation.

Tender ID: 2018_AAI_15726_1
This guarantee is confirmed and irrevocable and shall remain in effect until ____________________________
(the validity shall be eight months from the notified date of opening of Tender) and such extended periods which may be mutually agreed to. We hereby expressly waive notice of any said extension of the time for performance and alteration or change in any of the term and conditions of the said tender.
Very truly yours,

____________________
(Authorized Signatory of the Bank)
Annexure XI: Format for Undertaking of Not being Blacklisted

UNDERTAKING OF NOT BEING BLACK LISTED
(To be submitted on the Letterhead of the Bidder)

<Date>

General Manager (IT)
Airports Authority of India, CHQ
Safdarjang Airport,
New Delhi

Kind Attn: Director (IT)

Dear Sir,
We confirm that our company is not blacklisted in any manner whatsoever by any State Government, Central Government or any other Public Sector undertaking or Corporation or Any other Autonomous organization of Central or State Government as on Bid submission date.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Sincerely,

<Signature> <Company Seal>
Name:
Designation:
Name and Address of Company:
Annexure XII: No Deviation Certificate

The certificate below is to be provided by the bidder.

<To be printed on Company letterhead>

This is to certify that our offer is exactly in consonance with your RFP no. __________ dated __________ and subsequent amendments / corrigendum’s etc. This is to expressly certify that our offer contains no deviation on Technical (including but not limited to Scope of Work, Functional Requirements Specification, Technical Requirements Specification, Operational and Infrastructure requirements of Digital Sky Platform as laid out in RFP), Legal or Commercial aspects in either direct or indirect form.

Any deviations in respect to the RFP may thus be liable for rejection.

Yours sincerely,
<Date>
<on behalf of Bidder Name>
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Firm:
Address:
Seal/Stamp of Bidder:
Airports Authority of India
Information Technology Division
Safdarjung Airport, New Delhi - 110 003

SCOPE OF WORK

Development, Hosting and Maintenance of Digital Sky Platform for Ministry of Civil Aviation

TENDER NO.: IT-11042/1/2018-DIRECTORATE OF IT
Tender ID: 2018_AAI_15726_1

Date: 26-09-2018
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

**Table of Contents**

1. Digital Sky Program Overview................................................. 3
2. Digital Sky Project Requirements - Summary................................. 5
3. Scope of work........................................................................ 7
4. Roles & Responsibilities.......................................................... 40
5. Change Control Process ........................................................... 41
6. Project Governance.................................................................. 46
7. Manpower requirements............................................................ 46
8. Project Management................................................................. 48
9. Compliance to Industry Standards.............................................. 49
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

1. Digital Sky Program Overview

The global technology landscape is emerging at a fast pace which provides both an opportunity and a challenge. Governments worldwide must ensure that policy fundamentals are contemporary and forward looking to provide a strong foundation for technology enabled growth. UAV technology is one such area that is gaining momentum worldwide due to its varied scope of application, and diverse set of use cases for developed as well as developing countries.

The UAV technology has myriad use cases relevant to India for application in areas such as healthcare, security, agriculture, energy etc. to name a few. India already has a significant number of operational UAVs, which are most likely to grow in numbers at an exponential pace. To support this emerging and promising technology, a strong regulatory framework is essential to ensure that the technology proliferates in a sustainable manner without any unintended consequences. To this effect, a Civil Aviation Rule (CAR) was issued by the DGCA which lays down the fundamentals for UAV operations in India.

With the issuance of the rules, there is expected an exponential growth of Drones adoption in India. In order to support such growth, India will require a strong technology platform for governance of Drones. In this regards, Digital Sky platform is envisioned to provide end-to-end governance of drones related activities.

The key objective of Digital Sky are as follows:

1. Registration and Approvals: Allow manufacturers and pilot to obtain permits and licenses online
2. Permissions: Provide online approvals for drones flights without manual intervention
3. Enforcement: Enforce drones flight activities as per approvals and compliance requirements
4. Compliance Vigilance: Undertake continuous checks through analytics to ensure overall compliance

1.1 Digital Sky Process Envisaged

The envisaged platform will cover the entire gamut of activities related to governance of UAVs to ensure that each step is executed digitally for efficient monitoring. The process will cover various participants in the ecosystem such as manufacturers, operators and pilots for activities ranging from registration, approval, operation and post flight analysis. The broad areas to be covered under the Digital Sky framework are the following:

- **Registration of Manufacturers/Drones**: Approvals for manufacturing and sale of UAVs after seeking requisite approvals wherein various aspects such as operating procedures, maintenance requirements etc. shall be reviewed by DGCA. Further, issuance of Unique Identification (UID) for Drones shall also be undertaken through Digital Sky.

- **Pilot License/Operator Permits**: Licenses and Permits provided to individuals and organizations to undertake activities related to Drones in India

- **Airspace Management**: Automate air space management (no fly zone, flight paths, altitude, etc) to ensure UAV flight approvals/operations are within the bounds of regulation and under the scope of intended usage.

- **Flight Approvals**: Automated approvals with compliance checks related to drone type, pilot, operator, flight path, intended usage, etc. undertaken automatically and approval provided based on pre-defined rules.
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

- **Digital Enforcement**: Drones flight compliance to ensure that no flight is undertaken without prior approval and all flights adhere to boundaries defined within the approval certificate.

- **Analytics**: Continuous vigilance on flights undertaken and identifying non-compliance and other insights for action/improvements in policy, implementation of Digital Sky.

- **Incident reporting and enforcement**: Provision for pilots and operators to report any incidents for necessary action by the regulator. Provision for regulator to check compliance and undertake enforcement actions at a granular level such as grounding UAVs of a particular manufacturer, restricting operators/pilots etc.

The diagram below provides a brief snapshot of how the Digital Sky is envisioned to work:

**HOW DIGITAL SKY WILL WORK**

For further process details and functional requirements, please refer Appendix of Scope of Work.
2. Digital Sky Project Requirements - Summary

2.1 Current Status

DGCA and AAI in collaboration with iSPIRIT has developed Digital Sky Application for testing purpose. For the same, the application has also been demonstrated in a controlled environment.

The details of the application and functionalities is provided in Scope of Work - Appendix 1 - Development of Digital Sky Pilot Phase

2.2 Project Scope

The overall Digital Sky project is broadly comprising of the following areas:

1. **Implementation Phase Scope**
   a. Project Planning
   b. Hosting of Beta Version of Developed Digital Sky Application
   c. **System Requirement Elicitation and System Design**: Understanding the envisaged operations of Digital Sky and thereon developing required documents such as FRS, BRD, SRS, etc. based on such understanding.
   d. **Solution Development, Testing & Go Live** of Digital Sky System in 2 Phases including integration with other systems
   e. **Cloud Provisioning and Commissioning**

2. **O&M Phase Scope**
   a. **O&M** (5 Years post Go Live of all phases)
   b. **Training Execution**
   c. **Digital Sky Business Support and Grievance Cell** (5 Years post Go Live): For providing business and technical support.

2.3 Digital Sky Project Timelines

<table>
<thead>
<tr>
<th>Deliverables/Activities</th>
<th>Timelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1: Hosting of Beta Version of Application Developed by AAI</td>
<td>Hosting (Go-Live) of Beta Version</td>
</tr>
<tr>
<td>System Design</td>
<td>Refer Section 3.1 and 3.2</td>
</tr>
</tbody>
</table>

---

1 Refer Section 3.3
2 Code Handoff and Deployment of the Code in the new CSP Environment and will maintain the system in Beta Phase; No SLAs are applicable during this period
3 The MSP at this stage will be fully responsible for the hosted application and SLA shall start to apply on MSP for the hosted application. Further, the MSP is required to Go-Live with the latest application version (and the hosted application shall no more be categorized as the beta version)
2.4 Payment Schedule

All payments will be made upon due approval(s) of the deliverables from AAI.

<table>
<thead>
<tr>
<th>Milestones</th>
<th>Payments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1: Hosting of Beta Version of Application Developed by AAI</td>
<td>5% of Implementation Phase</td>
</tr>
<tr>
<td>SRS Sign-off</td>
<td>5% of Implementation Phase</td>
</tr>
<tr>
<td>Completion of Testing of Beta Version and Security Certification of Hosted Beta Version Digital Sky Application</td>
<td>10% of Implementation Phase</td>
</tr>
<tr>
<td>Go Live of Phase 2 Services</td>
<td>30% of Implementation Phase</td>
</tr>
<tr>
<td>Go Live of Phase 3 Services</td>
<td>35% of Implementation Phase</td>
</tr>
<tr>
<td>3 months post Go-Live of Phase 3</td>
<td>15% of Implementation Phase</td>
</tr>
<tr>
<td>Operations and Maintenance phase including hosting cost</td>
<td>In Equal quarterly instalments as per O&amp;M Phase value post Go Live of Phase 3</td>
</tr>
</tbody>
</table>

**NOTE:** The project (O&M Phase) can be extended by upto 2 years at the sole discretion of AAI, on same terms and conditions on which current contract (under this RFP and any other corrigendum/addendum issued thereto) has been finalized between AAI and MSP.

---

4 Phase 2: Process and Services in Pre Flight Module (Refer Scope of Work - Appendix 3 - Digital Sky - Envisioned Process Flow)
5 Phase 3: Process and Services in Take off Module + Post Flight Module (Refer Scope of Work - Appendix 3 - Digital Sky - Envisioned Process Flow)
6 O&M Phase shall start post Go-Live of all phases. Any Go-Live of services in Phase 1 & 2 will have to be operated and maintained during the implementation phase in accordance to scope laid down for O&M. In this regards, for the purpose of costing, MSP should consider all O&M support (prior to Go-Live of all services) for Phase 1 & 2 services as part of Implementation Phase.
3. Scope of work
The following sections provide details of the scope of work:

3.1 Project Planning
1. The MSP needs to prepare an Integrated Project Plan for the entire project. Project plan should provide a detailed drill down of all activities to be undertaken. This includes details of tasks, assigned teams for undertaking responsibilities for the task, schedule of deliverables and milestones, key assumptions and dependencies, associated risks and mitigation plans.
2. The MSP’s program of work should be synchronized with the staff deployment plan proposed; the deployment plan shall clearly define onsite and offsite deployment plan and personnels under each deployment category along with engagement period for the project.
3. The MSP should use cloud based project management tool and provide access to the same to key stakeholders identified by AAI/DGCA (100 stakeholders). The tool should provide all features related to project management requirements of the project. Also, the PM tool have function to auto update stakeholders over Email/SMS
4. The prepared project plan should allow teams to track the progress of various deliverables and milestones, through the scheduled review mechanisms.
5. The acceptance of the Integrated Project Plan by AAI is necessary before proceeding to the next phase of the project.
6. Approval by AAI of the proposed plan shall not relieve the MSP of any of his duties or responsibilities under the Contract. However, if the MSP’s work plans necessitate a disruption/shutdown in Digital Sky’s operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum.
7. The program so submitted by the MSP shall conform to the requirements and timelines specified in the RFP.
8. Any time and cost arising due to failure of the MSP to develop/adhere such a work plan shall be to his account.

Deliverable(s)7:
1. Integrated Project Plan including:
   a. Milestones
   b. Resource deployment
   c. Risks and their mitigation plan
   d. Dependencies
   e. Responsibility matrix
2. Configuration of Project Management Tool
3. Submission of Project Charter to include:
   a. Risk Management and Mitigation plan
   b. Information Security Plan
   c. Communication Plan
   d. Data Migration plan

7 Please note that the deliverables are indicative in terms of enlistment; kindly refer the entire section for comprehensive view on the deliverables requirements. The same holds for the all the sections in the scope of work.
3.2 System Requirement Elicitation and System Design

3.2.1 Requirement Gathering & Analysis

1. Detailed functional requirements and process flow (Appendix) is provided in this RFP. MSP is required to validate the same and fill gaps (that may be identified at this stage). Further, the MSP is to further elaborate the functional requirements and process flow, based on discussion with AAI, from a systems perspective.

2. The requirement gathering should cover (but not be limited to) workflows, business rules, validations, regulatory / legal requirements/security requirements etc. On basis of the requirements gathered, the MSP is required to prepare an SRS document.

3. SRS document shall comply with the latest and most relevant IEEE standards.

4. The MSP is also required to prepare a Requirements Traceability Matrix (RTM) to establish the design, development, testing and roll-out of various functionalities and non-functional (and Technical) requirements. It should include mapping of: BRD, FRS, SRS, LLD, DFD, and other relevant documents (as per need).

5. The RTM will act as basis for analysis of change requests that may arise during the course of operations and maintenance of the solution.

6. The MSP is required to get a sign-off / approval on the SRS document in order to commence the design stage of the project.

**Deliverable(s):**

1. Business Requirement Document (BRD)
2. Functional Requirement Specification (FRS)
3. Data Flow Diagram (DFD)
4. Software Requirement Specifications (SRS)
5. Requirements Traceability Matrix (RTM)

3.2.2 Solution Design

1. The MSP shall design the solution architecture and specifications to meet the functional and technical requirements mentioned as part of this RFP. The MSP shall be entirely responsible for the design and architecture of the proposed Digital Sky system and its successful operations for the period defined in the RFP. Please refer Appendix for the details of solution requirements. Solution architecture description provided in Appendix of RFP is for reference only and the MSP is expected to propose the best solution (software, hosting environment, security components etc.) which address the requirements of Digital Sky.

2. MSP would need to appropriately size the solution (including the bandwidth) for successful operations, meeting the SLAs, for the contract period. Any additional component required for the successful operations of the Digital Sky solution, during the contract period, would be provided by the MSP at no extra cost to AAI.

3. The system architecture for the integrated solution shall be designed, developed & delivered as per following:
## General Guidelines

1. Solution components should be open source based and should be provided with enterprise support. All supported product by CSP is acceptable provided they are open source. In case of COTS products proposed, MSP shall provide detailed explanation of selection of the same in the proposal. Despite this, MSP may be still demanded to adopt open source product if deemed necessary by AAI.

2. It is declared that any source code shared with AAI shall be used only for non-commercial purposes and limited to use for Digital Sky. Hence, in case of proprietary products, MSP solution proposal may be accepted in case source code is shared for any proposed proprietary product except for standard software (OS/DB).

3. The solution design should be based on open industry standards and protocols.

4. The solution should be centrally deployed and globally accessed.

5. The solution should provide interoperability across Cloud Providers, Platforms.

6. The solution may use concepts such as Micro service based Container Architecture.

7. The solution should be modular, scalable and flexible as a true ‘Cloud Deployable’ solution.

8. Mobility services (mobile applications) should be a key solution component.

## Application

1. The solution design should be n-tier services based architecture for all environments.

2. The solution design should focus on developing workflow and business transaction, rules management, configuration management.

3. The solution design should be done in such a manner that components are loosely coupled; ensuring that the application components are treated individually and dependencies are reduced. The MSP should ensure that addition, removal, failure or update of one component has a minimum impact on other components.

4. The MSP should ensure that services should be written in such a way that they can be automated for testing. Test automation is necessary to ensure services can be upgraded, re-factored, etc. without breaking other services that use them. The MSP should ensure that all services should be inherently versioned and all invocations must specify the version of service.

5. The MSP should ensure that new versions of services should be backward compatible with at least three previous versions so that users of the service can start using new version of the service without mandatorily making changes to their code.

6. The solutions design should provide for service abstraction, to control what part of the service logic of a particular application needs to be private (hidden) and which parts need to be made public (consumable).

7. The solution should not only be modular in nature, but be adaptive to converse with other technology components such as platforms and databases, complete with management suites or with the induction of adaptors and interfaces or even smaller bespoke solutions to support the same.

8. All applications must take into account appropriate security, performance, efficiency and maintainability issues based on the functional, technical and non-functional requirements and the defined SLAs.

9. The ownership of the product licenses, wherever applicable, would be with AAI or nominated government agency by AAI.

10. The solution must be supported by at least ‘N-3’ versions of any underlying products. This will be required in case some / other functionalities become non-functional upon deployment on the latest version, or in case a roll-back is required.

11. Any products (wherever applicable) which would be part of the solution must be of the latest commercially available version.

   - Products must be supported in terms of upgrades, bug fixes, functionality enhancements and patches to cater to changes to statutory requirements.
by their respective OEM for the entire duration of the contract plus 6 months after end of contract.
- OEM support should be made available on all deployed versions for the contract period.

12. The MSP shall provision for following hosting environments –
- Development Environment
- UAT environment
- Production Environment
- DR Environment

The development setups shall be outside the cloud hosting environment.

<table>
<thead>
<tr>
<th>3</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Data will be owned, shared, controlled and protected as a corporate asset of AAI or nominated government agency by AAI.</td>
</tr>
<tr>
<td>2.</td>
<td>Data should only be accessed through application / interfaces for create, update and delete. There should not be any direct access to the data layer for users.</td>
</tr>
<tr>
<td>3.</td>
<td>The MSP shall provide the details of data synchronization strategy both in batch mode and in real time. AAI, in consultation with MSP, shall decide on the methodology of data synchronization based on service requirements</td>
</tr>
<tr>
<td>4.</td>
<td>Data Entry: All the data entry in the system shall be performed in English only</td>
</tr>
</tbody>
</table>

**Deliverable(s):**

1. High Level Design (HLD)
2. Low Level Design (LLD)
3. Solution Architecture, including:
   a. Business Architecture
   b. Application Architecture
   c. Integration Architecture
   d. Technology Architecture
   e. Security architecture
   f. Deployment Architecture
3.3 Hosting of Beta Version of Digital Sky Pilot Application Developed by AAI

AAI in collaboration with iSPIRIT has developed a pilot Digital Sky application, both portal and mobile (Refer Scope of Work - Appendix 1 - Development of Digital Sky Pilot Phase).

The same application is required to be hosted on the cloud (as per defined criteria in the cloud section) and maintain the application accordingly. Further, MSP in collaboration with iSPIRIT is required to undertake all necessary performance testing, load testing, security testing on the application and highlight all gaps and issues in the current features of the developed application by MSP. Such identified errors are to be thereon rectified in collaboration with iSPIRIT team. The MSP in this regards is thereon required to undertake responsibility of the hosted application as per timelines defined in Section 2 of the Scope of Work Document.

It is to be noted that MSP is encouraged to use the developed application and build on the same for completion of Digital Sky application (as part of scope defined in Phase 2 and 3). MSP however, will be responsible for the application developed overall irrespective of the method adopted (develop application from scratch or on already developed application by iSPIRIT/AAI). It is further highlighted that the code developed by iSPIRIT and other enhancements shall be closed source and the same shall not be re-used for any other purpose unless written consent is received from AAI.

3.4 Solution Development, Testing and Go-Live of Digital Sky Platform

3.4.1 Development of Digital Sky Portal

1. Based on the approved design and requirements finalized, the MSP will undertake development of solution

2. The MSP will be responsible for supplying the application, licenses, database and related software, integration tools and installing the same so as to meet the requirements mentioned in various sections of this RFP.

3. The MSP needs to provide configuration, customization and installation reports to AAI. In case of any COTS products, the MSP should follow disciplined approach (as per the best practice defined by the OEM) for configuration and customization which should not restrict AAI for any future upgrades to its solution.

4. The MSP should ensure solution sustainability to meet all RFP requirements, any additional procurement required will have to be taken by the MSP with no additional cost to AAI

5. Other related requirements are mentioned below:

   a) The application software developed by the MSP has to be user friendly so that users can access it without having extensive training.

   b) The MSP shall also supply any other tools & accessories required to complete the integrated solution per requirements. For the integrated solution, the MSP shall supply:

      i. Software & licenses

      ii. Tools, accessories, documentation and prepare a list of items supplied. Tools and accessories shall be part of the solution. MSP should provide technologies matrix.
iii. Supply latest supported version of all software to support the solution and any other software, tools and bolt-on/add-on application.

iv. System Documentation: System Documentation both in hard copy and soft copy.

3.4.2 Development of Digital Sky Mobile App

The key responsibilities of the MSP with regard to native mobile apps development for various Digital Sky services include:-

1. The primary scope of work of MSP is to launch, install, integrate, scale-up, test and maintain mobile applications on Android and iOS Platform.
2. To enable all the functionalities & services for the mobile app as per the provision of this RFP.
3. The MSP shall develop and manage the app with all the appropriate security features as per industry standards.
4. MSP shall ensure regular updation of mobile app to keep it abreast with latest operating system changes
5. MSP shall take regular feedback from users to continuously upgrade the UI/UX of design aspects of app.
6. MSP shall extend the functionality of AI based virtual assistant, chat agents and click-to-call options to app and portal.
7. MSP shall make all efforts to keep the app as light as possible to ensure fast and responsive design
8. The MSP shall perform a comprehensive mobile application testing. The test plans, test cases and results for each of the phases will be shared by MSP with AAI.
9. The application shall support deep linking
10. The mobile app should be Resolution independent that will automatically expand/compress itself as per the device screen resolution.
11. Product Delivery should be in the form of a published mobile application on each platform in the market place (Google Play store, Apple App store) and will be under the AAI accounts of these stores. No additional payments shall be made to MSP for publishing of mobile application
12. Web and Mobile applications source code and documents will be the property of AAI
13. App design complies with each platform’s advocated, documented design principles. The iOS app shall comply with Apple’s Human Interface Guidelines, while the Android version follows Material Design principles
14. App shall provide option to store data locally in App
15. Mobile applications shall support the low end smartphones devices
16. The Applications should provide a force update feature in case of newly published version of the applications. All apps shall be kept updated in terms of changes/updates undertaken
17. The App must be able to send reminder email, SMS or push notifications to respective registered user to enter/ update the relevant information. SMS Services Application/Module/Gateway to be fully integrate with the application by the vendor at no extra cost to AAI
18. Mobile applications developed on development platform provided by the bidder should run on all types of handsets/TAB/Smart phone existing as well as new handsets coming in the market. The bidder shall provide upgrades/patches etc. required for the same without any additional cost
19. Guidelines for the development of e-Governance applications (GuDAApps) as developed by NIC shall be followed for the development of the Digital Sky
20. The MSP shall also facilitate user acceptance testing (UAT) environment for the mobile apps.

3.4.3 Solution Testing

a. Planning for Testing

1. Once the SRS is approved and design has started, the MSP would prepare all necessary Test Plans (including test cases), i.e., plans for Unit Testing, Integration and System Testing and User Acceptance Testing.
2. Test cases for UAT would be developed by MSP and approval of the same is to be obtained by AAI.
3. The Test Plans also include planning for the testing to demonstrate the ability to integrate with 3rd party solutions. The Test Plans should also specify any assistance required from AAI and should be followed upon by the MSP.
4. The MSP is required to get a sign-off / approval on the Test Deliverables (Strategy, Plan, Designs and Specifications etc.) in order to commence the testing for the proposed solution.
5. The MSP is required to make all necessary arrangements for testing (integration, system, functional and user acceptance) including the preparation of test data, scripts where necessary; and procurement and setup of test environments and shall be the responsibility of the MSP.

Deliverable(s):

1. Test Strategy
2. Test Plan
3. Test Design
4. Test Case Specification

b. Unit Testing, Integration Testing, UAT

1. MSP shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing.
2. Though AAI is required to provide formal approval for the test plan, it is the responsibility of MSP to ensure that the end product delivered meets all the requirements (including functional and technical requirements) of the project processes specified in the RFP.
3. MSP shall carry out the unit testing of the application in accordance with the approved test plans.
4. After successful unit testing of all components, MSP shall conduct integration testing in accordance with the approved test plans. This shall include exhaustive testing including functional testing and security testing. Functional testing will be led by the MSP’s domain experts.
5. MSP will plan all aspects of UAT (including the preparation of test data) and obtain required assistance from AAI to ensure its success. AAI will assemble representatives from different user groups based on inputs from MSP and shall facilitate UAT. MSP shall make the necessary changes to the application to ensure that Digital Sky successfully goes through UAT.
6. MSP shall be required to make necessary changes in the SRS as well as other necessary documents based on the changes made during UAT.
7. It is the responsibility of the MSP to ensure that all required infrastructure to conduct the User Acceptance Testing are installed at required locations.
8. For the purposes of this RFP, User Acceptance (for Digital Sky) will include successful service provisioning to stakeholders on the new Digital Sky system to the satisfaction of the AAI project director.
Deliverable(s):

1. Test Logs
2. Test Data
3. User Acceptance Report

c. Performance Testing, Security Certification

1. Performance testing of the solution would be carried out using the envisaged peak load with a multiplier, to monitor the application response times and other performance parameters. Performance testing would be carried out every 6 months to ensure the application performance is as per requirement. Any additional hardware, software and any other components required to meet the performance SLAs, would be provided by the MSP at no extra cost.

2. MSP is required to submit the report for the performance testing to Digital Sky; the testing will be monitored by PMU or TPA

3. Performance testing would include load / stress testing. This would need to be carried out on the exact architecture as would be used in the production environment (solution architecture as well as computing capacity). All necessary tools to carry out testing would be provided by MSP.

4. MSP is required to obtain ISO27001-13 certifications within 6 months of GO-LIVE of Digital Sky services and must maintain the same throughout the contract duration.

Deliverable(s):

1. Performance Test Reports
2. Load Test Report
3. Security Certifications

d. Go-Live

1. For the purpose of RFP, “Go-Live” is the defined as the date on which all of the services listed in various phases is completely operational and accepted by AAI as per the requirements in this RFP. The below describe the criteria of acceptance:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Criteria of acceptance</th>
</tr>
</thead>
</table>
| Functional Requirements Review           | ▪ The Digital Sky system developed/customized by MSP shall be reviewed and verified by the agency against the functional requirements signed-off between AAI and MSP.  
                                           | ▪ One of the key inputs for this testing shall be the traceability matrix to be developed by the MSP for Digital Sky system.                          
                                           | ▪ Apart from Traceability Matrix, MSP may develop its own testing plans for validation of compliance of system against the defined requirements.      
<pre><code>                                       | ▪ The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (external auditors) as well as the select internal department users (for User Acceptance Testing). |
</code></pre>
<p>| Cloud Infrastructure compliance review   | ▪ Third party agency shall perform the Cloud Infrastructure Compliance Review to verify the conformity of the Infrastructure                          |</p>
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Criteria of acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement supplied by the CSP/MSP against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by MSP.</td>
<td>▪ Compliance review shall not absolve MSP from ensuring that proposed infrastructure meets the Service Levels requirements.</td>
</tr>
<tr>
<td><strong>Security Review</strong></td>
<td>The software developed/customized for Digital Sky system shall be audited by the agency from a security and controls perspective. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the Digital Sky system for the following activities:</td>
</tr>
<tr>
<td></td>
<td>▪ Audit of Network, Server and Application security mechanisms</td>
</tr>
<tr>
<td></td>
<td>▪ Assessment of authentication mechanism provided in the application/components/modules</td>
</tr>
<tr>
<td></td>
<td>▪ Assessment of data encryption mechanisms implemented for the solution</td>
</tr>
<tr>
<td></td>
<td>▪ Assessment of data access privileges, retention periods and archival mechanisms</td>
</tr>
<tr>
<td></td>
<td>▪ Server and Application security features incorporated etc.</td>
</tr>
<tr>
<td><strong>Performance/Load testing</strong></td>
<td>▪ Performance/load is another key requirement for Digital Sky system and agency shall review the performance of the deployed solution against certain key parameters defined in requirements and the service level metrics described in this RFP and/or agreement between AAI and MSP.</td>
</tr>
<tr>
<td></td>
<td>▪ Such parameters includes request response time, work-flow processing time, volume, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc.</td>
</tr>
<tr>
<td></td>
<td>▪ The performance/load review also includes verification of scalability provisioned in the Digital Sky system for catering to the requirements of application volume growth in future.</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>▪ Integrated Digital Sky system should be designed to remove all single point failures.</td>
</tr>
<tr>
<td></td>
<td>▪ Appropriate redundancy shall be built into all the components to provide the ability to recover from failures.</td>
</tr>
<tr>
<td></td>
<td>▪ The agency shall perform various tests including network, server, security, DC/DR failover tests to verify the availability of the services in case of component/location failures.</td>
</tr>
<tr>
<td></td>
<td>▪ The agency shall also verify the high availability of services to all the users of Digital Sky</td>
</tr>
<tr>
<td><strong>Manageability Review</strong></td>
<td>▪ The agency shall verify the manageability of the Digital Sky system and its supporting infrastructure deployed</td>
</tr>
<tr>
<td></td>
<td>▪ The manageability requirements such as remote monitoring, administration, configuration, fault identification etc. shall have to be tested out.</td>
</tr>
<tr>
<td><strong>Service Levels Monitoring System</strong></td>
<td>▪ The Acceptance Testing and Certification agency shall verify the accuracy and completeness of the information captured by the Service Levels monitoring system implemented by the MSP and shall certify the same.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Criteria of acceptance</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>▪ The solution deployed for service levels measurement shall be configured to calculate the penalties as defined in the SLA. The MSP shall provide complete access to the Service Levels Reporting System/BI tool including the manner in which the configuration of the system has been done.</td>
</tr>
<tr>
<td></td>
<td>▪ The MSP shall provide full access to generate reports from the systems to AAI/DGCA officials or its nominees.</td>
</tr>
<tr>
<td>Project Documentation</td>
<td>▪ The Agency shall review the project documents developed by MSP including requirements, design, source code, installation, training and administration manuals, version control etc.</td>
</tr>
<tr>
<td></td>
<td>▪ Any issues/gaps identified by the Agency, in any of the above areas, shall be addressed by the MSP to the complete satisfaction of AAI/DGCA.</td>
</tr>
<tr>
<td>Data Quality</td>
<td>▪ The Agency shall perform the Data Quality Assessment for the entire data</td>
</tr>
<tr>
<td></td>
<td>▪ The errors/gaps identified during the Data Quality Assessment shall be addressed by MSP before moving the data into production environment, which is a key milestone for Go-live of the solution.</td>
</tr>
</tbody>
</table>

2. In case there is any shortcoming (which does not impact any of the Service levels) in the deliverables as above, AAI/DGCA may, at its discretion, permit Conditional Go-Live. However, MSP is responsible for completion of all related pending activities within stipulated time as defined in conditional GO-LIVE approval. It is to be noted that the next phase timelines shall be initiated at time of Conditional Go-Live approval.

**Deliverable(s):**
1. Defect Reports
2. Post Go-Live:
   i) Updated system design documents, specifications,
   ii) Latest source code, application deployment files, configuration files for entire solution
   iii) Updated user manuals, administration manuals, training manuals etc.
   iv) Software change logs etc.

**3.4.4 Solution Documentation**
1. The MSP shall document all the installation and commissioning procedures and provide the same to the AAI within one week of the completion of the go-live.
2. The MSP shall be responsible for preparing process documentation relating to operation and maintenance of the solution. The process documents shall be formally signed off by AAI.
3. All documentation will be supplied both in Hardcopy and Softcopy format.
4. Each process document shall clearly define the roles and responsibilities, detailed steps for execution the defined task, detailed configuration steps etc.
5. AAI expects the MSP to document the operations and management processes as per standards defined in “Compliance to Standards and Certifications”.

### 3.5 Cloud Provisioning & Commissioning

The MSP shall be responsible for deploying the entire Digital Sky Solution on a Virtual Private Cloud /Government Community Cloud Services of MEITY Empaneled Cloud Service Provider. The MSP shall select a Cloud Service Provider (CSP) meeting the eligibility requirements as specified in the RFP document.

All the requirements/scope of work mentioned in this section shall be the responsibility of the MSP. MSP shall also ensure that as a Lead Bidder, the CSP chosen provides the following features in the cloud and also performs the scope of work which is directly attributable to CSP.

Alternatively,

**MSP may choose and decide to host the services on NIC Cloud for which AAI shall support MSP in obtaining necessary administrative approvals for hosting services at NIC. Since, hosting services of NIC is on paid basis, it is informed that all costs associated with hosting the services at NIC shall be on account of MSP. In this regards, AAI shall deduct all charges from the payments to MSP on actuals including recovery of payments from MSP if the total amount exceeds the value of the contract. Further, it is informed that in case the actual hosting cost at NIC is below the quoted price by MSP, payments shall be made on actuals and not on quoted price for NIC hosted cloud services. Further, it is informed that the ultimate responsibility for such hosting at NIC shall be with MSP (including SLAs).**

1. The MSP shall deploy the developed Digital Sky Solution on a “Meity Empaneled Virtual Private Cloud/Government Community Cloud Services” of the CSP.

2. The MSP is required to prepare and submit along with their technical proposal, the details of methodologies & computations for sizing & capacity of storage, compute, backup, network and security.

3. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the Contract) during any unanticipated spikes in the user load.

4. The MSP will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.

5. While, the initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) may be carried out for the first year; subsequently, it is expected that the MSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up the compute, memory, storage, and bandwidth requirements to support the scalability and performance.

---

*In case MSP decides to host services at NIC, MSP may interchange-ably refer CSP as NIC, wherever applicable*
requirements of the solution and meet the SLAs. Any such scaling up would be the responsibility of MSP during the contract period, with no additional cost to AAI.

6. MSPs shall provide interoperability support with regards to available APIs, data portability etc. for the Purchaser to utilize in case of:
   a) Change of Cloud Service Provider,
   b) Migration back to in-house infrastructure,
   c) Burst to a different cloud service provider for a short duration
   d) Availing backup or DR services from a different service provider

7. The MSP shall provide required Support to AAI in migration of the VMs, data, content and any other assets to the new environment created by the Government Department or any Agency (on behalf of the Government) on alternate cloud service provider’s offerings to enable successful deployment and running of Digital Sky solution on the new infrastructure.

8. The Purchaser retains ownership of all virtual machine, templates, clones, and scripts/applications including application code (all versions) created for the Digital Sky system, and all perpetual licenses purchased during the contractual period. The Purchaser retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

9. The detailed Cloud Services Requirements for Digital Sky System are given in Scope of Work – Appendix 5 and 6

10. It is to be noted for Aadhar related information, separate hosting infrastructure shall be provided to MSP by AAI. MSP is required to use such hosting infrastructure for storage of Aadhar related information. No information related to Aadhar shall be hosted at CSP, unless indicated by AAI.

### 3.5.1 Change in CSP

At any point of time during the duration of the project, it might be decided to migrate to an on premise private cloud environment or to any other cloud service provider (Hereafter refer to as the new environment) depending upon the situations that might be observed. Accordingly, it would be the responsibility of the MSP to make sure all the provisioned resources in the Cloud Service provider (including the data) is migrated back to the new environment. The decision to move back to the new environment would rest upon AAI. The following point should be noted in this aspect:

1. The MSP would need to check and re-size the application and infrastructure to the new environment including all the licenses
2. Data migration would be the responsibility of the MSP. MSP should ensure that all requisite interfaces to existing systems are available.
3. Operating process for working in the new environment would have to be defined by the MSP.
4. The MSP should make sure that adequate support is available from CSP for the purpose of migration to new environment. For the same reason, the MSP should choose a model of deployment on Cloud Service Provider taking the consideration that the model should be easily portable to the new environment.

The MSP should design the migration strategy keeping in mind that there should not be any downtime during the transition.
3.6 Digital Sky Business Support and Grievance Cell

This track includes setting up a call center helpdesk for the project period after Go-Live. The key areas of assistance to be provided by the Support Cell

1. The Digital Sky support Cell will handle technical queries and provide guidance for queries related to using the Digital Sky portal (for both Internal & External stakeholders).

2. Provide business support

3.6.1 Digital Sky Business Support

3.6.1.1 First Level Evaluation of Submission

The MSP is to provide support for all business related matters:

1. The Digital Sky Support Cell will cater to validation of all supporting documents submitted by applicants including scanned documents. For the purpose of validation of all scanned/supporting documents submitted, all objective parameters will be required to be validated by the Digital Sky support cell. For example
   a. Marksheets – Name, Marks etc
   b. Supporting documents titles, etc.
   c. Data Entry correction on parameters from attached supported documents, etc

2. Business related queries forwarded to relevant authorities in AAI/DGCA for resolution

3. Providing status of application / queries

4. Information Sharing with Relevant Stakeholders based on demand.

5. MSP may sub-contract the mentioned scope of work in the section

3.6.2 Call Centre/GRM

1. Development of call centre (with inbound and outbound call facility) to provide guidance and services related to Digital Sky. For the same, a country wide toll free number is to be purchased by the MSP.

2. It is to be noted that the MSP is to estimate the cost associated with SMS/calls generated by the call center in its commercial bid. No extra payments shall be made for the same on account of such expenses incurred by MSP. Further, it is highlighted that for purpose of status intimation, mobile app based alerts can also be sent instead of SMS for non-registration based services. However, in all services requiring authentication, SMS has to be used

3. The call centre shall be operational 8 hours on all working days and is to provide all business and technical support for stakeholders. The minimum services envisaged through the call centre includes:
   i. Guiding stakeholders during the registration/approval process
   ii. Guiding stakeholders on usage of Digital Sky
   iii. Assisting stakeholders on IT related issues
   iv. Providing status of application
   v. Escalating business related grievances to right authorities within AAI/DGCA/MoCA

4. A menu structure shall be created for callers in order to allow knowledgeable users to access information more quickly. The information about status/ grievance shall be provided to the callers
after their identification based on the required query. The system must have an authentication mechanism through Application number/ reference number/Digital Sky ID. Further, a 4 digit password for authentication is required to be created.

5. A dual-tone multi-frequency (DTMF) signalling menu service must be available for users to retrieve information from the service. The service shall be accessible in English.

6. The MSP shall provide for the requisite team size in its technical proposal for the call centre.

7. MSP shall enable a grievance management system in such a manner that allows user to interact with system through different modes such as virtual assistant, chat agents, contact center, paper, email and Digital Sky portal itself.

8. The MSP shall integrate its systems in such a way that if a grievance or a query is posted at any of the communication channels (portal, mobile app, call centre, paper mode etc.) the same are registered at one database and resolved in the similar fashion so that a unified or an integrated view of the communications is viewed by the stakeholder).

9. The MSP shall, in consultation with the AAI/DGCA, design and implement an escalation matrix for providing resolution of issues so reported by the stakeholders through any of the communication channels.

10. All interactions with users will be assigned a ticket number and the number will be made available to the user along with the identification of the agent (need not be the real name) without the user having to make a request in this regard, at the beginning of the interaction.

11. The ticket number shall be linked to the service request of the caller for monitoring purposes. All interactions will be noted on the system.

12. All the issues on logging shall be assigned a severity level based on definition below. Basic guidelines for assigning severity are as follows:
13. The MSP shall provision for outbound calls for some standardized messages to be made through IVRS to reduce the pendency of outbound calls and such IVRS calls may also be made on non-working days except national holidays.

14. All calls received or made by the Call Centre would recorded and a quality audit would be carried out by the AAI or its representative.

15. Electronic acknowledgements should be sent to the user along with a service ticket number immediately on call logging. The system shall keep the user informed on various stages of resolution through email/SMS.

16. Continuous Improvement:
   
   i. Prepare Knowledge base for frequently reported problems along with the resolution steps/solutions and publish it on the portal.
   
   ii. Publish and continuously update the knowledge base on the website that can enable a user to find a solution to a problem at hand without calling Digital Sky Support.
   
   iii. On a quarterly basis, the MSP shall carry out the analysis of the tickets (open and closed) to identify the recurring incidents and conduct a root cause analysis on them. The MSP shall submit a report to the AAI with the analysis performed and provide inputs to the AAI on user training requirements, awareness messages to be posted on the portal, redesign recommendations and/or application enhancements (functional/design) based on ticket analysis. The objective of the analysis should be to address the cause for repeated incidents and enhance the quality of delivery of services to the end users.
17. The MSP shall prepare and submit reports to the AAI team per the mutually agreed reporting structure. These reports shall include but not limited to the following:
   i. Calls per week, month or other period.
   ii. Numeric and graphical representation of call volume
   iii. Calls for each interaction tracked by type (calls for information on specific service, calls for specific enquiries)
   iv. Number of dropped calls after answering, including:
      v. Calls that ended while on hold, indicating that the caller hung up;
      vi. Call that ended due to entry errors using the automated system indicating difficulty in using the system
   vii. No. of rings before a Call was picked up (max., min, avg. for a day)
   viii. Incident logs (category, severity and status of call etc.)
   ix. Incidents escalated
   x. SLA compliance/non-compliance reports with reasons for non-compliance
   xi. Problem management
   xii. Detailed analysis of calls containing opportunities for automation, trainings, FAQs, etc.

18. To ensure Customer Service Quality, the AAI shall conduct regular audits, random audits and call barging
   i. The AAI will complete a random sample survey of calls for call quality check as well as participate in calls without prior notification. For this purpose, administration level permissions to access all sub-systems/servers to monitor and generate reports including those required for cross-verification of SLAs and related payments will be provided by the MSP.
   ii. All calls should be recorded. The call data from the voice logger should be archived on to the hard disk every 15 days. The data on the hard disk should be stored using naming conventions that support easy retrieval. These records shall be retained on the hard disk for another 30 days.
   iii. If it is observed by the AAI that a CSE has misbehaved with a caller on telephone, or if complaint is received against any of the CSE and if his/her performance is found to be lacking in the AAI's opinion, they may instruct the MSP to remove the concerned individual from the AAI Support Cell immediately and arrange for a suitable replacement within 1 week.

19. Incidents which do not meet SLAs and are exceptional in nature (highly critical, wider spread etc.) shall be escalated as defined in the escalation matrix.

20. The Support Cell should comply with SLAs applicable to them as mentioned in this RFP. Non-adherence to SLAs shall lead to imposition of liquidated damages.

3.6.3 Set up IT Infrastructure

The MSP shall Procure, Install and Commission an Interactive Voice Response System (IVRS), Dialler, and any other related hardware and network components to initiate the Helpdesk operations.

1. Toll Free Number
   a. The MSP shall procure All India Toll Free Number

2. IVR
a. The MSP shall configure and implement the IVR product and dialler along with any required third party solutions to meet the complete functional requirements as mentioned in this RFP.

b. The MSP shall design the IVR tree structure in consultation with the AAI and seek their approval. AAI may suggest changes with regard to customization in the IVR tree structure from time to time, which the MSP shall execute within 1 working day at no additional cost.

c. There shall also be a provision for a caller to surpass the IVRS and directly speak to a Customer Service Executive (CSE) regarding issues faced.

3. Helpdesk application:
   a. The software would maintain a complete history of all calls received at the helpdesk.
   b. A unique id/ticket number shall be generated for all service requests/complaints and tracked until closure.
   c. The Customer Service Executive (CSE) would be capturing all relevant caller information in the Helpdesk application for recording customer communication and should be integrated with required the Digital Sky applications etc.
   d. The MSP shall provide the Digital Sky with all the data of the Helpdesk application at the time of contract completion.

4. Automatic Call Distributor (ACD):
   ACD distributes all incoming calls to individual agents as they are received. It should be pre-integrated with the IVR and include the following features:
   a. Routing callers to CSEs based on their availability to take calls on a first come first serve basis.
   b. Standard features like Call Transfer, Conference, Barge in, Dialed Number Identification Sequence (DNIS), Automatic Number Identification (ANI) and Caller Line Identification (CLI) etc.
   c. Announcement of the queue waiting time for each caller before being attended to by an agent.
   d. The ability to play customized announcements per queue as defined by the administration.

5. Other Infrastructure components that need to be provided by the MSP are:
   a. Call barging and recording software
   b. Customer Service Executives’ computers, phone sets and head sets.

Refer Scope of Work - Appendix 7 - Digital Sky Help Desk Solution for details related to Help Desk

6. The entire call center set up is to be off site or at MSP premises
3.7 Development of IT Systems for AUA /KUA/eSign

1. AAI/MoCA is to become an AUA/KUA and will obtain the AUA/KUA license

2. MSP is required to develop the IT infrastructure for AAI/MoCA to operate as AUA/KUA; this includes AUA/KUA Software including necessary APIs, servers, database, Vault etc. and any associated hardware/software required to operate as AUA/KUA for AAI/MoCA. The software component may include front end application and backend application, APIs etc. to conduct authentication, e-KYC, offline verification etc.

3. The application should support all modalities as per the Aadhaar Act 2016 such as demographic authentication, OTP, biometric (fingerprint/IRIS), fac authentication, offline verification etc. and any other modality that may be provided by UIDAI either single factor or multiple factors such as combination of biometric and face authentication.

4. The application should support the latest specification from UIDAI from time to time such as use of virtual ID, UID token etc. The MSP is expected to know the latest requirements from UIDAI available on UIDAI website or public domain and implement the same and upgrade from time to time.

5. MSP shall integrate the Authentication application and e-KYC application with the ASA appointed by AAI/MoCA to ensure that authentication and e-KYC is being conducted successfully.

6. The AUA/KUA application hosting can be outside MEITY empaneled CSP and in that case hosting environment can be at NIC Cloud, AAI DC/DR, etc. All configuration costs associated with hosting the application and maintaining the application at selected DC/DR shall be borne by MSP. The hosting charges for the same though shall be borne by AAI for the application in case of hosting outside the MEITY empaneled CSP.

7. It will be the responsibility of the Vendor to run the AUA/KUA services

8. MSP is responsible to ensure compliance to all Aadhaar Act 2016 requirements including but not limited to below:

   - Aadhaar (Authentication) Regulations, 2016
   - Aadhaar (Data Security) Regulations, 2016
   - Aadhaar (Sharing of Information) Regulations, 2016
   - AUA / KUA agreement version 4.0 dated June 2017
   - Latest APIs ( Aadhaar Authentication API specification version 2.5, Aadhaar eKYC API specification version 2.5 and Aadhaar OTP request API specification version 2.5)
   - Aadhaar Registered devices Technical specifications – version 2.0 and Circular for Registered devices dated 25.01.2017
   - Implementation of HSM AUA/KUA/ASA dated 22.06.2017
   - Circular for Reference key dated 25.07.2017 and Frequently asked questions for Aadhaar vault and Reference keys dated December 2017
   - Dos and Donts for Aadhaar User agencies/Departments dated October 2017
   - Submission of Audit report by a certified auditor and go live checklist before onboarding of requesting entities etc.
9. HSM for encryption / decryption needs to be deployed by MSP for secure management of the keys involved in Aadhaar authentication and other aspects. In case HSM is deployed in the cloud, the PED keys for HSM management shall be in control of MSP under a dual authentication biometric locker. Biometric locker may be physically placed within the Cloud data center, however access to biometric locker shall only be available with MSP or AAI/MoCA.

10. The MSP should develop the AUA that complies with UIDAI Guidelines, Circulars and Regulations (Refer [Link](#)).

**The following define the e-sign related scope of work for vendor:**

1. AAI/MoCA shall form a contract with e-sign service provider to e-sign service.

2. MSP shall develop ASP application, esign front end and backend application to avail e-sign services. Integration with ESP application and infrastructure shall be done by MSP and maintenance of the same shall also be done by MSP. All modalities of e-sign such as biometric authentication based or OTP based or multi factor (face auth combined etc.) shall be supported by MSP application. Management of e-sign application and infrastructure shall be done by MSP.

### 3.8 Operating & Managing Digital Sky

The MSP will operate and maintain all the components of the Digital Sky System for a period of five (5) years from the date of Go-Live. The O&M is divided into the following parts:

**3.8.1 Application Support and Maintenance**

Application support includes, but not limited to, production monitoring, troubleshooting and addressing functionality/availability and performance issues and also implementing system change requests etc. The MSP shall maintain the application software in good working conditions; and perform changes and upgrades to the applications as requested by the AAI. All tickets related to any issue/complaint/observation about the system shall be maintained in an ITIL compliant comprehensive ticketing solution. Key activities to be performed by the MSP during the application support phase are as follows:

1. **Compliance to SLA**

   The MSP shall ensure compliance with SLAs as indicated in the RFP and any upgrades/major changes to the software shall be planned by the MSP while ensuring that the SLA requirements are met at no additional cost to the AAI.

2. **Annual Technology Support**

   The MSP shall be responsible for arranging annual technology support to the Digital Sky for the OEM products (if applicable) provided by respective OEMs during the entire O&M phase. It is mandatory for the MSP to take enterprise level annual support over the entire contract duration from the date of delivery and installation of licenses at minimum for the software(s) mentioned below:

   a. Operating System
   b. Virtualization layers
   c. RDBMS
   d. Middle ware
e. Data warehouse

f. Analytics tool

g. All third party products/ engines deployed in the Digital Sky Solution

Note:
For anything not included as part of cloud services, it is mandatory for the MSP to take enterprise level annual support over the entire contract duration.

For CSP services, the CSP has to ensure that the components of cloud services are updated/ upgraded for the latest version to support the application.

The MSP & CSP shall provide proof of the update/ upgrade on annual basis.

3. Application Software Maintenance

a) The MSP shall provide continuous and indefinite support through on-site team/telephone/E-mail/ installation visits as required.

b) The MSP shall address all the errors/bugs/gaps in the functionalities of the solution (vis-à-vis the FRS, BRD and SRS signed off) at no additional cost during the O&M phase.

c) All patches and upgrades from OEMs shall be implemented by the MSP. All patches shall have to be updated on a fixed interval, say quarterly basis. Security patches can be updated on immediate basis. Each release comes with a risk of system stabilization and hence periodic updates with full testing needs to be done to mitigate the risk. Technical upgrades of installation to the new version, as and when required, shall be done by the MSP. Any version upgrades of the software/tool/application will be done by the MSP after seeking prior approval from the AAI and submitting the impact assessment of an upgrade as such.

d) Any changes/upgrades to the software performed during the support phase shall be subject to comprehensive and integrated testing by the MSP in order to ensure that the changes implemented in the system meet the specified requirements and do not impact any other existing functions of the system. A detailed process in this regard will be finalized by the MSP in consultation with the AAI.

e) An Issue log shall be maintained by the MSP for the errors and bugs identified in the solution as well as any changes implemented in the solution and shall be periodically submitted to the AAI team.

f) The MSP will inform the AAI (at least on a monthly basis) about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the MSP shall inform the AAI immediately along with any relevant recommendations. The report shall also contain the MSP’s recommendations on update/upgrade, benefits, impact analysis etc.

g) The MSP needs to execute updates/upgrades though a formal change management process and subsequently update all documentations and Knowledge databases etc.

h) The MSP will carry out all required updates/upgrades by following defined processes at no additional cost.

4. Problem identification and Resolution:
a. Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve in turn lead to application hindrances. The MSP shall resolve all the application problems through implementation of the identified solution (e.g. system malfunctions, performance problems and data corruption etc.)

b. Monthly reports on problems identified and resolved would be submitted to the Digital Sky team along with recommended solutions.

5. Change and Version Control

All planned or emergency changes to any component of the system shall be carried out through the approved Change Management process. The MSP needs to follow all such processes (based on industry ITSM framework) at all times. For any change, MSP shall ensure:

a. Detailed impact analysis is conducted

b. All Change plans are backed by Roll back plans

c. Appropriate communication on change required has taken place

d. Requisite approvals have been received

e. Schedules have been adjusted to minimize impact on the Production environment

f. All associated documentation is updated post stabilization of the implemented change

g. Version control is maintained for all software changes

The MSP shall define the Software Change Management and Version Control Process. For any changes to the solution, the MSP has to prepare detailed documentation including proposed changes and impact to the system in terms of functional outcomes/additional features added to the system etc. The MSP shall ensure that software and hardware version control is carried out for the entire contract duration.

6. Maintain configuration information

The MSP shall maintain version control and configuration information for application software and any relevant system documentation.

7. Training

The MSP shall conduct trainings for the AAI personnel whenever there is any change in the system functionality. All Training plans have to be mutually agreed on with the AAI team.

8. Maintain System documentation

The MSP shall maintain at least the following minimum documentation with respect to the Digital Sky system:

a. High level design of whole system

b. Low level design for whole system/module design level

c. System Requirements Specifications (SRS)
d. Any other explanatory notes about system

e. Traceability matrix

f. Compilation environment

9. The MSP shall also ensure that any software system documentation is updated with regard to the following:

a. Source code is documented

b. Functional specifications are documented

c. Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS in accordance with the defined standards

d. User manuals and training manuals are updated to reflect on-going changes/enhancements

e. Standard practices of version control and management are adopted and followed

10. All project documents need to follow a proper version control mechanism. The MSP will be required to keep all project documentation updated and ensure the updated project documents are submitted to the AAI by the end of next quarter in case of any change.

11. For application support, the MSP shall assign a dedicated software support team to be based at the MSP’s location as a single point of contact for resolution of all application related issues. This team will receive and resolve all the application related tickets/incidents. In the technical proposal, the MSP needs to provide the proposed application support team structure including the number of team members proposed to be deployed along with roles and skills of each. The Application support team shall comprise of the MSP’s employees.

12. Any software changes required due to problems/bugs in the developed software/application will not be considered as part of change control and will have to be completed by the MSP at no additional cost (even if it requires any enhancements/customizations).

13. Software License Management: The MSP shall provide for software license management and control. MSP shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance.

Note: OEM should perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. MSP is responsible for any exceptions or breach of the terms and conditions.

3.8.2 Master Data Maintenance

MSP shall be responsible for maintaining all the master data for the platform

3.8.3 Web based SLA Monitoring Tool

1. The MSP will customize a commercially available web-based SLA Monitoring Tool.
2. The MSP shall implement the SLA Monitoring System to measure performance against each of the indicators listed under SLAs specified in the RFP. The SLA Monitoring System implemented by MSP shall be reviewed by AAI before usage.

3. The MSP shall ensure that proposed SLA monitoring system addresses all the SLA measurement requirements and enables calculation of eligible compensation to the MSP on a quarterly basis, including the penalties as specified in the SLA.

4. Bidder shall provide software tools and solutions monitoring of solution deployment and alert mechanism tools for the deployed applications (for ex. Zabbix, Nagios).

1. The SLA monitoring tool should be able to monitor all the service levels defined in the service level agreement.

2. The proposed tool should provide comprehensive and end-to-end management of all the components for each service including network, systems, application and Infrastructure.

3. The proposed SLA monitoring tool should automatically document problems and interruptions for Digital Sky Solution services and provide the consolidated violations as per the SLA.

4. MSP should deploy Mobile App crash reporting tool for iOS and Android.

5. The proposed tool should allow changing the parameters of the measurement and should allow adding new SLAs on need basis.

6. SLA monitoring tool should enable AAI to have a unified view of the entire Digital Sky Solution SLA.

7. The proposed tool should provide the following performance reports, in addition to SLA report.
   i) Executive Summary report
   ii) Capacity Planning report which provides a view of under-and-over-utilized elements.
   iii) Availability report
   iv) The tool should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.

8. The proposed tool should be able to monitor various operating system parameters.

9. The proposed tool should provide self-monitoring wherein it will track critical status such as (but not limited to):
   i) CPU utilization
   ii) Memory capacity
   iii) File system space and other important data

   A consolidated performance report shall also be generated to monitor the above parameters.

10. The indicative services as part of this support are as below:
   i) System Administration, Maintenance & Management Services
   ii) Application Monitoring Services
   iii) Storage Administration and Management Services
   iv) Replication, Backup and Restore Services

**Deliverable(s):**

1. SLA Reports on weekly/monthly basis

**3.8.4 System Administration, Maintenance & Management Services**

The objective of this service is to support and maintain all the Systems provided as a part of this project by MSP, and shall include:

1. Regular monitoring of all the applications hosted.
2. Operating System administration, including but not limited to management of users, processes, preventive maintenance and management of servers including updates, upgrades and patches to ensure that the system is properly updated.

3. Installation and Re-installation of the server and other hardware in the event of system crash/failures.

4. Regular analysis of events and logs generated in all the sub-systems including but not limited to servers, operating systems, security devices, etc. to identify vulnerabilities. Necessary Action shall be taken by the MSP in accordance with the results of the log analysis. Suitable mechanism has to be maintained for security and forensic related logs or as per requirement of IT Act and that of other government regulations issued from time to time.

5. Adoption of policies and procedure, compliances, guideline or international standard as defined by the AAI.

6. Troubleshoot problems with web services, mail services, applications software, desktop/server relationship issues and overall aspects of a server environment.

7. Problems shall be logged in at the Help Desk and resolved as per the SLAs defined.


9. Prepare and keep up to date document containing configurations of all server, IT infrastructure etc.


11. Carry out the DC and DRC failure testing and Quarterly BCP real drills.

12. Configuration of server parameters, operating systems administration and tuning

13. Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of upgrades including migration to higher versions and patches to ensure that the system is properly updated.

14. Periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures

15. Perform Database Administration activities for Database. The MSP agrees that all databases of the AAI will be administered as per standards and requirements. The service covers all the databases running on servers / SAN at DC including but not limited to:-
   i) Start-up and shutdown of databases.
   ii) Daily / Weekly / Monthly backup of databases.
   iii) Database recovery when required.
   iv) Weekly database recovery checks.
   v) Required logs maintenance as per policies of the AAI.
   vi) Disaster recovery as per polices of the AAI.
   vii) Documentation upkeep and records maintenance.
   viii) User account management.
   ix) Database problem resolution.
   x) Performance tuning.

3.8.5 Application Monitoring Services

The services to be provided by the MSP for Application Monitoring which includes following but not limited to:

1. Web services
2. Application server
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

3. Database server
4. Middleware
5. Other components as proposed by MSP

3.8.6 Storage Administration & Management Services

The services to be provided by the MSP shall include:

1. Installation and configuration of the storage system.
2. Management of storage environment to maintain performance at desired optimum levels.
3. Management of any changes to database schema, disk space, storage, user roles
4. Identify key resources in the Storage solution.
5. Identify interconnects between key resources in the Storage solution.
6. Identify the health of key resources in the Storage solution.
7. Identify the available performance of interconnects in the Storage solution.
8. Identify the zones being enforced in the Storage solution.
9. Create/delete and enable/disable zones in the Storage solution.
10. Identify the storage volumes in the Storage solution.
11. Create/delete/modify storage volumes in the Storage solution.
12. Identify the connectivity and access rights to Storage Volumes in the Storage solution.
13. Create/delete and enable/disable connectivity and access rights to Storage Volumes in the Storage solution.
14. To provide off-site storage of production data and Digital Sky Solution on appropriate media at regular intervals as required by AAI.

3.8.7 Backup and Restore Services

The services to be provided by MSP shall include:

1. Backup of storage as per the defined policies.
2. Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies as defined by AAI.
3. Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.
4. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
5. Media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).
6. 365x24x7 support for file and volume restoration requests at the DC

3.8.8 User Profiles & Account Management

1. Routine functional changes that include user and access management, creating new report formats, and configuration of reports.
2. MSP shall provide user support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application.
3. The MSP shall perform user ID and group management services. The user-id naming & protocol shall be designed and implemented for all the user ids. Such naming convention and protocol shall be signed-off with the AAI.
4. The MSP shall maintain access controls to protect and limit access to the authorized end users of AAI.
5. The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support related to Digital Sky Solution.

6. System administration tasks such as managing the access control system, creating and managing users etc.

3.8.9 Portal Management

1. The MSP is required to maintain/update the portal on regular basis for the period of the contract.

2. The MSP is required to ensure that the portal maintains and meets GIGW standards continuously and certification for the same is maintained throughout the duration of the contract.

3. It shall regularly design, upload and update the content of the portal.

4. Performance tuning of the system to ensure proper functioning of the portal.

5. Updating content (text, graphics, audio, video) on the website as per direction given by AAI.

6. MSP shall have the functionality of AI based virtual assistant, chat agents and click-to-call options.

3.8.10 Periodic Reporting

The Digital Sky shall provide user-friendly reporting for points of access like – AAI and/or Designated monitoring system shall provide a facility for generating and viewing online, real-time project, BI and MIS reports for services handled during a specified period, transaction density trends for any specified periodicity (hourly, daily, weekly, monthly) and any bottleneck situation creating dependency at any stage. The BI and MIS reporting system shall be an integrated system which office. The MSP shall provide complete access to the service levels Reporting System including the manner in which the configuration of the system has been done, SRS and system manuals. Full access to generate reports from the systems to AAI officials or its nominees.

Also, in addition to the reports that are identified in the RFP, it must be appreciated that so far as a particular data is available in the system it should be possible to get a report on that for the sake of helping AAI or its designated agencies in analysis and/or decision making. The system shall provide BI and MIS reporting with multiple “Slice and Dice” options to generate reports in flexible formats based on user specific needs. The MIS reporting requirements can be stated from the following perspectives:

From the Digital Sky system perspective, the reports should present historical, statistical and predictive views in addition to the daily/weekly/monthly views. In regards to the above, The MSP shall submit the following period reports (but not limited to) to AAI:

1. Updation of Documentation on successful completion of O&M operations for each quarter
2. Regular updation of all policies designed by MSP for AAI
3. Updated system design documents, specifications
4. Latest source code, application deployment files, configuration files for entire solution Software change logs etc.
5. Corrective Action report in response to the any audit findings/ other concerns as identified by AAI
6. Monthly report on the central helpdesk centre operations
7. SLA Monitoring Reports
8. Develop various MIS reports as required by AAI/MoCA/DGCA.
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

i) The application shall provide option to AAI/MoCA to generate MIS reports based on various category, stakeholders, regions, approval type, etc..

ii) Solution should be able to generate reports of different complexity – high, medium and simple for various stakeholder types or information types. For example

   i. Highly complex, 10 reports - requiring analysis and data fetch for 10 or more parameters

   ii. Medium complex, 15 reports - requiring analysis and data fetch for 5-10 parameters

   iii. Medium complex, 25 reports - requiring analysis and data fetch for 1-5 parameters

9. Solution shall provide a custom report builder for the Web portal UI.
10. There should be Reporting and Dashboards for Airspace Metrics, Business Metrics, and Engineering Metrics overall

11. MIS report should be auto generated (periodically or need basis) in real time.
12. A different MIS and Dashboard for the Complaints registered as per the roles defined for nodal officer, agents, DGCA/AAI/MoCA officials.
3.9 Training on Digital Sky

The MSP is required to conduct the training workshops for AAI/DGCA staff in a phased manner, in line with the overall implementation plan. The workshops should be conducted for various levels of officials/employees. The workshop content and material should be designed with specific focus on the requirements of each of these levels and work domain. MSP should conduct workshops for each group of employees (MSP will finalise the actual number of sessions in consultation with AAI in sync with the training plan and as part of the training module). MSP has to provide required material for the workshops including presentations, training material etc. It is required that MSP undertakes training and monitoring at a holistic level for AAI/DGCA employees (and other nominated stakeholders by AAI). Some of the key requirements include:

3.9.1 Training and Capacity Building

1. The purpose of this section is to define the minimum scope of work for training and capacity building to be implemented at various levels namely:
   a. DGCA/AAI officials (30 training sessions). The sessions will be spread across days Each session is assumed for period of 4 hours each.
   b. Trainings for stakeholders (30 sessions) of minimum 2 hours each on Digital Sky portal
2. The Service Provider's scope of work also includes preparing necessary documentation and aid required for successful delivery of such trainings.
3. The details provided in this section are indicative and the number of training sessions may increase.
4. The schedule for the training sessions shall be discussed with AAI. Based on the requirements, AAI shall inform MSP of the requirements of the training and same shall be conducted in accordance to the required timelines. It is to be noted that training sessions will be considered part of deliverables for the period defined by AAI and shall be

3.9.1.1 Types of training

<table>
<thead>
<tr>
<th>Type of training</th>
<th>Relevant Stakeholder</th>
<th>Scope</th>
</tr>
</thead>
</table>
| Functional       | AAI                  | • Application level details and functional aspects of the system  
                    |                      | • Training on Business Intelligence (BI) system and Dynamic reporting |
| Technical        | The Digital Sky Technical team  
                    | AAI | • Technical details  
                    | | • API details  
                    | | • Integration requirements  
                    | | • System operations |
3.9.1.2 Preparation of training aids

1. The Service Provider will prepare all the requisite audio/visual training aids required for successful completion of training for all stakeholders/persona. These include the following:
   a. Training manuals for Stakeholders/AAI/DGCA officials
   b. Presentations
   c. User manuals
   d. Operational and maintenance manuals for the modules
   e. Application/modules training prototype for hands on training using dummy data
   f. Regular updates to the training aids prepared under this project
   g. FAQs

2. The Service Provider will maintain a copy of all the training material on the Portal/website and access will be provided to relevant stakeholders depending on their need and role. The access to training on the portal would be finalized with AAI.

3. All training material shall be provided in electronic format to trainees

3.9.1.3 On-site support

1. The Service Provider has to provide on-site support at the AAI and DGCA HQ office to ensure a smooth functioning of the new system.

2. This team will be based for the contract duration and will be available during working hours. They will provide all application related support to the users. These resources should have experience in application support.

3.9.1.4 Training Effectiveness

1. The Service Provider has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently using the guidance provided as part of the training. Hence, it is necessary that the effectiveness of training sessions is measured. The Service Provider will prepare a comprehensive feedback form that will capture all necessary parameters on measuring the effectiveness of the training sessions. This form will be discussed and finalized with the AAI.

2. After each training session, feedback will be sought from each of the attendees on either printed feedback forms or through a link available on the web portal. One member of the stakeholder group would be involved in the feedback process and he/she has to oversee the feedback process. The feedback received would be reported to the AAI for each training session.

3. For each training session, the Service Provider will categorise the feedback on a scale of 1 to 10, where 10 will denote excellent and 1 will denote unsatisfactory.

4. The training session would be considered effective only after the cumulative score of the feedback as an outcome of the process [sum of all feedback divided by number of attendees] is more than 7.5.
3.10 Solution Audit and Third Party Code Review

1. The MSP is required to conduct a bi-annual Information Security Audit of the developed Digital Sky Solution from Year 1 onwards. For the same, MSP will get the system audited by 3rd party auditors at its own discretion. Further, MSP shall provision an option for online audit option for Auditors.

2. The MSP is required to prepare an Audit Plan for the period of the duration of the project and subsequently update on need basis. Due approval on the IS Audit Plan is required from AAI for commencement of the IS Audit activities.

3. The Information security audit of cloud services should include DC, DRC, gateway components of project locations and functional application audit in line with ISO-27001:2013 guidelines by a third party CERT-IN empanelled auditor and submit the report to AAI. The audits are to cover at least the following:
   i) Network mapping
   ii) Vulnerability assessment
   iii) Internal and external network penetration testing
   iv) Password cracking
   v) Log review, incident response and forensic auditing
   vi) Integrity checks
   vii) Malware/Virus detection
   viii) War dialling etc.

4. Functional audit should cover at least the following (but not be limited to):
   i) User Authentication:
      ▪ Review of User Account Management
      ▪ Privilege Management and Access Restrictions User ID Scrutiny and Evaluation
   ii) User Authorization:
      ▪ Segregation of Duties
      ▪ Evaluating Access Controls
      ▪ Critical Access Review
   iii) Auditing & Logging:
      ▪ Recording of security events for future investigations and access control
      ▪ Change Management Review
      ▪ Modifications done to the programs and the configurations
      ▪ Segregation between the development and production
      ▪ Testing process
      ▪ Quality assurance
   iv) Configuration Management
      ▪ Verification and evaluation of configurations relating to business processes

5. The IS Audit Report should include (but not limited to):
   i) Dates and Location(s) of audit
   ii) Audit components, including benchmarks for assessment
   iii) Summary of audit findings including identification tests, tools used and results of tests performed
   iv) Analysis of vulnerabilities and issues of concern
   v) Plan for inclusion / rectifications needs to be prepared by the MSP
   vi) Recommendations for action

6. The MSP should close all vulnerabilities, observations & recommendations of such an audit and the cost of closure of all such audit vulnerabilities, observations & recommendations to be borne by MSP.
7. Upon rectification based on the recommendations, the IS Auditor will be required to re-audit the system to ensure that all recommendations accepted for inclusion are complied with.

8. The final report is to be submitted immediately upon completion of the activity. Presentations on the report, its findings, conclusions and recommendations need to be made to AAI’s Management and to other audience, if required.

9. Scope of work also covers evaluating the confidentiality, safety & security of the data & servers, assess & strengthen the security posture of IT systems and networks for protection against external threats, by way of remote infrastructure security assessment, internal threats, by way of on-site infrastructure security assessment and integrated system threats, by way of application security assessment.

10. Confidentiality: All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner whatsoever to any third party.

**Third Party Code Review**

1. The MSP is required to get an annual Third Party Code Review done for the developed solution. The cost of conduct of third party code review needs to be borne by the MSP.

2. Planning for the Third Party Code Review needs to be done in consultation with AAI. The MSP needs to update all relevant documentation and make available the latest source code for the purpose of third party audit.

3. The 'Third Party' to conduct the Code Review should be the OEM for the development platform for the first time. Thereon, MSP in consultation with AAI shall decide on the agency to undertake such review.

4. The code review shall include but not be limited to:
   i) Defect count starting UT till UAT
   ii) Functional coverage
   iii) Coding Standards compliance
   iv) Performance parameters being considered at all the tiers of the solution
   v) Modularity being maintained
   vi) Batch job scheduling and kick off parameters
   vii) Performance and load test results review

5. The cost of rectification of any recommendations shall be borne by the MSP.

6. All suggestions and recommendations that are required to be incorporated as a result of the third party audit shall be the responsibility of the MSP.

It is to be noted that AAI can also get audits undertaken by third parties at its own discretion. MSP is required to support such audits undertaken by AAI nominated auditors. MSP is not required to make any payments for audit services undertaken by auditors nominated by AAI. However, regular audit requirements mentioned in the section above are within scope of MSP to arrange and undertake; such regular audits shall bear no financial implication on AAI beyond the quoted price by MSP in the bid.
3.11 Exit and transition management

The responsibilities of the MSP pertaining to exit management after the end of the contract for Digital Sky are as follows:

1. The MSP shall submit its structured and detailed Transition and Exit Management plan after 2 year of GO-LIVE of all services.

2. The MSP needs to update the Transition and Exit management plan one year before the contract expiration and submit the same to AAI for approval and sign-off which shall supersede the initial plan.

3. All risk during transition stage shall be properly documented by the MSP and mitigation measures shall be planned in advance so as to ensure a smooth transition without any service disruption.

4. Replacement of key resources during exit management shall be subject to AAI approval.

5. Service Level ownership, during exit, shall belong to the MSP.

6. Immediately prior to the initiation of the exit, the MSP shall provide for an updated plan for approval of the AAI.

7. At the end of the contract period or during the contract period, if any other agency is identified or selected for providing services related to the MSP’s scope of work, the MSP shall ensure that a proper and satisfactory handover is made to the other agency. This shall include transfer of all assets (Hardware, Software and all the documents) in working conditions with warranty after inspection and approval of AAI. If any upgrade, repair, replacement is required MSP will carry out the same at no extra cost to the AAI.

8. The MSP shall adhere and align itself with the transition and knowledge transfer plan of the new MSP (for Digital Sky 2.0)

9. The MSP shall ensure business continuity i.e. business as usual of Digital Sky during exit management. The MSP shall be in complete ownership of all scope related items.

10. The MSP must ensure that no end of support products (software/hardware) exist at time of transition for up to 18 months from the end of contract (including any extensions) and should ensure equivalent or better replacement/refresh.

11. MSP shall ensure that AMC/ATS shall be taken up to 6 months from the end of contract (including any extensions) for all items in scope of Digital Sky.

12. The transition and exit management period will start 6 months before the expiration of the contract. The MSP will provide shadow support for at least three months and secondary support for an additional three months before the end of the O&M period or termination of the contract, as applicable at no additional cost to AAI during the period of secondary support. In case of termination, the exit management period will start from effective date of termination or such other date as may be decided by the AAI but not later than 6 months from effective date of termination.

13. Closing off all critical open issues as on date of exit. All other open issues as on date of Exit shall be listed and provided to AAI.

14. The MSP shall provide necessary knowledge transfer and transition support to the incoming MSP. The deliverables are indicated below:

   a) Updated transition plan on periodic basis
   b) Complete documentation for the entire system handed over to the AAI/identified agency/new MSP.
   c) Handover of all AMC/ATS support related documents, credentials etc. for all OEM products supplied/maintained in the system. Handover MOUs signed for taking services taken from any of the sub-contracted agencies.
d) Handover of the list of complete inventory of all assets created for the project.

e) Assisting the new MSP/AAI with the complete audit of the system including licenses and physical assets.

f) Detailed walk-throughs and demos for the solution.

g) Hand-over of the entire software including source code, program files, configuration files, setup files, project documentation, user IDs, passwords, security policies, scripts etc.

h) Hand-over of the user IDs, passwords, security policies, scripts etc.

15. Knowledge transfer of the system to the incoming MSP to the satisfaction of the AAI per the specified timelines.

16. The MSP shall be released from the project once successful transition is completed by meeting the parameters defined for successful transition.

17. In case the MSP fails to observe any of the above points, the MSP shall not be released and all the pending payments shall be put on hold till the successful completion of the exit management to the satisfaction of the AAI.

18. Key artefacts (not limited to) required to be prepared for the purpose of exit include:

   i) Software Documentation
      - Design Documents
      - Software Requirement Specifications
      - Requirements Traceability Matrix
      - Source Code
      - Approved Versions
      - User Manual
      - Search Tool Manual
      - Test Plan & Cases
      - DC / DR Documentation

   ii) Hardware (DC / DR), if any
        - Asset Register
        - S/w and H/w End-of-Life Details (h/w: in case applicable, s/w: for COTS)
        - S/w and H/w End-of-Shelf Details (h/w: in case applicable, s/w: for COTS)
        - S/w Licenses details (in case of COTS)
        - Agreement details with Bandwidth Service Provider

   iii) Operations Documentation
         - Updated Runbook
         - Incidents list with RCA
         - Computer Based Training Manual
         - Helpdesk – Standard Operating Procedure
         - SLA compliance reports
         - Training Presentation
         - ToT - Training Manual
         - User Training Manual

   iv) Project Governance Documentation
       - Pending Action Items List
       - Activities, Dates, Responsibility
4. Roles & Responsibilities

4.1 Roles & Responsibilities of MSP

1. Procure, install, commission, operate and maintain:
   i) Requisite Digital Sky Solution as per the requirements mentioned in this RFP
   ii) Meet the defined SLAs for the performance of the system.
2. Develop and Undertake necessary trainings for AAI, DGCA staff and external stakeholders
3. Provide necessary support for the resolution of bugs, patches & upgrades of the software solution.
4. Provide necessary manpower for managing the Change Requests
5. Design various manuals like User manual, Trouble Shooting manual etc. for the system.
6. Deploy the required manpower to manage the operations and Digital Sky Support Cell.
7. Management and quality control of all services.
8. Any other services which is required for the successful execution of the project.
9. Generation of MIS reports as per the requirements of AAI.
10. Generation of the report for the monitoring of SLAs.
11. Adherence to all notifications and communication set forth by AAI in context of the scope of services.

4.2 Roles & Responsibilities of AAI

1. Coordination between all the stakeholders for providing necessary information for the study and development / customization of the necessary solution.
2. Coordinate with the MSP for conducting workshops for the Stakeholders.
3. Monitoring of overall timelines, SLAs and calculation of penalties accordingly.
4. Assist in conducting UAT for the application solution deployed.
5. Issuing the Acceptance Certificate on successful deployment of the software application, and for other components of the Scope of Work (wherever required).
6. Any other requirements that could arise during operations for effective governance and to meet any administrative requirement.
7. Ensuring the staff members and other stakeholders attend the training programs as per the schedule defined by the MSP and agreed upon by AAI.
8. Undertake agreements with stakeholders for integration with their systems
9. Provide sign off on the deliverables of the project.
5. Change Control Process

5.1 Purpose

1. This Section applies to and describes the procedure to be followed in the event of any proposed change to the Proposal submitted by MSP or in MSA after Go-Live/Stabilization Phase.
2. Such change shall include, but shall be limited to, changes in the scope of services and Key personnel’s and SLAs provided by the MSP.
3. AAI and the MSP recognize that change is an inevitable part of delivering services and that a significant element of this change can be accomplished by reorganizing processes and responsibilities without a material effect on the cost.
4. System Integrator to ensure that all changes are discussed and managed in a constructive manner in consultation with AAI.
5. MSP shall estimate the effort required for the change and the same shall be notified to AAI Project Manager/PMU for further validation and finalization.

5.2 Process, Procedure, Scope of Change Request

1. The change request procedure has the following objectives:
   i) To protect the environment from uncontrolled changes
   ii) To minimize the occurrence of unintended affects during the implementation of necessary changes
   iii) To avoid implementation of any changes which is not reviewed, approved or analysed
   iv) To control the impact of changes and minimize the effect on effective as well as efficient service delivery

2. Change Control Board (CCB): CCB will be responsible for ensuring that the change management guidelines is implemented and maintained. AAI will create a committee, which will act as a CCB, may also involve PMU as advisors, to oversee the administration of the Change Request Management procedures and guidelines.
3. The CCB will be authorized to review, approve and schedule all changes to the Digital Sky application. All decisions of the CCB will be final and binding on all parties involved.
4. For the purpose of change request, man month rates are being asked from prospective MSP in this RFP.
5. MSP would also provision for additional 300 Man-Month for carrying out work other than the scope of work mentioned in the RFP, its corrigendum (if published) and the SRS document and its revisions, as mentioned above. The effort estimation for the same would be decided by CCB and shall be binding on MSP & DGCA/AAI. The CCB may require the bidder to provide the model/methodology/ working used for arriving at the effort estimates for the change request.
6. Any changes within the services identified in the SRS document shall not be considered as change request, till 3 months post go-live of all the phases. Further, statutory/regulatory/ICAO mandated changes that are required for services that have been identified in the SRS will not be considered for Change Request for the entire contract period.
7. Any configuration, performance tuning, mitigation of security observation during annual/ periodical audits, changes required to accommodate patches, upgrades, bugs fixing, etc. which are required for the operation of the project shall not qualify as change request.
8. The functional requirements given in the RFP are indicative only and not exhaustive in any manner and/or kind and/or form and shall be finalized in consultation with AAI during Software Requirement Specification.

9. All the development / customization/ configuration must meet the requirements for security, performance and ease of use for operations, administration and management.

10. Any report whose data is residing in the Digital Sky solution or which can be arrived at by using some logic on the available data will not fall/ qualify as change request.

11. Change requests and CCNs will be reported monthly to AAI who will prioritize and review progress. MSP shall be required to implement any proposed changes once approved with effect from the date agreed for implementation.

12. The final sign-off and “Acceptance Certificate” would be provided by CCB after final implementation of the change and provide satisfactory completion certificate or the reasons for non-acceptance. Till that certificate is issued, all such changes will be deemed unaccepted and all the necessary SLAs and penalties will apply on the MSP.

13. The MSP shall take all necessary steps to implement the change as per the project plan submitted, without compromising on quality and performance standards. If the MSP fails to comply with the acceptable standards & requirements of implementing the requested change, or denies implementation of the requested change at any stage during the contract period, CCB will have complete authority to get the change implemented from any of the third party / nominated government agency independently. The integration of the change developed shall be the responsibility of MSP at no additional cost to AAI, provided the acceptance of deliverable(s) by CCB and Technical Committee of the change undertaken by the third party.

14. If CCB gives any new requirement or change request, the MSP should follow the change management procedure to implement the change on additional payment basis. The requirements for required infrastructure to implement the change should be specified by the MSP so that CCB can make necessary provisions. The change request procedure would be considered complete only when the training is imparted to the target users for whom the change is being done and the feedback is evaluated by both CCB and the AAI/PMU.

15. It is proposed that the prevailing rates for all kinds of change, as and when initiated by CCB will be taken into consideration and the proposals accordingly evaluated. In all such matters the decision of the CCB will be final and binding on all parties.

16. Any change requirement not pertaining to items and scope listed or elaborated in the current RFP can be undertaken by AAI through separate service provider(s); further, in case of additional volume of work (beyond the indicated volume in the RFP), AAI has an option to undertake such additional work through separate service provider(s).

The entire change request process will be implemented as mentioned below by MSP. The proposed timelines for each steps / activity and the corresponding responsibility centre is also shown in the table below:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Process</th>
<th>Responsibility Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Authorized official from MSP requesting a change will initiate a request by filling up the ‘Change Initiation Form’ after logging in with their own credentials.</td>
<td>MSP</td>
</tr>
<tr>
<td>S.No</td>
<td>Process</td>
<td>Responsibility Center</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
| 2.   | Once the Change request is submitted in the system, an email will automatically be triggered to:  
      a) the AAI/PMU  
      b) the MSP and  
      c) Copy to the CCB members | System |
| 3.   | PMU/AAI will evaluate the change request for risks, process of evaluating & implementing change, time required for completing the change(s) and any other additional requirement / information needed to clarify the Change requested; and will provide the recommendations in the change request module by logging with their credentials. | PMU/AAI |
| 4.   | The CCB/ PMU/AAI will discuss and provide adequate responses to the queries / suggestions from the MSP on the requested change. The committee will further decide on the responses to the queries / suggestions and log the final decision in the system. | CCB & PMU/AAI |
| 5.   | Based on the responses provided by CCB, MSP will prepare and submit a techno commercial proposal. | MSP |
| 6.   | a) The MSP can submit their Techno Commercial proposal either in hard copy or upload soft copy through the Change Request Module in the system. However MSP must submit the details of the proposal in the electronic ‘change evaluation and finalization’ form in the change management module.  
      b) After submission, an email will be auto triggered to AAI/PMU along with a copy to all the CCB committee members. In case hard copy is submitted by the MSP, CCB will officially handover the proposal to PMU/AAI for evaluation. | MSP |
| 7.   | a) PMU/AAI will evaluate the techno commercial proposal submitted by MSP and provide the recommendations to CCB.  
      b) CCB will review the evaluation and comments provided by the PMU and decide on the final status. This will be logged in the change request module by authorized representatives. | CCB & PMU/AAI |
| 8.   | c) If CCB does not approve the proposal in its entirety, then CCB will initiate negotiation with the MSP based on any of the aspects like cost, time, resources, impact on systems and/or operations and additional parameters, whichever applicable.  
      d) Based on the negotiation, the PMU/AAI will submit the final recommendation to CCB and log the decisions in the change request module.  
      e) If CCB approves the proposal in its entirety the Change request sign-off between CCB and MSP will be initiated. | CCB & PMU/AAI |
<table>
<thead>
<tr>
<th>S.No</th>
<th>Process</th>
<th>Responsibility Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>During Sign-off, the form will be printed, with all supporting annexure as logged in the system. The authorized signatory from AAI as well as the MSP will sign the Change Request Evaluation and Finalization form (at first place) and accordingly a formal Go-Ahead will be provided by AAI. This form will be signed in two copies; one for the MSP and other for CCB / AAI.</td>
<td>AAI/ MSP</td>
</tr>
<tr>
<td>10.</td>
<td>MSP will then initiate the change following a standard SDLC procedure like requirements gathering, design, development and testing, etc., as required, along with proper documentation at each stage.</td>
<td>MSP</td>
</tr>
<tr>
<td>11.</td>
<td>Once the change is completed as per agreed timelines and specifications, CCB representatives and the AAI/PMU will do the User Acceptance Testing and Auditing respectively to provide comments / recommendations to the committee members.</td>
<td>CCB &amp; PMU/AAI</td>
</tr>
<tr>
<td>12.</td>
<td>If any further activities need to be carried out as per the recommendations during UAT and Audit, it will be done by the MSP. After that an Acceptance Certificate will be issued to MSP by CCB and instructions for deployment / implementation, again as per standard deployment plan. This will follow a second sign-off on the ‘Change Request Evaluation &amp; Finalization’ Form.</td>
<td>CCB &amp; MSP</td>
</tr>
<tr>
<td>13.</td>
<td>MSP will deploy the changed solution and notify CCB and PMU/AAI.</td>
<td>MSP</td>
</tr>
<tr>
<td>14.</td>
<td>The PMU/AAI will finally review and confirm the deployed solution as per agreed standard, specifications and requirements, and provide status to CCB.</td>
<td>CCB</td>
</tr>
<tr>
<td>15.</td>
<td>A final sign off will be done on the ‘Change Request Evaluation &amp; Finalization’ Form and completion Certificate will be issued to the MSP by CCB along with a copy to the PMU/AAI. A copy of this completion certificate will have to be submitted to CCB along with the invoices for this change implementation.</td>
<td>CCB</td>
</tr>
</tbody>
</table>

**NOTE 1:**

1. **Change Control Note ("CCN")**
   a) Change requests in respect of the MSA, the Project Implementation, or the Operation and Management of SLA will emanate from the Parties’ respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process. CCNs will be presented to the Project Manager who will acknowledge receipt by signature of the CCN.

   b) The MSP and AAI, while preparing the CCN, shall consider the change in the context that it is beyond the scope of work as detailed in the RFP. Also, the value of additional work entrusted to MSP shall not exceed 30% of project cost during the Term.
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

c) It is hereby also clarified that the payment for the changes brought in after project certification and ‘Go Live’ date will be calculated on the basis of man-month rate quoted by the System Integrator in its bid and estimated man-month effort to be submitted by the MSP prior to taking up the change of control event and accepted by the AAI. AAI shall be given detailed breakup for the estimates.

2. Quotation

a) The System Integrator shall assess the CCN and shall provide as a minimum:
   i. Description of the change;
   ii. List of deliverables required for implementing the change;
   iii. Time table for implementation;
   iv. An estimate of the timelines and person-month efforts of any proposed change;
   v. The unit of measure to cost the change (either the resource cost as in the proposal, lines of code change etc).
   vi. Any relevant acceptance criteria;
   vii. An assessment of the value of the proposed change;
   viii. Material evidence to prove that the proposed change is not already covered within the scope of the Project, SLA, or MSA.

b) Alternative options possible to address the change if any and the implications of these alternative options.

c) Prior to submission of the completed CCN to the AAI, or its nominated agencies, the MSP will undertake its own internal review of the proposed CCN and obtain all necessary internal approvals. As a part of this internal review process, the MSP shall consider the materiality of the proposed change in the context of the MSA, the Project Implementation, SLA affected by the change and the total effect that may arise from implementation of the change.

d) Final effort estimate for change request will be established by AAI nominated committee (CCB).

3. Costs

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided the MSP meets the obligations as set in the CCN.

4. Obligations

The System Integrator shall be obliged to implement any proposed changes once approval in accordance with above provisions has been given, with effect from the date agreed for implementation and within an agreed timeframe. The penalty of 1% per week shall be applicable for delay in deliverable after agreed timeline. Such penalty shall not exceed 10% of the respective change control cost.
6. Project Governance

1. The project would require a close supervision and appropriate project control for successfully meeting the objectives and its timely completion. The following stakeholders / Committees / working groups are proposed for adequate program governance:
   i) Project and Contract Monitoring Committee
   ii) Project Management Unit (in case applicable)
   iii) Change Control Board (CCB) – CCB shall comprise of representative of MSP

   It is to be noted that above proposed governance could be changed at discretion of AAI

2. Project and Contract Monitoring Committee will be the approving authority for project related matters. However, the committee itself may refer the matter to Subject Matter Experts or Sub-Committee(s) for decision/comments/feedback.

3. Project Management Unit (PMU), if formed, would comprise of a team of consultants who would be responsible for monitoring all the project implementation, operations and maintenance activities, on behalf of AAI, and provide status reports, action taken reports, recommendation on deliverables, risks, etc.

4. CCB would be responsible for addressing all issues related to proposed change requests by the MSP. The committee would approve / reject (as case may be) all proposed change requests from the MSP, following an appropriate Change Control Process defined in the RFP.

5. MSP Project Manager: PM will serve as a single-point contact within the institutional framework for the purpose of project monitoring / reporting purposes and should be deployed by the selected MSP. The PM will be responsible for day to day coordination between PMU/AAI and all implementation teams. PM will be responsible for all the activities within the project scope and will report to Project Management Unit / Team. They will be directly responsible for providing Periodic Project Statuses, Tasks Schedule and Action Taken Reports (ATRs).

6. Delivery Team: They will be the actual delivery team deployed by the MSP and will work on all areas of the implementation phases. They may also constitute of various other teams as required for successful implementation

7. The MSP shall form a project team comprising the key experts indicated in RFP

8. Project Review Meetings: The following will be required to be undertaken by the MSP during the duration of the project:
   i) Weekly Status Review Meeting
   ii) Monthly Project Review Meeting
   iii) Defect Meetings (during major and minor release cycles)
   iv) Issue Management Meetings (on need basis)

MSP is required to prepare a detailed Action Taken Report for all meetings to ascertain and maintain a log of actions required and taken for successful project delivery

7. Manpower requirements

1. MSP shall assess the requirement of resources to design and implement the solution including number, skill sets and duration and provision the same for implementation of this project.

2. MSP has to necessarily maintain a team of requisite size of skilled professionals as per the requirements of the project.
3. MSP is required to maintain necessary business team (Business Analysts) team at site throughout the contract period to support AAI to support in any project related activity, coordination etc.

4. The resources proposed must not be changed unless replaced with equivalent or higher qualification and experience.

5. MSP shall deploy suitable technical resources for Digital Sky as per activities expected to be carried out, and all the resources should be trained in the use of the deployed tools, technologies and should have requisite functional knowledge.

6. MSP shall ensure that all the resources deployed for Digital Sky undergo suitable trainings in relation to security aspects of the project, and maintain the confidentiality of data.

7. MSP shall ensure requisite support from the OEM for various aspects of project including configuration, customization, sizing, performance tuning and implementation support.

8. MSP will maintain adequate leave reserve for personnel deployed.

9. The personnel deployed by the MSP (or by sub-contracting agencies/OEMs) should be their employees and they will have absolutely no claim to any category of appointment in any Government organisation. The terms of employment for the personnel deployed by the MSP shall be strictly as agreed between them and the MSP. Also, the MSP shall be completely responsible to personnel deployed by him for payment of salary, perks, incentives, any monetary and non-monetary compensation and all statutory contributions like Insurance, EMSP and PPF, meeting requirements of Central Minimum Wages Act, etc. Any touting activity taken up by any of the MSP personnel will be taken very strongly against MSP and necessary action will be taken by the AAI against the personnel and/or MSP

7.1 Sub-contracting

The following is the list of functionalities/ requirements for which the MSP may provision for sub-contracting services for the Digital Sky project. However sub-contracting for these requirements shall be optional in nature -

a) Digital Sky Support Cell for undertaking all non-technical (non-core) support activities listed under Digital Sky Business Support and Grievance Cell

b) Trainings

Note:

1. Any other sub-contracting can only be done after approval from AAI.

2. MSP is to ensure single level sub-contracting is only undertaken. Direct sub-contractors of MSP is not be allowed to further sub-contract work to other agencies.

3. MSP may hire services of individuals with domain expertise; however, such individuals are to be part of team implementing the project and not deliverables are to be completely sub contracted to them

4. MSP may seek support for products deployed for the application

5. **No Joint Venture is allowed for the project**

1. **Sub-contracting would be subject to the following conditions:**

   a) All sub-contracting contracts must be entered into by the MSP

   b) The list of all the sub-contractors of the MSP needs to be declared in the bid by the MSP.

   c) Sub-contracting will not dilute the responsibility and liability of the MSP.
TENDER DOCUMENT - SCOPE OF WORK – DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

d) The MSP will be responsible for meeting all obligations of its sub-contractors and the delivery of goods and services mentioned in all volumes of this RFP. The MSP will be solely responsible for all acts of its sub-contractors

e) AAI reserves its right to subject the sub-contractors to security clearances as it deems necessary and ALL the personnel of the sub-contractor before they are appointed to the Digital Sky project.

2. The MSP will be responsible for:

   a) The management of its sub-contractors who are a part of the proposal and for the delivery of all products and services in accordance with the agreement.

   b) The supply, delivery and installation, commissioning of all products and providing all services as submitted in their proposal.

   c) Internal arrangement between the MSP and its sub-contractors is left to the MSP, subject to compliance to relevant terms of this RFP. It shall be the responsibility of the MSP to ensure that its sub-contractors are compliant to all the clauses as mentioned in the bid, failing which bid can be disqualified.

8. Project Management

   MSP will use a project management tool to manage and operate all processes of the project using a proven SDLC methodology in consultation with AAI. The MSP is required to design and implement a comprehensive and effective project management methodology and deploy efficient and reliable PM tool/application with access provided to identified stakeholders. The PM tool/application should also allow for updates on email and SMS to all identified stakeholders. Further the tool/application should be accessible through a mobile app. The MSP shall address at the minimum the following using PM Tools:

   1. Define an organised set of activities for the project
   2. Establish and measure resource assignments and responsibilities
   3. Construct a project plan schedule with milestones
   4. Measure project deadlines, budget figures, and performance objectives
   5. Communicate the project plan to stakeholders with meaningful reports
   6. Provide facility for detecting problems and inconsistencies in the plan
   7. Provide Dashboards
   8. Maintain all documents/deliverables/approvals
   9. During the project implementation the MSP shall report to the AAI, on following items:

      a. Results accomplished during the period (fortnightly) ;
      b. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalised Project Plan;
      c. Corrective actions to be taken to return to planned schedule of progress;
      d. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the MSP;
      e. Other issues and outstanding problems, and actions proposed to be taken;

   10. Progress reports on a fortnightly basis and project quality assurance reports
   11. Audit trail and searchable history of all artefacts presented and approved shall be maintained on tool/application where admin password shall be in the custody of AAI.
   12. This tool/application shall be used, maintained and enhanced as per AAI requirement throughout the project lifecycle for all software, documentation, project, control or change requests
   13. The MSP should maintain a document repository and shall maintain version control of the documents using the document management solution with appropriate controls for document approvals
8.1 Risk and Issue management

1. The MSP shall develop a Risk Management Plan and identify, analyse and evaluate the project risks, developing cost effective strategies and action plans to mitigate those risks.

2. The MSP shall carry out a Risk Assessment exercise and document the Risk profile of the project based on the risk appetite, and prepare and share the enterprise risk register. The MSP shall develop an issues management procedure to identify, track, and resolve all issues faced on the project. The Risk management plan and issue management procedure shall be carried out in consultation with AAI.

3. The MSP shall monitor, report and update the project risk profile. The risks should be discussed with AAI and a mitigation plan should be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

8.2 Requirement Traceability Matrix

1. MSP shall be responsible for maintenance of a Requirement Traceability Matrix through-out the project.

2. MSP would ensure that Digital Sky is fully compliant with the requirements and specifications as mentioned in the RFP. For ensuring this, MSP shall prepare a Requirements Traceability Matrix on the basis of Functional Requirements Specifications (FRS) and Technical Requirements provided by AAI (updated by MSP as necessary) and the System Requirements Specifications (SRS) prepared by MSP.

3. This matrix would keep track of the requirements and trace their compliance through different stages of the project including software design, coding, unit testing, integration testing, user acceptance testing and final acceptance testing. The requirements traceability matrix would be a live document throughout the project, with the MSP team updating the matrix at every stage to reflect the compliance of each specification at every stage. All changes made on the document should allow PM application/tool to auto inform over SMS/Email to key stakeholders.

4. Through the duration of the project, AAI will periodically review the Traceability Matrix. AAI would provide the final approval once they are satisfied that all requirements are met.

9. Compliance to Industry Standards

The MSP will ensure that the Digital Sky setup is certified, wherever applicable, and is in compliance with the applicable standards throughout the duration of the contract.

Following table depicts the standards, which AAI intends to get certified within 6 months of GO LIVE. However, the list below is just for reference and is not to be treated as exhaustive.

<table>
<thead>
<tr>
<th>Solution Element</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information access/transfer protocols</td>
<td>W3C Specifications</td>
</tr>
<tr>
<td>Portal Development</td>
<td>W3C, GIGW</td>
</tr>
<tr>
<td>Interoperability</td>
<td>API, Web Services, Open Standards</td>
</tr>
<tr>
<td>Encryption</td>
<td>PKCS specifications</td>
</tr>
<tr>
<td>Information Security/Operational Integrity &amp; Security Management</td>
<td>ISO 27001-13 certification (or above)*</td>
</tr>
</tbody>
</table>
Solution Element | Standards
--- | ---
Operations | ISO 9001 certification (or above)*
IT Infrastructure management | EITM specifications
Service Management | ITIL
Project Documentation and software development | IEEE/ISO/CMMI (where applicable)
Business Continuity Management | ISO 27001
IT Governance | ITIL
IT Operations | ISO 20000/ITIL
Document the Operations and Management Standards | ISO 20000-1:2011 or relevant latest standard

a) The Standard/Certification will be the latest version as at the time of implementation. In case any standard/certification is withdrawn or replaced with a new standard/certification, the MSP has to ensure that the new standard/certification is taken within defined timelines or within 6 months of declaration of such change. Cost relating to compliance with the above standards/certification including documentation and certification fees etc. to be borne by the MSP.

Apart from the above the MSP need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

b) The Information Technology Act, 2000* and amendments thereof and Guidelines and advisories for information security published by Cert-In/DeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

The MSP shall also adhere to the relevant guidelines and standards (as applicable) issued by CERT-IN, MeITy and Government of India including the following –

1. Information Technology Act 2000 (revised 2008) (http://www.meity.gov.in/content/information-technology-act)
2. CERT-In security guidelines for Indian Government websites (http://www.cert-in.org.in/)
3. E-SAFE Guidelines for Information Security (http://egovstandards.gov.in/)
4. e-Governance Standards for Preservation Information Documentation of e-Records (http://egovstandards.gov.in/)
5. e-Governance standards on Biometric standards (http://egovstandards.gov.in/)
7. Guidelines for Indian Government Websites (http://egovstandards.gov.in/)
1. Qualification and Selection criteria for Bidder

1.1 Bid opening process

i. The bids will be opened in three sessions - one each for Pre-qualification, Technical and Commercial bids in the presence of bidders’ representatives duly authorized to attend the bid opening sessions on the specified date, time and address.

ii. The bids will be opened at each stage from the CPP portal, by the evaluation committee to be setup by the AAI.

iii. The representatives of the bidders are advised to carry the identity card or a letter of authority from the bidder firms to identify their bonafide for attending the opening of the proposal. The bidder’s representatives who are present may require to sign evidencing their attendance.

iv. In the event of the specified date of bid opening being declared a holiday for AAI, the Bids shall be opened at the same time and location on the next working day or as specified by AAI.

v. During each session of bid opening, preliminary scrutiny of the bid documents will be made to determine whether they are complete, whether required bid security has been furnished, whether the documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements will be prima facie rejected at the discretion of AAI.

vi. There will be three bid-opening events:
   - Envelope A (Pre-Qualification bid)
   - Envelope B (Technical bid)
   - Envelope C (Commercial bid)

vii. The venue, date and time for opening the Pre-qualification bid, Technical and commercial bid are mentioned in Tender Document.

viii. The Commercial Bids of only those bidders will be opened who score equal to or more than qualifying marks in Technical Bid.

1.2 Preliminary Examination of Bids

AAI will examine the Bids to determine whether they are complete, whether the documents have been properly signed and the Bids are generally in order. Any Bids found to be non-responsive for any reason or not meeting any criteria specified in this RFP, will be rejected by the AAI and shall not be included for further consideration.
Initial Bid scrutiny will be held and the Bids will be treated as non-responsive, if Bids are:

- Not submitted in the format as specified in this RFP document;
- Received without the Letter of Authorization;
- Power of Attorney/Board Resolution;
- EMD and Tender Fees Receipts;
- Found with suppression of details;
- Submitted with incomplete information, subjective, conditional offers and partial offers;
- Submitted without the documents required under this RFP;
- Non-compliant to any of the clauses mentioned in this RFP;
- With lesser validity period than prescribed in this RFP.

### 1.3 Clarification on Bids

During the bid evaluation (at any stage whether during pre-qualification, technical or commercial evaluation), AAI may, at its discretion, ask the Bidder for a clarification of its bid and the decision of AAI or Evaluation Committee will be final. The request for clarification and the response shall be in writing, and no change in the price or substance of the bid shall be sought, offered, or permitted.

### 1.4 Evaluation Process

- AAI will constitute a Evaluation Committee to evaluate the bids
- The Evaluation Committee shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability to submit requisite supporting documents / documentary evidence, may lead to rejection.
- The decision of the Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of discussion with the Committee.
- Presentation by the bidder during the technical evaluation process is mandatory. The Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their bids.
The Evaluation Committee reserves the right to reject any or all bids on the basis of any deviations. Each of the responses / Proposals shall be evaluated as per the criteria and requirements specified in this RFP.

The evaluation stages are as follows:-

1.4.1 Stage 1: Pre-Qualification

- The evaluation committee shall open Pre-Qualification Bid.
- If the response to “pre-qualification” is received as per requirements and prescribed format then the AAI shall evaluate the response to the Pre-Qualification requirements in accordance with the Pre-qualification requirements specified in this RFP.
- The Pre-Qualification bid MUST contain all the documents mentioned for Submission of the Pre-Qualification Bid. Each of the Pre-Qualification condition mentioned is MANDATORY. In case the Bidder does not meet any one of the conditions, the bidder will be disqualified.
- A checklist has to be created by the bidder and be submitted along the proposal with proper page-wise indexing of all supporting documents.
- Results of the Pre-Qualification Bid will be published on the CPP portal.

1.4.2 Stage 2: Technical Evaluation

- Technical Bid will be evaluated only for Bidders who are declared successful in Stage 1.
- The evaluation committee will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at the AAI’s discretion.
- The bidders’ technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework.
- The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g. detailed project citations and completion certificates, and all others) as required for technical evaluation.
- AAI and the evaluation committee may seek written clarifications from the bidders. The primary function of clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the bid documents. Written clarifications provide the opportunity for the evaluation committee / AAI to state its requirements clearly and for the bidder to more clearly state its proposal. AAI and the evaluation committee may seek inputs.
from their professional, technical experts in the evaluation process. However, the bidder will not be allowed to modify or amend their proposals during these clarifications.

- Each technical bid shall be awarded an absolute technical score of ‘T1’ marks out of a total of 100 marks. A detailed evaluation matrix is provided in the following section.

- Only bidders who score a total Technical score of 70 or more will qualify for the evaluation of their commercial bids.

- **Technical Score Formulation:** The highest evaluated absolute Technical score (Tmax) will be given the maximum technical score (Tn) of 100 points. The technical scores (Tn) of the other bidders will be computed as per the formula for determining the technical scores as given below:

\[ Tn = 100 \times \left( \frac{T1}{Tmax} \right) \]

Where,

- \( Tn \) = Normalized Technical score for the bidder under consideration,
- \( T1 \) = Absolute Technical Score for the bidder under consideration,
- \( Tmax \) = Maximum absolute Technical Score obtained by any bidder

Results of the Technical Bid opening will be published on the CPP portal.

Evaluation Committee’s decision in this regard shall be final & binding and no further discussion/interface will be held with the bidders whose bids are technically disqualified/rejected. Evaluation of Technical Proposals by Evaluation Committee shall not be questioned by any of the Bidders. Evaluation Committee may ask Bidder(s) for additional information to verify claims made in Technical Bid documentation from the Bidder on the already submitted Technical Proposal at any point of time before opening of the Price bid.

### 1.4.3 Stage 3: Commercial Evaluation process

The Commercial Bids of only the technically qualified bidders will be opened by the Evaluation Committee for evaluation in the presence of the bidder’s representatives.

- The bid value shall include all taxes and shall be in Indian Rupees (₹).

- If there is a discrepancy between words and figures, the amount in words will prevail.

- **Financial Score Formulation:** The lowest evaluated Financial quote (Fmin) based on NPV value (refer section Annexure III) will be given the maximum financial score (Fn) of 100 points. The financial scores (Fn) of the other Financial quotes will be computed as per the formula for determining the financial scores given below:
\[ Fn = 100 \times \left( \frac{F_{\min}}{F_1} \right) \]

Where,

\( Fn \) = Normalized financial score for the bidder under consideration,
\( F_1 \) = Absolute financial quote for the bidder under consideration,
\( F_{\min} \) = Minimum absolute financial quote obtained from any bidder

### 1.4.4 Final Evaluation

- Proposals will be ranked according to the combined normalised technical (Tn) and financial (Fn) scores using the weights.

- The combined technical and financial score

\[ (S) = T_n \times T + F_n \times F \]

Where:

\( T = 0.80 \), the weight given to the Technical Score;
\( F = 0.20 \), the weight given to the Financial Score;
\( T + F = 1 \)

- The bidder who scores the highest combined technical and financial score as detailed above will be considered for selection and award of the contract.

- If two or more bidders have same combined technical and financial score, then the bidder with the higher financial score will be selected. Further, if two or more bidders have same financial score, then the bidder with higher technical score will be selected.

- Results of the Commercial Bid opening will be published on the CPP portal.
1.5 Pre-Qualification Criteria

1.5.1 Pre-qualification Criteria of Bidders

The Bidder's pre-qualification bid will be evaluated as per the following criteria:

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Criteria</th>
<th>Documentary proof to be submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registered Legal entity</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1 | The bidder should be –  
- A company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013  
- Registered with the GST Authorities  
- Company should have a valid PAN number  
OR  
- Partnerships Firm registered under the Limited Liability Partnerships (registered under LLP Act, 2008)  
- Registered with the GST Authorities  
- Should have a valid PAN and GSTN number |  
- Certificate of Incorporation; and  
- GST Registration certificate issued by GSTN authorities (copy)  
- PAN Card (copy) |
| **Duration of Operations** | | |
| 2 | The bidder should have been in operation for a period of at least 3 years (i.e. for FY 2015-16, FY 2016-17, FY 2017-18) in India prior to the date of submission of bid | Certificate by company secretary |
| **Financial Stability** | | |
| 3 | The Bidder should have a positive net worth ending 31st March 2018 as evidenced by the audited accounts of the company. Refer Net worth definition in the section below | Audited Financial Statements or statutory auditor certificate/ certificate from Company Secretary of Bidder specifying the net worth for the specified year. |
| 4 | The bidder should have minimum annual turnover of ₹ 231.10 crore from system/software development or implementation or systems integration in each of the last three financial years (Financial years FY 2015-16, FY 2016-17, FY 2017-18). | Audited Financial Statement for Financial years FY 2015-16, FY 2016-17, FY 2017-18;  
Statutory auditor’s certificate OR certificate from Company Secretary of the bidder clearly specifying the turnover from software development or implementation or systems integration for the specified years. |
## Project Experience

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Criteria</th>
<th>Documentary proof to be submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bidder (or its parent company) should have the experience in System Integration/application development projects** for Central Government/any State Government/PSU or private companies (such companies should be public limited having turnover of minimum Rs. 231.10 Cr.) in last 5 financial years (FY 2013-18) in software development or implementation or systems integration. Projects under model BOOT/BOT/BOO model will not be considered for evaluation criteria.</td>
<td>• Copy of work order/client certificate as documentary proof for the stated project value and implementation status; in case of certain phase completion, client certificate for the value of the phase and its completion certificate or Certificate by the Company Secretary of the bidder for the stated project value and implementation status. in case of certain phase completion, Company Secretary certificate for the value of the phase and its status.</td>
</tr>
<tr>
<td>5</td>
<td><strong>1. At least one (1) such project of value that is 80% or more of Total Estimated Cost</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>2. At least two (2) such projects each of value that is 50% or more of Total Estimated Cost</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>3. At least three (3) such projects each of value that is 40% or more of Total Estimated Cost</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For evaluation of project value, Financial value of completed milestones will only be considered for the projects cited. The projects cited should have at least one completed milestone as Go-Live to be considered.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>“All projects with at least one Go-Live in the last 5 years will only be considered. For example, if a project was awarded in 2011 and one of the Go-Live occurred in 2014, such project shall be considered. However, if the project that was awarded in 2011 and all phase Go-Live occurred prior to 2013, such projects on basis of ongoing O&amp;M in last 5 year period shall not be considered.”</strong></td>
<td></td>
</tr>
</tbody>
</table>

## Certifications

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Criteria</th>
<th>Documentary proof to be submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>The bidder should have experience of obtaining ISO 27001-2013 certifications (or above) OR obtained CERT-IN Certification for client or its own organization in last 5 years</td>
<td>• Copy of certificate for its own organization OR • letter from client certifying that the Bidder had obtained the certification on behalf of the client; or • Certificate by the Company Secretary of the bidder to this effect</td>
</tr>
</tbody>
</table>
**Note:** Any bid failing to meet the above pre-qualification criteria shall be rejected and will not be considered for Technical Evaluation.

**Additional Mandatory requirements in provided format in Tender 1 document**

The bidder should submit all the following mandatory additional documents listed. If any of the mandatory documents are not in order, such proposals are liable to be rejected without further evaluation.

(i) Acceptance Letter  
(ii) Force Majeure  
(iii) Undertaking Letter  
(iv) MAF  
(v) Integrity Pact  
(vi) Non-Disclosure Agreement (NDA)  
(vii) Undertaking for Not Black Listed  
(viii) Board Resolution/ OR Power of Attorney in favor of authorized signatory  
(ix) No Deviation Certificate  

**Formats for the same are provided in Tender Document 1**

1. **Change in Pre-Qualification Criteria**

   If there is a change in the status of the bidder with reference to any of the pre-qualification criterion specified above, during the bid process till the award of the project, the bidder should immediately bring the same to the notice of AAI. The same shall be presented to Steering Committee and be evaluated for decision on rejection/acceptance of bid based on nature of change(s).

2. **Key Terms for Pre-Qualification Criteria**

   For the purposes of this RFP, some key terms that have been used for pre-qualification criteria have been defined below:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net-worth (Consolidated)</td>
<td>Means the aggregate value of the paid-up share capital and all reserves created out of the profits and securities premium account, after deducting the aggregate value of the accumulated losses, deferred expenditure and miscellaneous expenditure not written off, as per the audited balance sheet, but does not include reserves created out of revaluation of assets, write-back of depreciation and amalgamation.</td>
</tr>
<tr>
<td><strong>Turnover</strong></td>
<td>Means the aggregate value of the realisation of amount made from the sale, supply or distribution of goods or on account of services rendered, or both, by the company during a financial year.</td>
</tr>
</tbody>
</table>
| **Financial Year (Company)** | In relation to any company or body corporate, means the period ending on the 31st day of March every year, and where it has been incorporated on or after the 1st day of January of a year, the period ending on the 31st day of March of the following year, in respect whereof financial statement of the company or body corporate is made up:  
Provided that on an application made by a company or body corporate, which is a holding company or a subsidiary of a company incorporated outside India and is required to follow a different financial year for consolidation of its accounts outside India, the Tribunal may, if it is satisfied, allow any period as its financial year, whether or not that period is a year.  
Provided further that a company or body corporate, existing on the commencement of this Act, shall, within a period of two years from such commencement, align its financial year as per the provisions of this clause. |
| **Financial Year (LLP)** | Means the period from the 1st day of April of a year to the 31st day of March of the year next following that year; Provided that in the case of a limited liability partnership incorporated after the 30th day of September of a year, the financial year may end on the 31st day of March of the year next following that year. |
| **Auditor** | Auditor shall mean the Statutory auditor of a company |
1.6 Technical Evaluation Framework

AAI (or a nominated party) reserves the right to check/validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the Bidder.

The following sections explain how the Bidders will be evaluated on each of the technical evaluation criteria:

<table>
<thead>
<tr>
<th>#</th>
<th>Evaluation Criteria</th>
<th>Total Marks</th>
<th>Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bidder’s Experience</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Proposed Solution</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Approach and Methodology</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Key Resources, Deployment Plan and Team Composition</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Technical Presentation</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

The following sections explain how the Bidders will be evaluated on each of the technical evaluation criteria.
1.6.1 Bidder’s Experience

The bidders are required to provide the details regarding their relevant experience in form of citations as mentioned in the following table. Bidders to note –

1. In case, if more than the required numbers of citations are submitted by the bidder then in such a situation only the first few required citations in sequence shall be evaluated by the Evaluation Committee and a score shall be assigned to each citation. The rest of the other citations (of that category) shall be declined.

2. The citations provided in pre-qualification criteria can be reused for technical proposal as well.

3. The bidder’s shall mandatorily provide a “Client reference” for each of the citations it submits in its technical proposal to AAI along with their bids. AAI reserves the right to contact the client of the bidder for ascertaining the veracity of claims made in the citation. The citations without the client references are liable to be rejected.

4. The citations should be for projects which have declared atleast one phase of Go Live in last 5 years from date of bid submission. The go-live shall mean go-live of the entire project or go-live of a particular phase of the project. The value of the project to be considered shall be according to the milestones completed for the project (to be calculated based on invoice raised for the project).

5. Evidence Required: Copy of work order/client certificate as documentary proof for the stated project value and implementation status; in case of certain phase completion, client certificate for the value of the phase and its completion certificate or Certificate by the Company Secretary of the bidder for the stated project value and implementation status. In case of certain phase completion, Company Secretary certificate for the value of the phase and its status

6. Projects undertaken by the bidder (or its parent company) for Central Government/ any State Government/ PSU or private companies (such companies should be public limited having turnover of minimum Rs. 231.10 Cr.) during the last five (5) years from the date of submission of bid shall be considered for the below criteria

7. Projects under BOOT/BOO/BOT model will not be considered for evaluation

8. In case project that was executed as JV/consortium, only the percentage share in JV/consortium shall be taken as value for evaluation

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria 2</th>
<th>Details 3</th>
<th>Max. Marks Allocated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Experience in development of applications large scale projects</td>
<td>Experience in Application Development and System Integration during the last five (5) years from the date of submission of bid.</td>
<td>10</td>
</tr>
</tbody>
</table>

2 For purpose of experience, parent company experience can also be included
3 In case of foreign currency, use the exchange rate of date of completion of milestone for purpose of calculation
<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Details</th>
<th>Max. Marks Allocated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maximum of two citations are to be submitted that will be marked as per the following criteria on per project basis:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project value of 80% or more of the Estimated Project Cost = 5 Marks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project value of 50% to less than 80% of the Estimated Project Cost = 4 Marks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project value of 40% to less than 50% of the Estimated Project Cost = 3 Marks</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Experience in operations and maintenance of application</td>
<td>Experience in providing O&amp;M support for IT applications. Atleast one year of O&amp;M support should have been provided for the cited projects.</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum of two citations are to be submitted that will be marked as per the following criteria on per project basis:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Project value of &gt;INR20cr. = 5 Marks per project</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Analytics based Project</td>
<td>Experience in implementing projects that include analytics (either machine learning or big data or data science) as part of scope</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum size of project shall be INR10cr. Citations will be marked as per the following criteria:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Citation Meeting Criteria – 2.5 Marks per citation (max two citation)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Portal/ Mobile Apps development</td>
<td>Experience in development/ development cum maintenance of Web Portal and Mobile App</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum size of project shall be INR10cr. Citations will be marked as per the following criteria:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Citation Meeting Criteria (Max 2 Citation required)– 2.5 Marks</td>
<td></td>
</tr>
</tbody>
</table>
### Criteria Details

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Details</th>
<th>Max. Marks Allocated</th>
</tr>
</thead>
</table>
| 5  | **Application Development in Area of Civil Aviation Airspace Management, Civil Aviation Regulations, Drones Flight Approval** | Experience in development/ development cum maintenance of application for Civil Aviation Airspace Management, Civil Aviation Regulations, Drones Flight Approval.  
Minimum size of project shall be INR2cr. Citations will be marked as per the following criteria:  
Single Citation for Civil Aviation Airspace Management – 2 Marks  
Single Citation for Civil Aviation Regulations – 1 Mark  
Single Citation for Drones Flight Approval – 2 Mark | 5                                                                                     |

Total |                                                                                             | 35                                                                                                                                     |                      |

#### 1.6.2 Proposed Solution

| 1  | Solution Design and Approach                                                                 | The bidder must propose an Architecture of Digital Sky. The proposed architecture should cover detailed explanation and diagrams for –  
- Business Architecture  
- Application Architecture  
- Integration Architecture  
- Technology Architecture  
- Security architecture  
- Sizing Considerations  
- Deployment Architecture | 9                                                                                   |
| 2  | Technologies Proposed                                                                      | Technologies that have been proposed to meet the technical requirements of Digital Sky                                                                 | 9                                                                 |

**TOTAL** |                                                                                             | 18                                                                                                                                     |                      |
1.6.3 Approach and Methodology

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Criteria Details</th>
<th>Marks Allocated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Understanding of Business and Scope of work and all aspect of the Project</td>
<td>Demonstrated level of understanding of the business requirements, the project purpose and scope of work. Understanding of the international best practices, risks &amp; mitigation.</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Approach for Implementation of the project, O&amp;M Exit Management</td>
<td>Approach for project implementation, timelines management and bidder’s plan for performing the required services as detailed in scope of work in the RFP and to meet the desired SLAs</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

1.6.4 Key Resources, Deployment Plan and Team Composition

1. Managed Service Provider (MSP) should deploy best of class professionals to ensure successful execution of this project.

2. The Technical expertise should come from the IT System Integrator.

3. The MSP will, in its proposal, include the names and detailed Curriculum Vitae (CV) of their Key Resources in the CV Pro-forma as given in Appendix. All supporting documents such as copy of education qualification degree/certificate, experience certificate, technical/professional certifications (if any), etc. shall be submitted by the selected bidder at time of on-boarding.

4. Points will be allocated according to the following:
   a. Educational Qualification, relevant Trainings & Certification (0.5 points)
   b. Total experience (0.5 points)
   c. Experience in similar role in 2 projects or more OR with similar career experience (applicable for aviation expert only) (2 points)

5. The following is the list of key resources:-

<table>
<thead>
<tr>
<th>Title</th>
<th>Exp.</th>
<th>Qualification</th>
<th>Project Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager</td>
<td>Min 10 years</td>
<td>BE/BTech degree in Computer Science or related field plus MBA.</td>
<td>Responsible for project management of projects requiring application development, O&amp;M of the developed application, and analytics.</td>
</tr>
<tr>
<td>(3 points)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Exp.</td>
<td>Qualification</td>
<td>Project Experience</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Principal Architect (3 points)</td>
<td>Min 10 years</td>
<td>BE/BTech degree in Computer Science or related field.</td>
<td>Candidate should have Comprehensive knowledge of software engineering methodologies; project Management in the field of Information Technology. Excellent communication and presentation skills.</td>
</tr>
<tr>
<td>Product Manager (3 points)</td>
<td>Min 8 years</td>
<td>BE/BTech/BS degree in engineering, Computer science</td>
<td>Candidate should have Comprehensive knowledge of software engineering methodologies, principles, practices, consulting Process Improvement, Applications, project Management in the field of Information Technology, knowledge of product management practices, processes, and tools in software industry. Excellent communication and presentation skills.</td>
</tr>
<tr>
<td>Architect, Front end/Back end (3 points)</td>
<td>Min 8 years</td>
<td>BE/B. Tech in Computers Sc.,/IS/Electronics /MCA</td>
<td>Candidate should have specific hands-on experience as the Architect of a large scale software system using open source stack. The candidate must also have hands on experience in designing, developing, testing and deploying high performance and throughput systems. The candidate must have strong expertise in the core technologies for the profile. Experience with the specific tools in the technology stack (or equivalents) is preferred. Experience in automated builds, deployments, debugging, and other open source tools are required.</td>
</tr>
<tr>
<td>Security Architect (3 points)</td>
<td>Min 8 years</td>
<td>BE/B. Tech in Computer Science/ IS/ Electronics /MCA</td>
<td>For Security Architect, Candidate should have specific hands-on experience as Security Architect of a large scale software system using open source stack. The candidate must also have hands on experience in IPS, TATACS, Content filtering, SSIM, SIEM, Firewalls, HIPS management. Ability to architect solution at application, system and Network levels and manage. Good understanding of OSI model, TCP/IP protocol suite (IP, ARP, ICMP, TCP, UDP, SNMP, FTP, TFTP), Windows/Linus/Citrix (ADS, DNS, DHCP), Network security, VPN, Firewall, RSA, PKI, Digital certificate etc. Experience in development of technical strategy for handling various types of vulnerabilities, cyber-attack scenarios and security issues.</td>
</tr>
<tr>
<td>Technical lead (3 points)</td>
<td>Min 6 years</td>
<td>BE/B. Tech in Computer Science/ IS/ Electronics /MCA</td>
<td>Candidate should have specific hands-on experience as tech lead in the software development large scale systems using open source stack. The candidate should have experience in developing, testing and deploying high performance and throughput systems. Strong expertise in the core technologies as mentioned against the profile. Experience with the specific tools in the technology stack (or equivalents) is preferred. Ability to build APIs, automation scripts, build, deployment, monitoring scripts, and debugging/troubleshooting is required.</td>
</tr>
<tr>
<td>UX/UI Expert (3 points)</td>
<td>Min 6 years</td>
<td>BS/MS in Human-Computer Interaction, Interaction Design, or related</td>
<td>Candidate should have specific hands on experience in managing the aesthetic/optimization/interactive design in the projects undertaken.</td>
</tr>
</tbody>
</table>
Title | Exp. | Qualification | Project Experience
--- | --- | --- | ---
Aviation Industry Expert (3 points) | Min 8 years | MBA/PGDM/BE/B.Tech | The candidate in their experience should specifically have collaborated with product management and engineering team to define and implement innovative solutions for the product direction, visuals and experience and created interaction models, mockups and wireframes. The candidate should have experience of modelling information and flows using UX best practices for web and mobile and developed documents that capture UX requirements and standards.

GIS Expert (3 points) | Min 6 years | B.E., B. Tech, Post Graduate in RS/GIS | Candidate should have specific hands-on experience in aviation sector especially related to compliance/regulatory matters of aviation sector. Further should be well versed with Air Traffic Management systems.

The expert should have demonstrated knowledge GIS Skills (example in Auto CAD 2011, Arc GIS-10, ILLWIS and EARDAS 9.3, Map info professional 10.5, Global Mapper 10, Google Earth, QGIS).

The expert should have undertaken projects in area of GIS demonstrating experience in working with one or more of the above tools.

TOTAL: 27 POINTS

1.6.5 Technical Presentation

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Criteria Details</th>
<th>Marks Allotted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Understanding of the Project and Approach, including the Implementation and Project Plan with timelines and Solution Design</td>
<td>The bidder must share their understanding of the project. The bidder must showcase their proposed solution for the development and maintenance of the Digital Sky platform. The bidder is expected to give a summary of various plans submitted in the response to RFP</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Demonstration of relevant experience and successful execution of application development and maintenance of similar complexity</td>
<td>The bidder must share the relevant experience for development and maintenance of application of similar complexity. The bidders must showcase their submitted citations as per this RFP. The submitted citations must adhere to the qualification criterion mention in this RFP</td>
<td>2</td>
</tr>
</tbody>
</table>
# TENDER DOCUMENT 3 – QUALIFICATION AND SELECTION CRITERIA FOR DIGITAL SKY

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Criteria Details</th>
<th>Marks Allotted</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Demonstration of Technical Expertise and Required Skills for the project execution</td>
<td>The bidder must demonstrate the technical expertise for the successful execution of this projects</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Demonstration of UX/UI</td>
<td>The bidders must prepare a UX/UI and demonstrate its capability to build an attractive and user friendly interface</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL</strong></td>
<td></td>
<td><strong>10</strong></td>
</tr>
</tbody>
</table>
1.7 Commercial Bids Evaluation criteria

The following shall be the criteria for evaluation of commercial bids:

- Commercial proposals / bids of only those firms who are technically qualified shall be opened on the date & time to be intimated later, in the presence of the bidder’s representatives who choose to attend and shall be processed as per the process defined in the RFP.

- AAI and the evaluation committee may seek written clarifications from the bidders on their commercial bids during the evaluation process. AAI and the evaluation committee may seek inputs from their professional, technical experts in the evaluation process. However, the bidder will not be allowed to modify or amend their proposals during these clarifications.

- Further, if commercial bids are found to be unreasonable in terms of ratio of costs, in order to manipulate for early payments as per schedule, AAI can reject such bids.
2. Annexure I: Formats for Submission of the Pre-Qualification Bid

Instructions:

- Please provide details of compliance with reference to pre-qualification criteria in the formats provided below. Please note that provision of information in incorrect formats may lead to disqualification.

- Please provide requisite documentary proof (as specified in PQ section) for all information provided. Please note that non-submission of documentary proof may lead to disqualification.
## 2.1 Details of Bidder Organization

*<Company Letter Head>*

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Item</th>
<th>Bidder’s Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Company Name</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Year Established</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Name of the Directors as per MoA</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Incorporated in India (Yes or No)</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>PAN</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>GST</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>CIN (only in case of Company)</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Key representative for this project &amp; designation along with contact details (email, mobile)</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Name of the Authorized signatory along with contact details (email, mobile)</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Head Office Address</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Details of EMD (Name of Bank, Amount, Date of Issue, Validity)</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Brief Description of the Organization</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Office Address (from where services will be delivered)</td>
<td></td>
</tr>
</tbody>
</table>

### Sub-Contracting Partner Organization Details

<table>
<thead>
<tr>
<th>Company Name :</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Office</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td></td>
</tr>
<tr>
<td>Company Status (public, private)</td>
<td></td>
</tr>
<tr>
<td>Incorporation Date</td>
<td></td>
</tr>
<tr>
<td>ROC Number</td>
<td></td>
</tr>
<tr>
<td>Total Employees</td>
<td></td>
</tr>
<tr>
<td>Company Website URL</td>
<td></td>
</tr>
</tbody>
</table>
2.2 Financial Information of the Bidder

<Date>

<table>
<thead>
<tr>
<th>Financial Information</th>
<th>&lt;&lt;Insert FY&gt;&gt;</th>
<th>&lt;&lt;Insert FY&gt;&gt;</th>
<th>&lt;&lt;Insert FY&gt;&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue (in INR crores)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenue from IT services (in INR crore)*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Worth (in INR crores)*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other Relevant Information

Supporting Documents:

a. Audited financial statements for each of the three financial years (Please include only the sections on P&L, revenue and the assets, not the entire balance sheet.)
b. Certification by the company secretary or auditors supporting the revenue break-up and Net Worth

*As per requirements of Pre qualification Criteria Table

<Signature> <Company Seal>

Name: 
Designation: 
Name and Address of Auditor/ Company Secretary:
2.3 System Integrator Experience

<table>
<thead>
<tr>
<th>Client Information</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of client</td>
<td></td>
</tr>
<tr>
<td>Name of the person who can be referred to from Clients' side, with name, designation, postal address, contact phone, fax number, e-mail id,</td>
<td></td>
</tr>
<tr>
<td>Nature of business / operations of client</td>
<td></td>
</tr>
<tr>
<td>Project value in Crores</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief description of the Project</td>
<td></td>
</tr>
<tr>
<td>Functional areas of business covered in the project</td>
<td></td>
</tr>
<tr>
<td>Duration of engagement (with Start date and end-date/Go-Live date)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope of the Project</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Yes/No</td>
</tr>
<tr>
<td>Solution implementation</td>
<td></td>
</tr>
<tr>
<td>Cloud hosting services</td>
<td></td>
</tr>
<tr>
<td>Post-implementation operations</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>

**Supporting Documents**

**Note:** A client citation with reference to the above experience/citation for eGCA Application refers to one or more of the following, along with the Work order/Contract copy:

1) A Client Letter (in case of ongoing project) OR Company Secretary Certificate
2) Completion/Go-live certificate

The above supporting document(s) should clearly specify the value of the project and project status (i.e. Go-live/ completed) with date
The above document(s) should be duly certified by authorized signatory.

Please use separate forms for multiple citations.

<On behalf of Bidder Name>
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Firm:
Address:
Seal/Stamp of Bidder:
3. Annexure II: Formats for Submission of the Technical Bid

Bidder needs to submit the technical bid in the forms presented below. In case of information being sought in tabular format bidder must also provide excel file titled – section Technical_Bid_DigitalSky_<Section Number>_<Section Name>. In case of any discrepancy the PDF submission will supersede the excel version.
3.1 Proposed Solution

3.1.1 Technologies Proposed – Bill of Material (Hardware and Software)

The bidder needs to provide detailed bill of material covering all the hardware and software components to be used in the project.

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Solution Area</th>
<th>Hardware / Software</th>
<th>Reference to RFP Section, Page, Requirement</th>
<th>Name of Product and Technology</th>
<th>Version, Make, Model</th>
<th>Name of Offerer (Company name)</th>
<th>Brief Description (Including Product Name)</th>
<th>Brief description on applicability to project</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Including no. of licenses if applicable
3.1.2 Solution Design and Approach

<Provide details of the entire solution, along with the key differentiators covering all requirements as laid out in the RFP>

Include diagram and detailed description of –

1. Business Architecture
2. Application Architecture
3. Integration Architecture
4. Technology Architecture
5. Security architecture
6. Sizing Considerations
7. Deployment Architecture

Bidder must cover all aspects of the solution showcasing the suitability of the solution to meet all the requirements listed out in the tender. The document must be submitted in PDF and MS Word format.

In addition, bidder must fill and submit the table below in order to showcase compliance to all requirements mentioned in the RFP.

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Functional Requirement</th>
<th>FR#</th>
<th>Page number</th>
<th>Specify Name of the component to be used along with version (COTS/OSS/Bespoke)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Approach and Methodology

Bidder must submit the detailed document covering entire approach and methodology for running the project for the entire duration including but not limited to Governance, Program Management, Software Development Methodology, Operation and Maintenance Methodology, SLA Monitoring Approach, Business Support and Grievance Redressal Approach etc. Further, demonstrating understanding and implementing international best practices in the current project
Further, bidders are to demonstrate their understanding of the objectives of the assignment and mapping of the requirements to work plan, resource allocation, completeness and responsiveness (in terms of exhaustively catering to requirements indicated in the Scope of Work).

### 3.2.1 Project Plan

The bidder is required to submit integrated project plan up to Go-Live and an operations plan for O&M phase of the project. This can be submitted in MS Project format or MS Excel. Bidder must also cover this in the presentation to AAI.

<table>
<thead>
<tr>
<th>No</th>
<th>Activity(^5)</th>
<th>Calendar Months</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Duration of activities shall be indicated in the form of a bar chart.

\(^5\) Indicate all main activities of the assignment, including delivery of reports (e.g.: inception, interim, and final reports), and other benchmarks such as Purchaser approvals. For phased assignments indicate activities, delivery of reports, and benchmarks separately for each phase.
3.2.2 Resource Deployment Plan

The bidder is required to submit separate resource deployment plans for before and after “Go-Live” i.e. resource deployment plan during implementation phase and resource deployment plan during “Operations and maintenance phase”.

Bidder may add the resource details to the project plan itself and submit along with the project plan both for Implementation and Operations phase.

Bidder must provide details of the total number of resources to be deployed in the format below:

<table>
<thead>
<tr>
<th>Team Name</th>
<th>Team Lead</th>
<th>Task Assigned</th>
<th>Total number of resources</th>
<th>Total Man Months Effort</th>
<th>Weighted Average of Team Experience (yrs)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Functional&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Software Development – Phase 1&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Add more rows to the table above to cover all resources. The MSP must deploy only full time resources. If any team has less than FTE resource then it should be mentioned separately. If Team is proposed for entire duration of project then state – for entire duration of project, else provide Total Man-month effort

In addition, bidder must provide details of key resources mentioned in RFP in the below format –

<table>
<thead>
<tr>
<th>Position in the project</th>
<th>Name</th>
<th>Organization Name</th>
<th>Total Experience</th>
<th>Qualification</th>
<th>Years with bidder / Subcontractor</th>
</tr>
</thead>
</table>
### 3.3 Curriculum Vitae (CV) of Team Members

The bidder must provide CVs of all the key resources mentioned in the RFP.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Item</th>
<th>Bidder’s Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name of the Resource</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Specify role to be played in the project</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Name of Employer</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Number of years with the Current Employer</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Total Experience (in Years)</td>
<td></td>
</tr>
</tbody>
</table>

Experience in yrs. (Provide details regarding name of organizations worked for, Designation, responsibilities, tenure etc. atleast for last 5 years)

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Name of Employer</th>
<th>From</th>
<th>To</th>
<th>Designation/ Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Summarized professional experience (Relevant to the Current Project) in reverse chronological order

<table>
<thead>
<tr>
<th>S. No.</th>
<th>From</th>
<th>To</th>
<th>Company Project Position Relevant Functional, Technical and Managerial experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Educational Background, Training Certification including institutions, % of marks, specialization areas etc.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Degree</th>
<th>Year of Award of Degree</th>
<th>University</th>
<th>% of marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Selected Bidder is required to submit supporting documents related to individuals proposed in the bid. Any non-compliance identified w.r.t. supporting of documents may lead to disqualification of the bid of the bidder.
4. Annexure III: Formats for Submission of the Commercial Bid

Commercial Bid Format – Total Bid Value

Please refer to Scope of Work of this RFP (Payment terms and schedule) for quoting the bid value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Total Price (₹)</th>
<th>Basic Price (₹)</th>
<th>Taxes(₹)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Bid Value^6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECTION 1: Required Scope</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation Phase (PART A) – For development and Go-Live of web portal and mobile app (Android/iOS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O&amp;M Phase^7 (PART B)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECTION 2: Optional Items^8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blended Cost for Change Requests (300 man months) (PART C)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost for support for change in CSP^9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For the purpose of calculation of financial bid value, Net Present Value of the same shall be calculated. The discounting factor for the same shall be 10%. The following table describes the value inputs for each category head based on above cost.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Implementation Phase (Year 1)</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Year 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Phase (PART A) – For development and Go-</td>
<td>Value A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

^6 Sum of Section 1 and Section 2

^7 O&M Phase Cost should be minimum 40% of PART A + PART B

^8 Optional Items may not be utilized or minimally utilized during the course of the project. Such costs have been taken for purpose of any additional requirements that may be identified during the contract period. It is highlighted that payments against actual effort shall be paid for such optional items.

^9 The cost is related to requirement for change in CSP due to regulatory requirements that may come up in future. For the purpose, DGCA/AAI may demand MSP to host application in different environment due to such regulatory requirements. Please note that such cost shall be paid only in case the requirement for shift of CSP is exercised by DGCA/AAI.
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Implementation Phase (Year 1)</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Year 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live of web portal and mobile app (android/iOS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O&amp;M Phase (PART B)</td>
<td>Value B /5</td>
<td>Value B /5</td>
<td>Value B /5</td>
<td>Value B /5</td>
<td>Value B /5</td>
<td>Value B /5</td>
</tr>
<tr>
<td>Blended Cost for Change Requests (300 man months) (PART C)</td>
<td>Value D/5</td>
<td>Value D /5</td>
<td>Value D /5</td>
<td>Value D /5</td>
<td>Value D /5</td>
<td>Value D /5</td>
</tr>
<tr>
<td>Cost for support for change in CSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All areas colored grey are required to be filled and thereon, NPV is required to be calculated.

### Bid Price (NPV Value) (Discount Rate of 10%) Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>In Words</th>
<th>In Numerals</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL BID VALUE (Inclusive of taxes). Please highlight taxes in separate column</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please refer below sections for formats to provide detailed cost break up.

1. **PART A - Implementation Phase**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameter</th>
<th>Total Price (₹)</th>
<th>Basic Price (₹)</th>
<th>Taxes(₹)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Solution development, testing and implementation (this includes costs associated with manpower costs, license cost, helpdesk infrastructure development/provisioning, license costs, cloud provisioning, etc)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 2. Others

| Total Cost* |  |

**TOTAL VALUE IN WORDS :**

### 2. PART B - O&M Phase

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameter</th>
<th>TOTAL COST</th>
<th>Base Rate</th>
<th>Taxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application Support &amp; Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Help-Desk operations including physical license issuance for pilots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Hosting Cost# (please provide break up of hosting charges as per formats provided in below sections)(^{10})</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Other operational costs such as SMS, Audits, training, etc</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TOTAL COST***

\(^{#}\) In case there is a requirement for change in hosting environment, AAI/DGCA may decide to undertake the hosting charges by themselves. In this case, hosting charges shall not be paid to MSP post migration to new environment

**TOTAL O&M VALUE IN WORDS :**

### Hosting Charges

<table>
<thead>
<tr>
<th>Component</th>
<th>Unit Cost</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMs/Containers (for various sizes and tools proposed)</td>
<td></td>
<td>Cost :(^{*})</td>
</tr>
</tbody>
</table>

\(^{10}\) For the purpose of costing, live tracking of drones is not to be considered for cloud sizing provisioning though the functionality needs to be developed for the same as part of solution.
<table>
<thead>
<tr>
<th>Component</th>
<th>Unit Cost</th>
<th>Description</th>
<th>Quantity:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage (1TB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Block Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Object Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• File Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Include tax column to include taxes
3. **PART C – Optional - Additional Manpower**

AAI wants the bidder to provide the cost of additional person rate inclusive of travel, boarding and lodging costs. The cost required is for blended rates applicable for undertaking any change request related work to be undertaken by MSP. The utilization of such resources during the project is the sole discretion of AAI/DGCA. Such costs are taken shall be the financial benchmark for Change Request (in terms of man month rates).

**It is highlighted that the cost provided will be used for commercial evaluation.**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Type of Resource</th>
<th>Purpose</th>
<th>No. of Man Months</th>
<th>Rate per Man month in INR</th>
<th>Applicable Taxes</th>
<th>Total Price in INR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Blended Rate for Manpower</td>
<td>The following rates shall be taken for purpose of commercial calculation for Change Request undertaken during the course of the project</td>
<td>300</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Cost**

**AUTHORIZED SIGNATURE __________________________**

**NAME OF THE SIGNATORY _________________________**

**NAME & ADDRESS OF THE TENDERER**
Appendix 1 – Current Developed Digital Sky Platform – Pilot Phase

Some work has already been undertaken on the envisaged Digital Sky platform by iSPIRIT (www.ispirt.in) which can be used as a reference by the prospective vendor. It is the upto the prospective vendor to leverage the existing resources for developing the proposed solution. The prospective may also choose to use the existing resources only for reference purposes and develop the solution on their own.

The table below contains an overview of the existing resources that can be reviewed/used by the prospective vendor:

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1      | Digital Sky Registration and Permission Layer | The link (https://github.com/ispirt) contains the source code for various solution elements of Digital Sky registration layer such as code for front end, back end and some APIs.  
The demo for the same is available on the Link (https://digitalsky-uat.centralindia.cloudapp.azure.com:8080/)  
The link also contains information on aspects such as Architecture and Deployment for Registry. |
| 2      | Digital Sky APIs | The link (https://ispirt.github.io/digital-sky-docs/) contains various APIs that can be used to enable various functionalities on the Digital Sky platform. |
| 3      | UI Design Changes | The link (https://github.com/iSPIRT/digitalsky-frontend/commit/7a43bf355d22ca1252c9aeaa8af887c2aafe2b0e) contains UI design changes that could be considered. |
| 4      | Interoperability and Flight Logs | For interoperability between DSPs, the following link be used as reference: https://github.com/gutma-org/flight-declaration-protocol/blob/master/FlightDeclarationProtocol.md  
For flight logs, the following link be used as reference: https://github.com/gutma-org/flight-logging-protocol/blob/master/Flight_logging_protocol.md |

The list of resources shared above can support various aspects of the envisaged Digital Sky platform. The details of the same are as below:

<table>
<thead>
<tr>
<th>Story Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td></td>
</tr>
<tr>
<td>DS-0001</td>
<td>Initial Setup GitRepo, Trello Board</td>
</tr>
<tr>
<td>DS-0002</td>
<td>Ability to Register with basic details</td>
</tr>
<tr>
<td>DS-0003</td>
<td>Setup CI Server</td>
</tr>
<tr>
<td>DS-0004</td>
<td>Ability to login with basic credentials</td>
</tr>
<tr>
<td>DS-0005</td>
<td>Ability to reset and change password</td>
</tr>
</tbody>
</table>
# Appendix 1 – Tender for Development, Hosting and Maintenance of Digital Sky Platform

<table>
<thead>
<tr>
<th>Story Number Phase 1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS-0006</td>
<td>Secure all rest API's with JWT based authentication</td>
</tr>
<tr>
<td>DS-0007</td>
<td>Ability to Signup as Manufacturer/Operator/Pilot</td>
</tr>
<tr>
<td>DS-0008</td>
<td>Ability for user to build their profile as Individual/Organization with basic details like phone, email, fax, address and directors etc based on their role</td>
</tr>
<tr>
<td>DS-0009</td>
<td>Ability to apply for drone import license as an operator</td>
</tr>
<tr>
<td>DS-0010</td>
<td>Ability to apply for permission to acquire drones locally as an operator</td>
</tr>
<tr>
<td>DS-0011</td>
<td>Ability to apply for UAOP permit as an operator</td>
</tr>
<tr>
<td>DS-0012</td>
<td>Ability to apply for UIN for drones as an operator</td>
</tr>
<tr>
<td>DS-0013</td>
<td>Ability to log incident report as operator</td>
</tr>
<tr>
<td>DS-0019</td>
<td>Ability to associate a pilot with an operator</td>
</tr>
<tr>
<td>DS-0020</td>
<td>Ability to add drone type along with manufacturer information to system as admin</td>
</tr>
<tr>
<td>DS-0022</td>
<td>Ability to approve any application as admin with audit trail</td>
</tr>
<tr>
<td>DS-0025</td>
<td>Automate Deployment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Story Number Phase 2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS-1006</td>
<td>Configure digital sky frontend app to work with react-map-gl/react-open layers</td>
</tr>
<tr>
<td>DS-1007</td>
<td>Expose API's to Add airspace category i.e consume airspace zone (green, red, amber in polygons) coordinates provided in a excel format and parse them into lat-long coordinates and save</td>
</tr>
<tr>
<td>DS-1008</td>
<td>Plot airspace zones by using latitude longitude coordinates. Airspace zones will only be plotted after certain zoom level</td>
</tr>
<tr>
<td>DS-1009</td>
<td>Allow pilot/user to open permission application and select region on map (Polygon region) for which he is seeking permission to fly drones. Altitude will be captured as a number in regular html input</td>
</tr>
</tbody>
</table>
| DS-1010              | System should be able to detect airspace zone (red/green/amber) for region specified in application and then - 3 days  
  if Green Zone - Accept Application and generate Artefact, 
  if Red Zone - Reject Application 
  if Amber Zone - Send for approval |
| DS-1011              | Allow pilot/user to List and view his applications |
| DS-1012              | Allow pilot/user to download permission artefact once application is approved |
| DS-1013              | Allow admin to list all the permission applications sorted by application status and date |
| DS-1014              | Allow admin to review specific permission application with map |
| DS-1015              | Allow admin to approve or reject application with reason. System should maintain audit trail of approval |
| DS-1016              | Registration/Deregistration API for Devices (JSON API's) API Only |
| DS-1017              | Registration for Manufacturers |
| DS-1018              | Operator Drone Linkage by Manufacturers. API Only |
| DS-1019              | Pilot and Operator Linking |
Digital Sky
Technology Standard - Registered Flight Module
Table of Contents

1. Introduction 3
   1.1 Mission 3
   1.2 Vision 3
   1.3 Target Audience and Prerequisites 3
   1.4 Guiding Design Principles 4
      1.4.1 Universal Identity 4
      1.4.2 User-Centric 4
      1.4.3 Granular Control and Digital Enforceability 4
      1.4.4 Open Platform and Open Standards Based 4
      1.4.5 Security by Design 4
      1.4.6 Privacy by Design 4
      1.4.7 Ecosystem Driven Approach 4
      1.4.8 Trustable and IT Act Compliant 4
      1.4.9 Minimalist and Evolutionary Design 5

2. Registered Flight Modules 6
   2.1 Registered Flight Module (RFM) 6

3. Registration 6
   3.1 Registration of Flight Module 7
      3.1.1 Functionality of Flight Module Management Client 8
      3.1.2 Functionality of Flight Module Management Server 9
      3.1.3 Digital Sky APIs for Registration and Deregistration 9
      3.1.4 Certificates and Keys Policies 10
      3.1.5 Keystore Security 11
   3.2 Issuance of UIN 12

4. Registered Flight Module (RFM) APIs 13
   4.1 RFM Core Functionality 13
      4.1.1 UAS Identification (Internal ID) 13
      4.1.2 Verifying authenticity of the Permission Artefact 13
      4.1.3 Provide information of Time and Location bound restrictions to Flight Controller 15
      4.1.4 Collect Flight Logs 15
      4.1.5 Sending Flight Logs to Digital Sky Service Provider 15
   4.2 RFM API Reference 16

5. Test Structure for Certification 22

6. Definition of Terms 23

7. Appendix 24
   7.1 General Safety Guidelines 24
   7.2 Registry of Certified Registered Flight Modules 24
   7.3 Registry of Digital Sky Service Providers 24
1. Introduction

Imagine a future where Unmanned Aircraft Systems (UAS) augment human capabilities. They could help farmers prioritize where to apply fertilizer, or help energy companies monitor their infrastructure, or even enable emergency response teams to quickly map the extent of damage after natural disasters. In the near future, UAS could deliver packages, streamline agriculture management, reinvent human mobility, and even save lives. Therefore, Digital Sky puts in place a seamless and secure technology and regulatory framework to integrate this new technology into the Indian airspace.

Digital Sky enables a proactive approach to enforcement of safety and security guidelines by ensuring that a UAS does not take-off without a signed digital permission from Digital Sky and necessary flight logs and occurrence reports are reported back to Digital Sky.

We envision a future, when millions of UAVs are flying across the country, without significantly increasing the regulatory burden. Thus, Digital Sky can be extended in the future to carry out autonomous flights, automated UAV traffic control, air taxis, besides other use-cases.

1.1 Mission

The mission of Digital Sky is to create a completely digital, paperless, and presence less process, thus fast-forwarding to a future of on-demand seamless permissions for UAS/RPAS, operators, and pilots.

1.2 Vision

The vision is to create a digital infrastructure that will support safe, efficient, and secure access to Indian airspace for millions of UAS.

1.3 Target Audience and Prerequisites

This is a technical document and is targeted primarily at UAS/RPAS manufacturers or providers who want to build registered flight modules as per this specification.

In this document, the term “Flight Module Provider” is used to refer to a UAS/RPAS manufacturer or any agency who has partnership with the manufacturer to manage certification and related software/security aspects of registered flight modules:

- One provider may have many UAS makes/models
- One provider may have many versions of the RFM
- One RFM service may handle many models

The Flight Module Provider should be an entity registered in India and is responsible for certification, key management (as per this specification), and any security or other responsibilities set forth by DGCA.
1.4 Guiding Design Principles

1.4.1 Universal Identity
The technical framework should leverage universal, authenticable, non-repudiable, and digital identities to allow interoperability across all actors (pilot, manufacturer, operator, drone, etc.) in the system.

1.4.2 User-Centric
The framework should be designed by placing the user in the center, thus only adopting approaches that are convenient and easy for doing business.

1.4.3 Granular Control and Digital Enforceability
The framework should allow users to set permissions and rights for permission access at a granular level and the same must be enforced digitally, thus generating verifiable audit trails.

1.4.4 Open Platform and Open Standards Based
The framework should use open technology and legal standards available in the country. It should be agnostic to applications, programming languages, and platforms.

1.4.5 Security by Design
The software and systems must be designed from the ground up to be secure. There must be end-to-end security of data using PKI, DSC, tamper detection, and other security measures.

1.4.6 Privacy by Design
The following privacy principles must be embedded into the design:
- Proactive not reactive; Preventative not remedial
- Privacy as the default setting
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

1.4.7 Ecosystem Driven Approach
An ecosystem approach is necessitated such that the interfaces between the partners and systems are well defined and standardized. Hence, there must exist a technology backbone that would hold together this partner ecosystem.

1.4.8 Trustable and IT Act Compliant
The framework must use digital signatures to guarantee integrity of access permissions given by users in permission flows. This avoids security issues faced by existing approaches and also makes the framework fully legal under the IT Act.
1.4.9 Minimalist and Evolutionary Design
The design of the framework should be simple and minimalistic. It should not present adoption barriers for the ecosystem. The design of the systems should be evolutionarily - their capabilities should be built incrementally while allowing for rapid adoption.
2. Registered Flight Modules

2.1 Registered Flight Module (RFM)
Registered Flight Modules specification described in this document provides the following key features:

1. Non Repudiable Identification of UAS – every Flight Module has a unique identifier allowing end to end traceability, accountability, traffic management, and forms the foundation for issuance of UIN.
2. No Permission No Takeoff (NPNT) - every UAS must obtain a valid permissions artefact and verify the same before it can arm itself.
3. Eliminating use of synthetic flight logs - there should be no mechanism for any external system to provide simulated flight logs and get it signed.

It is important to note that it is in Flight Module Provider’s interest to ensure the above items are implemented securely since any compromise on these will result in fraudulent activities signed using the Flight Module Provider key. As per IT Act it is essential for the key owners (Flight Module Provider) to protect the signature key and take responsibility for any compromise.

Exhibit A: High-Level Overview

DGCA does not mandate any specific hardware design and Flight Module Providers are expected to innovate appropriate form factors for market use.
3. Registration

3.1 Registration of Flight Module

Prior to registration of a flight module, the Flight Module Provider must:

1. Register with Digital Sky and provide the list of certified models.
2. Procure a digital certificate from a valid CA\(^1\) in India and get it signed by DGCA. This would be the Flight Module Provider key and it’s then used to sign the flight module public key. Flight Module Providers can have one or more keys and can rotate, revoke their keys via Digital Sky.

For registration of each flight module, the Flight Module Provider must provide for a Flight Module Management Client and Flight Module Management Server.

---

\(^1\) [http://www.cca.gov.in/cca/?q=licensed_ca.html](http://www.cca.gov.in/cca/?q=licensed_ca.html)
### 3.1.1 Functionality of Flight Module Management Client

1. Management client may or may not be packaged with RFM Service as an installable.
2. Management client should implement an "init" method internally to check if flight module is registered, connect to management server, initialize and rotate keys, and check for software upgrades.
3. When running, management client should detect for physical flight module connected and readiness of it.
4. If flight module is not registered, it should auto initiate registration.
   a. Management client should authenticate the flight module to ensure it belongs to the Flight Module Provider using combinations of serial numbers, internal identifiers, signatures, etc. The Internal ID that is used to recognize the physical flight module (such as serial number) should be read automatically without any user input. Flight Module Providers must ensure that this Internal ID does not change during the life of that physical flight module.
   b. In addition, to avoid invalid/non-genuine flight modules being registered, a concept of "activation code" could be used to authentication if the flight module is genuine.
      i. Flight Module Providers can send activation codes to people/entities who procure the flight module.
      ii. This provides a mechanism to do out of band authentication.
      iii. Once it is activated, optionally user registration can be done and user authentication may be used for all management services in addition to client software authentication.
   c. Registration should include Internal ID (serial number or any other internal ID that is used to recognize physical flight module), host fingerprint, timestamp, flight module keys, and other flight module details for authentication, etc.
   d. Flight Module Provider may keep additional attributes/info for their own management and audit purposes.
   e. Flight Module Provider should check pre-existence of serial number or other physical unique attributes to ensure same flight module gets same flight module code UUID. In the case of new registration, server generates a new flight module code (UUID) and should send back to client.
   f. Flight Module Provider backend should call Digital Sky Register API to ensure flight module is registered with Digital Sky.
   g. After successful registration with Digital Sky, Flight Module Provider backend should sign the flight module public key and return to client.
5. If flight module is registered, it should initiate key rotation when necessary.
   a. Management service should trigger key rotation under 2 scenarios:
      i. based on the trigger from management server during "init" (ideally done at least once a day);
      ii. based on the manual trigger from management client UI (this is needed only in special conditions where manual key reset needs to be triggered). This trigger should call same "init" to re-initialize.
   b. When key needs to be rotated, flight module should generate new key pair, send public key to server for signing and updating management server registry.
3.1.2 Functionality of Flight Module Management Server

1. All management server communication must be via HTTPS.
2. Management server should authenticate management clients and allow registration, key rotation, triggering upgrades, and other necessary management services. See previous section for details.
3. Management server should use a Hardware Security Module (HSM) for key management.
4. Flight Module database, secret token for authenticating management client, flight module fingerprint, user credentials, etc. should be protected through controlled access, encryption, or other security best practices.
5. Appropriate security mechanisms should be in place to protect HSM and flight module database access.
6. Log files should not contain any sensitive data (like private keys, secret tokens, etc.).
7. Management server should implement configurable key rotation policies and should be configurable as per DGCA policies.
8. All flight modules should either generate an asymmetric key pair within the flight module (highly recommended) or securely initialize the key pair. This would be the flight module key pair. Every physical instance of the flight module should have its own flight module key pair.
9. Flight Module public key should be signed by one of the Flight Module Provider’s keys. Provider can sign the public key either within the flight module or on provider server over a secure channel during key initialization.
10. Flight Module Provider MUST ensure each physical flight module has a unique code. Maximum length of the code is 50 characters when represented as string. To ensure flight module codes are globally unique it is necessary that Flight Module Provider uses a 128-bit UUID (represented in HEX notation).
11. Note: Flight Module public-private key generation/initialization and signing of flight module public key with Flight Module Provider key can be performed at any point of time during flight module’s lifecycle.

3.1.3 Digital Sky APIs for Registration and Deregistration

The Flight Module Provider’s "Management Server" backend should request the Digital Sky Registration API whenever a new flight module needs to be registered. The Flight Module Management frontend to management server interfaces are specific to the Flight Module Provider.

These APIs will be provided by Digital Sky and only certified Flight Module Providers will be able to request the same. This will be made possible using IP Whitelisting and validation of the digital signature and API.

Register API
APPENDIX 2 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

Request URL: https://{baseUrl}/rfc/service/register

Input

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RegisterFlightModule ver="" ts=""txn="">
  <Flight Module dpId="" dc="" mi="" idHash="" />
  <Signature />
  <!-- digital signature of the provider -->
</RegisterFlightModule>
```

Output

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RegisterFlightModuleResp ts="" txn="" code="" err="" >
  <Signature />
  <!-- digital signature of Digital Sky -->
</RegisterFlightModuleResp>
```

DeRegister API

Request URL: https://{baseUrl}/rfc/service/deregister

Input

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DeRegisterFlightModule ver="" ts="" txn="">
  <Flight Module dpId="" dc="" mi="" />/
  <Signature />
  <!-- digital signature of the provider -->
</DeRegisterFlightModule>
```

Output

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DeRegisterFlightModuleResp ts="" txn="" code="" err="" >
  <Signature />
  <!-- digital signature of Digital Sky -->
</DeRegisterFlightModuleResp>
```

3.1.4 Certificates and Keys Policies

1. Below are the currently supported algorithms for digital signing:
   a. SHA256withRSA (2048 bit key)
2. All Flight Module Provider certificates should be procured from a certification authority (CA) as per Indian IT Act. (http://www.cca.gov.in/cca/?q=licensed_ca.html)
3. All Flight Module Provider certificates should be class II or class III and X509 v3 compliant.
4. Organization attribute in the certificate’s subject SHOULD match the Flight Module Provider’s name registered with Digital Sky

3.1.5 Keystore Security

1. Keystore file should be limited with read and write rights only for the user as whom the RFM service runs and no other user accounts should have access to the file/store.

2. Keystore password has to be complex and auto generated. The following list of approaches are possible:
   a. A combination of random data, user credentials and flight module identification data-derived key using identities
   b. The logic how key is derived using these values has to be obfuscated to avoid any possible security threats.
   a. The Key derivation logic should be in a compiled native machine dependent code and cannot be an Open API.
   c. The password should be changed for every Key rotation.
   d. Use White Box Cryptography to derive the password.
   a. The password should be more than 16 characters in length and should contain small letters, capital letters and numbers
   e. A server side logic to help with opening the keystore.

3. The RFM service should fail its integrity check upon the keystore file permissions not correct or has unwanted access and should inform the server about such failures. This failure would be tracked as an incident by the Flight Module Provider.

4. All type of access and access attempts to the keystore should have audit logs.

5. The private key should not be extractable (wrapped or direct)

6. It is recommended that key pair is generated inside the flight module service. If key pairs are generated on management server, then private key must be returned and MUST BE strongly encrypted using AES-256 session key generated at the client. Note that flight module authentication must be performed before allowing any connection to management server

7. The keystore has to be cleared and zeroed in case the RFM service is deleted.

For detailed recommendations and best practices on key management, you may refer to the following global standards by NIST

3.2 Issuance of UIN

Once the flight module has been successfully registered with Digital Sky based on the process outlined in 3.1, following steps need to be completed to receive a UIN:

- Approve Operator Linkage Request (linking drone with operator)
- Fill UIN Form on Digital Sky and Submit
- If approved, then UIN is issued and flight module is added to registry.

Through Digital Sky, an end to end linkage of the Flight Module Provider, RFM/UAS, Owner, Operator, and Pilot is formed providing traceability and ensuring accountability.
4. Registered Flight Module (RFM) APIs

The RFM should be implemented at the Flight Controller Level. The UAS Manufacturer should not allow unnotified access to the UA flight controls - the RFM service should be notified of every call (pertaining to conditions specified in this RFM specification) to the UA flight controller. There should not be any bypassed or unchecked access to the UAs flight controls.

The permission artefacts and the flight logs must not be stored by the RFM. It must be stateless and must provide a tamper-proof mechanism to offload any storage and state handling to the host system.

4.1 RFM Core Functionality

4.1.1 UAS Identification (Internal ID)

1. Items to be Uniquely Identified to avoid alterations:
   a. UID of Hardware modules used like MicroProcessor/Controller, Radio Modules.
   b. Version Hash of firmware and bootloader onboard.
   c. Unique License/Identifier of manufacturer

2. Layers for Identification:
   a. Flight Application: Connected Hardware modules identification, Manufacturer License Verification
   b. Co-Computer/GCS: Manufacturer License Verification.

4.1.2 Verifying authenticity of the Permission Artefact

Permission Artefact is an electronic representation of a permission to fly granted through the Digital Sky Platform. Here’s the XML structure of the artefact:

```
<PermissionArtefact>
  <UAPermission lastUpdated="" ttl="" txlnId="" permissionartefactId="" pilotPinHash="">
    <Owner operatorID="">
      <Pilot No="" validTo=""/>
    </Owner>
    <FlightDetails>
      <UADetails uinNo="/">
        <FlightPurpose shortDesc="/" frequency="/"/>
        <PayloadDetails payLoadWeight="/" payloadDetails="/"/>
        <FlightParameters gpsCoordinates="/" flightStartTime="/" flightStartEnd="/" frequenciesUsed="/"/>
      </UADetails>
    </FlightDetails>
    <DigitalSignature/>
  </UAPermission>
</PermissionArtefact>
```

<table>
<thead>
<tr>
<th>Element/Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission Artefact</td>
<td></td>
</tr>
<tr>
<td>&lt;UAPermission</td>
<td></td>
</tr>
<tr>
<td>lastUpdated</td>
<td></td>
</tr>
<tr>
<td>ttl</td>
<td></td>
</tr>
<tr>
<td>txlnId</td>
<td></td>
</tr>
<tr>
<td>permissionartefactId</td>
<td></td>
</tr>
<tr>
<td>pilotPinHash</td>
<td></td>
</tr>
<tr>
<td>&lt;Owner operatorID</td>
<td></td>
</tr>
<tr>
<td>&lt;Pilot No</td>
<td></td>
</tr>
<tr>
<td>validTo</td>
<td></td>
</tr>
<tr>
<td>&lt;/Owner&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;FlightDetails</td>
<td></td>
</tr>
<tr>
<td>&lt;UADetails uinNo</td>
<td></td>
</tr>
<tr>
<td>&lt;FlightPurpose shortDesc</td>
<td></td>
</tr>
<tr>
<td>frequency</td>
<td></td>
</tr>
<tr>
<td>&lt;/FlightPurpose shortDesc</td>
<td></td>
</tr>
<tr>
<td>&lt;PayloadDetails payLoadWeight</td>
<td></td>
</tr>
<tr>
<td>payloadDetails</td>
<td></td>
</tr>
<tr>
<td>&lt;FlightParameters</td>
<td></td>
</tr>
<tr>
<td>gpsCoordinates</td>
<td></td>
</tr>
<tr>
<td>flightStartTime</td>
<td></td>
</tr>
<tr>
<td>flightStartEnd</td>
<td></td>
</tr>
<tr>
<td>frequenciesUsed</td>
<td></td>
</tr>
<tr>
<td>&lt;/FlightParameters</td>
<td></td>
</tr>
<tr>
<td>DigitalSignature</td>
<td></td>
</tr>
<tr>
<td>&lt;/UAPermission&gt;</td>
<td></td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UAPermissionRequest</td>
<td>Root element for the permission request</td>
</tr>
<tr>
<td>UAPermissionRequest-&gt;lastUpdated</td>
<td>Timestamp information</td>
</tr>
<tr>
<td>UAPermissionRequest-&gt;ttl</td>
<td>Time to Live value in hours suggesting the caching and invalidation rules of the message</td>
</tr>
<tr>
<td>UAPermissionRequest-&gt;permissionartefactId</td>
<td>The unique identifier for the permission artefact. This would be the reference for any re-issue or revocation</td>
</tr>
<tr>
<td>UAPermissionRequest-&gt;txnId</td>
<td>The transaction identifier generated by the DSP</td>
</tr>
<tr>
<td>UAPermissionRequest-&gt;pilotPinHash</td>
<td>The salted hashed PIN which would be verified against what the pilot enters before take off</td>
</tr>
<tr>
<td>Owner</td>
<td>Root element of the UA owner</td>
</tr>
<tr>
<td>Owner-&gt;operatorID</td>
<td>The owner's Operator ID obtained during registration</td>
</tr>
<tr>
<td>Pilot</td>
<td>Root element of the UA pilot</td>
</tr>
<tr>
<td>Pilot-&gt;No</td>
<td>The Pilot Registration Number</td>
</tr>
<tr>
<td>Pilot-&gt;validTo</td>
<td>Expiry Date of the Pilot Registration</td>
</tr>
<tr>
<td>FlightDetails</td>
<td>Root element of the UA flight details</td>
</tr>
<tr>
<td>FlightDetails-&gt;UADetails-&gt;uinNo</td>
<td>The UIN of the UA for which the flight permissions are being requested</td>
</tr>
<tr>
<td>FlightPurpose-&gt;shortDesc</td>
<td>A short description for the purpose of the flight</td>
</tr>
<tr>
<td>FlightPurpose-&gt;frequency</td>
<td>Number of flights for the given flight parameters</td>
</tr>
<tr>
<td>Payload-&gt;payLoadWeight</td>
<td>The weight of the payload carried by the UA</td>
</tr>
<tr>
<td>Payload-&gt;payloadDetails</td>
<td>Any other details that can be furnished about the payload carried by the UA.</td>
</tr>
<tr>
<td>FlightParameters</td>
<td>The root element of for all details about the UA’s flight plan</td>
</tr>
<tr>
<td>FlightParameters-&gt;gpsCoordinates</td>
<td>The broad GPS coordinates (boundary) of the UA flight represented as a polygon of points</td>
</tr>
<tr>
<td>FlightParameters-&gt;flightStartTime</td>
<td>The start time and date of the planned UA flight</td>
</tr>
<tr>
<td>FlightParameters-&gt;flightStartEnd</td>
<td>The end time and date of the planned UA flight</td>
</tr>
<tr>
<td>FlightParameters-&gt;frequenciesUsed</td>
<td>The planned frequencies to be used by the UA</td>
</tr>
<tr>
<td>DigitalSignature</td>
<td>The element containing the cryptographically verifiable signature of the applicant</td>
</tr>
</tbody>
</table>
The permission artefacts will come with a digital signature (a form of Public key cryptography), encrypted using Digital Sky private encryption key. The RFM service must use the corresponding public keys (released by Digital Sky) to verify that the permission artefact is released by Digital Sky and has not been tampered with during transport. If the public key has to be changed (When Digital sky requests the manufacturers to change), the manufacturer has to release a firmware update to update the key. Manufacturer should build security measures to ensure that any 3rd party is not able to alter the public keys used to verify the permission artefact in the library.

4.1.3 Provide information of Time and Location bound restrictions to Flight Controller

The verified permission artefact will provide geofence information in horizontal and vertical plane to the Flight Controller. The permission artefact also consists of the time period for which the permission is valid.

4.1.4 Collect Flight Logs

The manufacturer is required to implement functionality to provide following data to the RFM service. This data will be saved against each permission artefact.

I. Date-time information from GPS data
II. Date-time information from system in case GPS fixture is unavailable.
III. System clock timestamp
IV. For each power cycle, the list of takeoff, land coordinates.
V. Upon breach of the geofence, the start/stop timestamp, a list of GPS coordinates during the time the drone was outside the geofence, captured at 1 Hz minimum.
VI. Upon breach of the time limits, the additional time, and list of start/end timestamp for which the UAS was in air should be provided to the library.
VII. The flight logs captured during the period of the permission artefact should be stored on the flight controller along with hash of the logs to ensure tamper-proof records. A record must be maintained onboard to connect next and previous flight logs to avoid omission and the same should be inaccessible to the user. Once the permission artefact is expired or when user wants to submit logs, the complete bundle of such logs should be signed using RFM private key and submitted to the DSP.

4.1.5 Sending Flight Logs to Digital Sky Service Provider

The Manufacturer is responsible for providing the communication interface between RFM and DSPs or external applications, which can ultimately interact with DSPs. Since, third party applications can provide the functionality for sharing permission artefact and flight log data between Digital Sky servers and RFM, it is suggested to provide a standardized communication interface to the external applications to interact with RFM’s permission artefact and Flight Log APIs. Finally, the manufacturer is responsible for providing to user, at least one way of sharing
this data, either over a direct link between RFM and Digital Sky Servers or through an external application (e.g. Ground Control Station).

### 4.2 RFM API Reference

1. **Get_rfmInfo**
   
   Parameter 1: UTC date-time (fetched from GPS data or any other source)
   
   Output 1: RFM public key
   
   Output 2: Manufacturer Public key being used in RFM
   
   Output 3: Digital Sky Public Key being used in RFM
   
   Output 4: Firmware Version
   
   Output 5: RFM version
   
   Output 6: UAS category
   
   Output 7: Operator ID obtained during registration
   
   [Provide UAS info]
   
   a. The API will return the required information for any external application.

2. **Apply Permission Artefact:**
   
   Parameter 1: Permission_artefact
   
   Parameter 2: UTC date-time (fetched from GPS data or any other source)
   
   [provide permission artefact to the RFM]
   
   a. This API should be called by Flight Controller or host system every time the UAS is powered on.
   
   b. RFM will verify the signed permission artefact using the Digital Sky Public Key.
   
   c. RFM, being stateless, will not store the permission artefacts in the memory, so manufacturer is responsible for providing relevant permission artefact to the RFM on every power cycle. The permission state is maintained by the RFM for the current power session only.
   
   d. RFM will use timestamp provided by manufacturer, the artefact publish timestamp (marked by Digital Sky server when the artefact is created), and the ttl (time to live) value to validate that the artefact is eligible at that time and that the system time-date is not falsified.

3. **Get_Geofence_restriction:**
   
   Parameter 1: UTC date-time
   
   [provides geofence information to the Flight Controller or Host system after a valid permission artefact has been applied]
   
   a. RFM will verify the date-time stamp to reassert the time validity of the permission artefact
   
   b. This API is provided by RFM for the Flight Controller or Host system. The Flight Controller is expected to use this data for enforcing safety restrictions or warning the pilot.
   
   c. It is responsibility of manufacturer to ensure that the UAS follows the geofence restrictions. In case of geofence or time limit violations, the manufacturer should provide the event details to the RFM.
4. Get_time_restriction:
   Parameter 1: UTC date-time
   [ Provides allowed time limit after a valid permission artefact has been applied ]
   a. RFM will verify the date-time stamp to reassert the time validity of the permission artefact.
   b. It is responsibility of manufacturer to ensure that the UAS is landed before the permitted time period expires. In case of time limit violations, the manufacturer should provide the event details to the RFM

5. Verify_pilot_pin:
   Parameter 1: Input Pin
   Parameter 2: UTC date-time
   Output 1: Pin verified (Boolean)
   [Verify that the pilot pin matches to that provided in permission artefact]
   a. Verify if the salted hashed PIN provided in the permission artefact matches with the pin provided as input parameter.
   b. Manufacturer is responsible to implement the functionality to ensure that this API is called before a takeoff event and if the response is False then takeoff is rejected.
   c. This should be verified only once in a power cycle.

6. Log_takeoff_location:
   Parameter 1: UTC date-time
   Parameter 2: GPS coordinates
   [To provide takeoff event information to library for internal logging.]
   a. The manufacturer is responsible to implement the functionality to ensure that this API is called immediately after takeoff event.
   b. The manufacturer should not provide any means to bypass the notification to RFM on a takeoff event.
   c. The RFM will store and package all such events in one flight log against a permission artefact.

7. Log_Land_location:
   Parameter 1: UTC date-time
   Parameter 2: GPS coordinates
   [To provide land event information to RFM for internal logging.]
   a. The manufacturer is responsible to implement the functionality to ensure that this API is called immediately after land event.
   b. The manufacturer should not provide any means to bypass the notification to RFM on a land event.
   c. The RFM will store and package all such events in one flight log against a permission artefact.

8. Log_geofence_breach:
   Parameter 1: UTC date-time
   Parameter 2: Breach_start_timestamp
   Parameter 3: Breach_stop_timestamp
   Parameter 2: GPS coordinates
   [To provide geofence breach event information to RFM for internal logging.]
a. The manufacturer is responsible to implement the functionality to ensure that this API is called immediately after a geofence breach incidence.

b. The manufacturer is responsible for implementing functionality to call this API at 1 Hz, from the time when Geofence is breached to when the drone lands.

c. The RFM will store and package all such events in one flight log against a permission artefact.

9. Log_timelimit_breach:
   Parameter1: UTC date-time
   Parameter2: time_overrun_start_timestamp
   Parameter3: time_overrun_land_timestamp
   [ To provide time limit breach event information to RFM for internal logging.]
   a. The manufacturer is responsible to implement the functionality to ensure that this API is called immediately for a time limit overrun event.
   b. During the first call, when the drone is still in flight, the time_overrun_timestamp parameter will not have any value. The event would be logged as start of time overrun.
   c. When the drone lands this API should be called again to indicate end of flight. In this case the API caller needs to provide time_overrun_start_timestamp again. This event will be registered as end of time-overrun event.
   d. The RFM will store and package all such events in flight log against a permission artefact.

10. Get_individual_flight_logs:
    Parameter1: UTC date-time
    [ To get the individual flight logs from the RFM for storage ]
    a. The RFM must prepare a flight log after each land and Geofence breach event.
    b. These flight logs will be digitally signed by the RFM to make sure that flight logs are not tampered with during the transport. It is manufacturer's responsibility to implement the functionality required to keep the private key secure. Also, manufacturer has to share the public key with Digital Sky Server where it will be used to verify the authenticity of the reports.
    c. It is responsibility of the Manufacturer to implement the functionality to collect these reports immediately after every takeoff, land, Geofence and time-limit breach event from RFM. In case of crash where such events were not registered, the RFM on next power cycle, should close the log with failed landing incidence.
    d. The manufacturer is responsible to implement the functionality to store all the flight logs captured during the period of last 10 permission artefacts in a non-volatile memory storage. This storage should provide the ‘write access’ only to the applications authorized by manufacturer. The read access to the storage should be available in case of accidents. The manufacturer is required to provide the authorities with the specialized equipment required to read the flight logs from a crashed/damaged UAS’s onboard storage.

11. Bundle_flight_logs:
    Parameter1: UTC time-stamp
    Parameter2: List_of_individual_incidence_reports_from_storage
    Parameter3: Permission Artefact
[ to bundle the signed flight logs from storage into a single bundle (a bundle per permission artefact). ]

a. After the time-period of a permission artefact is over, the user has to submit the flight logs to Digital Sky APIs within 3 days. The manufacturer is required to implement the functionality to provide all the flight logs associated with a particular permission artefact and pass them on to this API to get in return a signed bundle.

b. Manufacturer is responsible to provide communication interface to upload this bundle directly to Digital Sky servers or through external applications, such as Ground Control Station.

### JSON Schema for Flight Log


```json
{}

"$id": "http://dgca.gov.in/schema/incident_report_field.json",
"type": "object",
"properties": {
  "PermissionArtefact": {
    "$id": "/properties/PermissionArtefact",
    "type": "string",
    "format": "base64"
  }
}

"FlightLog": {
  "$id": "/properties/FlightLog",
  "type": "array",
  "items": {
    "$id": "/properties/FlightLog/items",
    "type": "object",
    "properties": {
      "TimeStamp": {
        "$id": "/properties/FlightLog/items/properties/TimeStamp",
        "type": "integer",
        "title": "Timestamp in MilliSeconds",
        "default": 0
      }
    }
  }
}
```
APPENDIX 2 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM
5. Test Structure for Certification

The certification of registered flight modules would involve test cases covering secure provisioning of keys, implementation of Flight Module Management Server and Client, functional tests, security tests, and other compliance related tests.

It is required by Flight Module Providers to minimize the attack surface at the system level using methods such as but not limited to protective meshing, encrypted communication, etc. In addition, it is highly recommended that tamper responsiveness be implemented for the system.

Here are a list of example test cases:

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Type of Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fake and authentic signed permission artefact test.</td>
</tr>
<tr>
<td>2</td>
<td>Individual flight log storage test (including digital signature verification)</td>
</tr>
<tr>
<td>3</td>
<td>Geofence breach flight log test</td>
</tr>
<tr>
<td>4</td>
<td>Time limit breach flight log test</td>
</tr>
<tr>
<td>5</td>
<td>Bundled flight log test (including digital signature verification)</td>
</tr>
<tr>
<td>6</td>
<td>RTH test in case of violation of permissions</td>
</tr>
<tr>
<td>7</td>
<td>Accidental storage data retrieval test with the specialized equipment</td>
</tr>
<tr>
<td>8</td>
<td>Overall no permission-no takeoff policy test</td>
</tr>
<tr>
<td>9</td>
<td>Secure Boot and Secure Upgrade</td>
</tr>
<tr>
<td>10</td>
<td>Secure Provision of Keys</td>
</tr>
<tr>
<td>11</td>
<td>System Level Tamper Responsiveness</td>
</tr>
<tr>
<td>12</td>
<td>Any other test as defined by Digital Sky or the Certification Agencies</td>
</tr>
</tbody>
</table>

There will be certification agencies that will be empaneled to certify the UAS, Registered Flight Module, etc. These agencies shall publish the detailed list of test requirements beforehand that would be necessary for certification.
6. Definition of Terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certifying Authorities</td>
</tr>
<tr>
<td>DSP</td>
<td>Digital Sky Service Provider</td>
</tr>
<tr>
<td>DGCA</td>
<td>Directorate General of Civil Aviation</td>
</tr>
<tr>
<td>UAS</td>
<td>Unmanned Aircraft System(s)</td>
</tr>
<tr>
<td>UIN</td>
<td>Unique Identification Number</td>
</tr>
<tr>
<td>RPAS</td>
<td>Remotely Piloted Aircraft System(s)</td>
</tr>
<tr>
<td>NPNT</td>
<td>No Permission No Takeoff</td>
</tr>
</tbody>
</table>
7. Appendix

7.1 General Safety Guidelines

1. Firmware Tamper Avoidance: *There is possibility to change firmware by the user so as to change the behavior of the drone which might not follow laid guidelines under which the drone was originally cleared.*
   a. Readout Protection on Microprocessor/Microcontroller for onboard firmware to avoid Copying of onboard keys and other sensitive information.
   b. Ensure keys are erased from memory during firmware update operation.
   c. Have authentication procedure to change Flight Parameters or have some parameters hidden or immutable unless manufacturer supplies it post verification.

2. Hardware Tamper Avoidance: *There can be a possibility of changes to the onboard hardware like replacing Flight Controller or GPS module, which might again lead to deviation from guidelines.*
   a. Secure Unique Identification of crucial hardware like Radio Modules, GPS and Flight Controller might be able to avoid this.

3. Spoof Avoidance: *Ensure that the Flight Controller can’t be run as hardware in the software loop by connecting over provided external interfaces, a feature available by default in many flight control software.*

4. Link Hijack Avoidance

5. Drone System Failure Actions: In cases of hardware or software failure, the drone system must have excessive audio visual notifications to raise alarm. Failures to Test for:
   a. GPS Failure.
   b. Sensor Failure.
   c. Inability to hold altitude due to one or more onboard hardware failures.
   d. Battery Failure, if there is a power cut-off for any reason, the notification system be given isolated power for raising alarm.

7.2 Registry of Certified Registered Flight Modules
The list of certified RFMs will be made available via a registry for third party applications to consume. These applications are expected to check with this registry during RFM service installation (if applications are managing these) and usage. There shall also be a registry for pre-certified RFM services.

7.3 Registry of Digital Sky Service Providers
DGCA shall make available a machine readable list of all certified DSPs
Appendix 3 - Digital Sky Detailed Process Flow

Digital Sky comprises of the following 3 key distinguished category of activities namely:

1. **Pre Flight**: Related to permits (organizations/manufacturers), license issuance (pilots), registration (drones), categorization of Airspace on Digital Maps (no-fly zone, free zone, semi restricted, etc.)

2. **Take Off**: Related to flight permits; includes considerations to airspace availability, digital approval certificate (to be uploaded into the drones for take-off, geo-fencing)

3. **Post Flight**: Actual Flight Path Data Analysis, Data Analytics on Potential Threats/Safety Issues, Non-Compliance Checks, Enforcements, AI based Data Authenticity Validation, etc.

**HOW DIGITAL SKY WILL WORK**

**Pre-Flight**
Manufacturers UIN issuance, Online Registration of Operators/Pilots

**Take-Off**
App-based permit request, UAV verifies Permission Artefact

**Post-Flight**
Logging of Flight Plans with DGCA, Incident Reporting

---

**Fully automated process from registration to tracking**

Layer 1
Online Registrations

Layer 2
Automated Permissions: No Permission No Takeoff

Layer 3
Analytics, Tracking & Configurable Policies (ATC)

Complemented by Anti-Drone Technology for highly sensitive areas
Further, it is envisaged that the platform enables “Digital Sky Service Providers (DSP)” to provide for maximum services through their own portal/app, while at back end interacting with Digital Sky Platform for all compliance requirements. Hence, it is required that the platform design should enable services to be routed through DSP wherever possible in secured manner. Such provisioning is in addition to the user interfacing to be provided by Digital Sky platform (portal/mobile app). Refer integration section of Solution Appendix for envisaged (illustrative) architecture diagram.

The following section provides illustrative detailed process requirements within each of the above the defined categories. It is to be noted that while the process flow is comprehensive in its explanation, there may be changes that may be required during the planning stages. For the same, a detailed discussion with DGCA is required to be undertaken by the MSP.

1. **Process and Services in Pre Flight Module**

The following section provides brief process flow for services to be included in the Pre-Flight Module

1.1 **Registration at Digital Sky of Stakeholders**

The following are the envisaged stakeholders for Digital Sky:

1. Drones Operators
2. Pilots
3. DGCA
4. AAI
5. Training Organizations
6. Other Government Agencies

For the purpose of ease of registration, each of the persona type indicated above shall have a template of registration. For purpose of ease of registration, Digital Sky shall be integrated with the upcoming eGCA portal (e-Governance of Civil Aviation, an e-governance initiative by DGCA) to ensure that all persona type register with eGCA shall have their data automatically synced with Digital Sky to avoid duplicity of information
provisioning.

Further, it is required that all other relevant data for undertaking background checks be sourced from eGCA (such as enforcement history on pilot, accident/incidents by the entity, compliance/risk scorecard, etc). It is also required that Digital Sky support cell support in evaluating the application by undertaking basic factual checks on documents submitted by applicant before passing on the application to AAI/DGCA officer for acceptance of registration (if required).

Based on the above process, it is require that Digital Sky Unique ID be created for organization, individuals. Further, it may be decided that in case eGCA ID exists of an entity, individuals, a separate Digital Sky ID may not be used and the eGCA ID be treated as Digital Sky ID.

It is required that vendor develop all such forms in consultation with DGCA/AAI both for first time registration and for stakeholders that already exist in eGCA records. It is to be noted that such information gathering should also include details that is required for smooth functioning and delivering of services through eGCA for each stakeholder.

1.2 Pilot License Issuance/Renewal/Endorsement

For the purpose of pilot license issuance, renewal and endorsements, a pilot is required to comply with requirements as per Civil Aviation Rules as published by DGCA. Currently such rules are under draft stage and shall be finalized soon. However, for purpose of process comparison, MSP is encouraged to refer to pilot licensing process for DGCA website. It is expected that the process shall be similar to that.

Since, the project is a long duration project and DGCA is at its infancy of rules and regulation design related to Drones, MSP is required to provision for process change w.r.t. the following areas:
- Integration with Central Examination Organization (CEO) of DGCA
- Renewal Process
- Endorsements based rules for various kinds of Drones

Such provisioning is to be considered part of scope of work.

**Broadly, the process flow for the pilot licensing issuance/renewal/endorsements will be the following**

- **Step 1:** Applicant logs in to Digital Sky and registers basic details
- **Step 2:** Applicant provides details for license issuance/renewal/endorsement request
- **Step 3:** Applicant provides details of credentials and uploads documents (training certificates/current license, etc)
- **Step 4:** Application submitted on Digital Sky
- **Step 5:** DGCA reviews application
- **Step 6:** DGCA issues digital license along with details such as validity, endorsements, etc.
1.3 Manufacturers

In order to streamline the process for approvals for manufacturers, there are three levels of approvals that is envisaged overall:

1.3.1 Approval of Type Certification for UAV in India

For the same, each manufacturer will be required to obtain approval for the Type of Drones that is planned to be manufactured. For the same, it is required that every drone type be provided with a certificate of airworthiness issued. The issuance valid of a certificate of airworthiness will be based on satisfactory evidence that the drones complies with the design aspects of the appropriate airworthiness requirements (i.e. the airworthiness standards).

Hence, forth, for each type acceptance, of the manufacturer complies with defined basic guidelines as per approval, the manufacturer can manufacture drones on the type accepted by AAI/DGCA. Further, in case of changes undertaken in design etc. special approvals will be required to be undertaken such as Approval for Modification/Design Acceptance

Step 1: Applicant submits the application in the specified application form along with all the required details such as specifications, operating guidelines, maintenance schedule etc.

Step 2: The application will be reviewed and clarifications (if any) can be requested by the applicant

Step 3: After the application is found satisfactory, the applicant will be required to initiate the process for obtaining UIN for the prototype and approval for test flight schedule

Step 4: After satisfactory results from the test flight/inspection and review of all the documents, the approval will be granted.

Note: The accepted drone types will be updated in the system, and while applicants apply for a UIN, the accepted UAV model types will be available in a drop down and the details available in the system will be prepopulated.

1.3.2 Approval for Modification to approved UAV types

This service can be availed for UAVs which have already been type accepted

Step 1: Applicant submits the application in the specified application form along with all the required details on elements that are sought to be modified such as specifications, operating guidelines, maintenance schedule etc.

Step 2: The application will be reviewed and clarifications (if any) can be requested by the applicant. In case the modifications are significant, test flight/inspection may also be required.

Step 3: In case a test flight is required, the applicant will be required to initiate the process for UIN of the modified UAV and approval for test flight schedule.

Step 4: After the results from test flight (if required) and the documentation review are found to be satisfactory, the approval will be granted.

Note: The modification number will be appended to the model type to distinguish the modified versions of the UAVs from the initially approved models.
1.3.1 Registration of Drones Manufacturer ID
For each drone manufactured, a unique ID is created by the manufacturer which is required to be registered at Digital Sky platform. Please refer Digital Sky - Technology Standards Appendix

1.4 Operators/Owners
1.4.1 Issuance of Permit
The purpose of Drones permit is to certify that specified operator is authorized by DGCA to undertake Drones related activities. The DGCA will be issuing permits in two parts, the permit itself and the associated operations specifications that specifies the nature and scope of operations authorized together with relevant conditions and limitations. The DGCA is authorized to suspend or cancel an permit, if one or more of the conditions stipulated is breached or not maintained to the same level as demonstrated at the initial certification. Prior to issuing an permit, the DGCA needs to be satisfied that the operator conforms to all the requirements of relevant rules, requirements and associated guidance published by the DGCA.

For the purpose of certification, the following process is to be followed:

1. Prospective operator provides required details as per requirement of CAR including security clearances, etc.
2. Digital Sky Platform validates the information provided (of what is digitally possible)
3. DGCA officer validates the information provided by the operator and checks for all compliance requirements including documents
4. DGCA approves the permit and an Operator Permit number is generated for the operator
5. The details of the same is automatically shared with required external government agencies

1.4.1 Issuance of UIN
The operator will be required to obtain a UIN for each UAV before any flights can be undertaken. The process for the same is as below:

Step 1: Apply for UIN for a Type of Drone based on the digital key provided by the manufacturer
Step 2: UIN for the type issued in serial number as per standards defined by DGCA/AAI
Step 3: Allocation and imbedding of UIN within each drone by manufacturer/operator. It is to be noted that manufacture will be providing for methodology of embedding unique numbers to each drones through their own applications

Please refer Digital Sky - Technology Standards Appendix for details

1.4.2 Endorsement of Drones UIN on Permit
Endorsement of Drones is undertaken to associate a Drone with an Operator. For the same, an Operator is required to undertake an application wherein, they indicate UIN number of a Drone to be endorsed on the Permit.

1.4.3 Import / Transfer Clearance
Refer CAR D3X-X1 for details of the requirements. The process for the same shall be enabled accordingly.
1.5 Registration of Digital Sky Service Providers
A module is required to be developed for the registration of DSPs. The rules for the same shall be shared by MSP by AAI during the project planning.

1.6 Digital Sky – Airspace Management Module
For the purpose of demarcating airspace rights and policies, it is required that a module be designed wherein, static/dynamic marking of airspace with respect to No-Fly Zone, Restricted, Free Zone, etc. can be undertaken. Further, it is required that multiple other parameters such as population, terrain, etc. can be marked. Based on such marking and business rules defined, specific permissions can be given automatically. It is to be noted that there should be layered approach for static/dynamic inputs for each kind of parameter defined. Below provides illustrative details of some of the parameters/functional requirements envisaged. Such airspace may be routinely updated based on requirements.

- Pre-loaded maps of the country’s airspace with provision to search, select and perform functions on geographical areas.
- Population of maps with information such as population density, terrain, landmarks etc. based on discussion with DGCA.
- Automatic population from external sources such as Met department for information on sunrise, sunset, visibility, wind speed, rain etc. for application of business rules.
- Provision for real time updation to fence airspace using coordinates and altitude.
- Provision to mark coordinates along with altitude to select airspace in the following or more categories:
  - Restricted
  - Semi Restricted
  - Unrestricted
  - Other categories which may be defined during SRS phase.
- Demarcation of airspace for specific purposes such as Emergency landing, Return to Home option etc.
- Demarcation of airspace with respect to tolerance for deviation from the approved flight paths.
- Mapping airspace with the type of UAVs such as Nano, Micro, Mini etc. which can be operated in the airspace.
- Mapping of airspace with access rights for different types of applicants. For examples, government bodies may be provided with elevated rights in restricted or semi restricted airspace.
• Real time view of activity in the airspace based on the approved flight schedules with option to view airspace on historical/future basis w.r.t. the accepted flight schedules; View of the historical activity in the airspace on the basis of submission of data on completed flights. This can also be used for limiting approvals in case of congestion in airspace/safety considerations.
• Maps should be configurable to allow/restrict routes on the basis of starting and end points in specific areas. Applicants may be able to select different flight paths on the basis of start and end points.
• Ability to enforce various conditions described above or similar conditions on the airspace for specified duration or indefinitely
• Rules based marking. Example, No Fly Zone on certain dates and Time

For the process of marking zones and information on the maps, the following is envisaged as a process:

Step 1: DGCA/AAI provide rights to various agencies and individuals to mark information on maps. The categories for selection will be based on the above parameters defined.

Step 2: Based on the rights provided, the map module will be made accessible to rights holders for marking the regions, rules etc. on the map

Step 3: Based on provided data, DGCA will be required to accept the same. Post acceptance by DGCA, the marked areas will be automatically defined as business rules for approval process.

2. Process and Services in Take-off Module

2.1 Flight Approval Application process

For the purpose of flight approval, each flight to be undertaken by the operators/pilots shall be required to be approved by DGCA/AAI through Digital Sky application. For the same, the following steps shall be followed:

Step 1: Applicant provides basic inputs such as UIN of Drone, Name of Pilot, Planned date of flight, Activity to be undertaken, Duration expected, etc.

Step 2: Based on data provided and backend checks on validity, the applicant is taken to Map module to provide and select details of flight path. Refer Map Module Functional Requirements for details of module capability in undertaking such selection

Step 3: Based on input data, summary of application is shown to applicant for final review

Step 4: Submission of application

It is to be noted that post submission of application email/SMS notifications are sent to applicant and application number generated.

Please refer functional requirements appendix for details.

2.2 Analytics/Process for Flight Approval

For the purpose of approval process post application submission for flight approval, the following steps are to be followed:

Step 1: Evaluation of the application in terms of business rules defined. It is to be noted that different sets of rules will be defined for “At Application Stage Filtering” and “At Evaluation Stage Filtering”.
- **At Application Stage Filters**: The rules defined in the category will be triggered based on non-compliance identified (no fly zone breach, UIN not registered, Pilot License not valid etc) at application stage only. Based on non-compliance identified at this stage will not allow applicants to submit application

- **At Evaluation Stage Filters**: Such rules triggering does not indicate non-compliance but evaluation of application manually to cross validate information before approvals being given. For example, drones flying over populated area will require additional checks to ensure safety related aspects. Hence, in case, triggers related to these rules apply to an application, intimation to designated officer shall be given for review along with rules that have been triggered.

**Step 2**: Risk Scorecard generated for each application based on Analytics.

**Step 3**: Based on defined risk, approvals either automatically generated or sent to DGCA/AAI officials for approval

**Step 4**: In case the application requires approval from DGCA/AAI, the application is forwarded to the concerned authorities.

**Step 5**: Authorities undertake necessary action (approved/rejected/clarification) on the application and thereon necessary workflow is initiated.

### 2.3 Issuance of Online Flight Approval Certificate

For the issuance of digital approval certificate, the following process is to be followed:

**Step 1**: Post approval (automated/DGCA/AAI approved), an intimation of approval is sent over SMS/Email.

**Step 2**: Acceptance initiation is sent to Operator and Pilot. Acceptance is necessary from both to authenticate the issuance.

**Step 3**: Online Digital Approval Certificate Issued.

**Step 4**: The Approval Certificate is downloaded by Applicant for uploading the same to Drones before flight undertaken

### 2.4 Flight Certificate Authentication and Flight Path Mapping

As an additional layer of security and validity of approval, it will be required that final authentication for take off is undertaken before undertaking the flight. For the same, following process shall be undertaken:

**Step 1**: Post uploading of approval certificate on drones, the drones is required to dial into the server of Digital Sky for activating the certificate

**Step 2**: Post dial in, Digital Sky application shall re-validate the authenticity and validity of approval certificate

**Step 3**: Digital Sky shall thereon provide activation code for the certificate that is auto inputted into the drones to allow for flight to be undertaken

**Step 4**: Intimation of the same sent to all stakeholders

**Step 5**: Flight Path Data Transmitted (*Real-Time Tracking via sending of Telemetry Data*) by Drones to Digital Sky application which is tracked on real time basis. It is to be ensured that approval certificate controls the flight path within defined limits; in this regards, the approval certificate should have geo fencing kind signal capability integrated into the drones. Further, the certificate should also have protocols in built for
emergency/forced landings, wherein, nearest locations for safe landing can be undertaken automatically. All transmitted flight paths are on real time basis evaluated and accordingly warning signals are activated in case of breach of air space.

It is to be noted that a Standard Operating Procedure will be defined in such cases to be activated. MSP is required to account for Call Center Support in this regards. Further, protocols of SOP will be defined in case flight path is not being transmitted real time from Drones.

3. Process and Services in Post Flight Module

3.1 Uploading of Flight Data for Compliance Check and Rating
For the purpose of post flight data evaluation, it is required that operators/pilots provide data in defined formats (to be extracted from the drones) and upload the same at Digital Sky.

**Step 1:** Applicant select the approved application and select upload post flight data

**Step 2:** Applicant upload data

**Step 3:** Digital Sky evaluates various parameters associated with flight data captured

**Step 4:** Based on approval, compliance comparison is drawn and compliance ratings provided

**Step 5:** All non-compliance related reports generated and submitted to DGCA for action

3.2 Pilot and other eLogBooks
Each pilot is to maintain a digital logbook that shall be in digital format. For the same, post each flight log books are to be filled by each pilot.
It is to be noted that logbooks will be used to validate the drones being flown by authorized persons only. In each application for drones, operator is required to submit details of the pilot who will be flying the drones. In this regards, log books shall enable a check on all activities related to the drones flying by the authorized person. Similarly, other stakeholders will be require to fill elogbooks in similar manner for drones, operators, etc.

3.3 Enforcement/Action Modules
The module will be developed to allow for undertaking actions such as cancellation of permits/license based on non-compliance observed. Further, the module shall allow for capturing all non-compliance history associated with a license/permit/UIN/manufacturer, etc.

It is to be noted services listed in D3X-X1 shall also be included within the scope. Further, MSP to refer to the draft CAR for process related details for all the services. Further, refer to FAQs and Do’s & Don’ts released by DGCA
### Appendix 4 - Functional Requirements

<table>
<thead>
<tr>
<th>S.no.</th>
<th>Major Stakeholders</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>DGCA/AAI</td>
<td>Officials will be responsible for approvals and monitoring</td>
</tr>
<tr>
<td>2.</td>
<td>UAV manufacturers</td>
<td>UAV manufacturers will be responsible for getting approvals for their UAV type acceptance</td>
</tr>
<tr>
<td>3.</td>
<td>UAV Pilots</td>
<td>UAV pilots/operators will get registered for operating UAVs</td>
</tr>
<tr>
<td>4.</td>
<td>UAV Pilot training schools</td>
<td>Registration and renewal of license/permit for providing pilot/UAV training</td>
</tr>
<tr>
<td>5.</td>
<td>UAV operators/Owners</td>
<td>UAV operators/Owners will take services for operating UAVs and approval of flight paths</td>
</tr>
<tr>
<td>6.</td>
<td>Others</td>
<td>Other Govt. Departments, Citizens</td>
</tr>
</tbody>
</table>

#### Integration Requirements

- Real-Time Integration with airspace existing systems
  - AFTN & AMSS for NOTAMs
  - MET for meteorological data
  - NOCAS for Building/Structure NOCs Data
  - ATS Automation System for Air Traffic Data & FIC/ADC Number
  - Military Operations Centre
- Other Integrations: Aadhaar Auth/eKYC Services, GSTN Auth Services, Payment Gateway/BharatKosh, Email, SMS Services, eSign, DSCs
- Certification agencies
- Digital Sky Providers
- eGCA
- Ministries such as MHA, CBEC, MCA
- Data.gov.in
- The vendor is responsible for to provide for e-SIGN and GSTN certification/authentication also as part of scope. All associated costs to be borne by vendor

In addition, any other integration requirements are to be taken up based on defined functional requirements below.
## 1. Common Functional Requirements with respect to Workflows/Compliance approvals

<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration Process</strong></td>
<td>All external/Internal stakeholders should be registered through Digital Sky portal. For the purpose of registration, secured two-step process of email verification and OTP based mobile verification be undertaken.</td>
</tr>
<tr>
<td><strong>Sub Category</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Login IDs</strong></td>
<td>System should allow organizations to create login IDs of specific individuals within their organizations against special post holders as per compliance requirement</td>
</tr>
<tr>
<td></td>
<td>Such login created will be treated under the umbrella of root login ID and hence, an action undertaken within this ID will be associated with root (parent) ID.</td>
</tr>
<tr>
<td></td>
<td>It is to be noted that the system should allow for root ID provide administrative rights to individuals registered under them. For example, specific teams of an organization should be allowed to access the modules under their ambit only.</td>
</tr>
<tr>
<td></td>
<td>The hierarchy defined by organizations could be multi-tiered and accordingly the sub-administrative rights can be provided by any individual to people below them in the tier based login requirements</td>
</tr>
<tr>
<td><strong>Aadhaar / GSTN Authentication</strong></td>
<td>It is required that AADHAAR / GSTN based validation is undertaken during registration.</td>
</tr>
<tr>
<td><strong>Digital Sky unique ID</strong></td>
<td>All stakeholders are required to have a unique Digital Sky ID. The unique Digital Sky ID should be created at the time of registration. The format for Digital Sky ID should identify the stakeholder type; for the formats, MSP is required to discuss with AAI at time of implementation.</td>
</tr>
<tr>
<td></td>
<td>Such unique ID is to be revoked in case the concerned individual/entity (especially internally) is no longer associated with Digital Sky related matters.</td>
</tr>
<tr>
<td><strong>Multiple ID associated with Individuals to be used interchange-ably</strong></td>
<td>For the purpose of requirements as per ICAO/DGCA/Other regulators, multiple IDs may be required to be created related to a stakeholder. For example, a UAV pilot is required to have a unique pilot license number which cannot be linked to their Digital Sky ID.</td>
</tr>
<tr>
<td></td>
<td>For this purpose, all services to be rendered to specific stakeholder can be provided through such IDs interchange-ably. Further, all information required by DGCA for any specific purpose can be sourced using such ID numbers interchange-ably.</td>
</tr>
<tr>
<td></td>
<td>Hence, for the purpose, all ID numbers created through Digital Sky for a stakeholder should be all linked to Digital Sky ID.</td>
</tr>
<tr>
<td><strong>Profile Management</strong></td>
<td>This component will manage the profile of each of the stakeholders on the Digital Sky platform. In this component, the DGCA officers as well as these users would be able to see the earlier transactions and status of the live transactions. The users would also be able manage the personal information related to their profile on the Digital Sky platform from here</td>
</tr>
<tr>
<td>Functional Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Persona based Home Page</td>
<td>The home page of the Digital Sky portal is required to be persona driven (personalized view for different set of stakeholders), wherein, all information and services displayed are related to the persona only. The services display on home page is hence, required to be dynamic and persona based (including for same category of stakeholders)</td>
</tr>
<tr>
<td></td>
<td>However, flexibility is required to be built in the system to include other services (not related to persona). For the same, MSP is required to discuss the services mapping and business rules associated with the same with AAI.</td>
</tr>
<tr>
<td>Multiple Login working on same application</td>
<td>Based on the access rights provided to individuals, multiple individuals could work on a single form. For example, in an organization, multiple people are required to fill the same form but different areas in the form. For the same, specific cell rights can be given on the same form and multiple people could work on it.</td>
</tr>
<tr>
<td>Ability to Generate Temporary Username/Password for Third Party for Providing Read Only Access to specific Information</td>
<td>Stakeholders should be able to generate a temporary username and passwords for third party and be able to provide read only access to specific information.</td>
</tr>
<tr>
<td></td>
<td>For example, a UAV manufacturer wants to provide their UAV specific details to Foreign country’s Regulatory body. For the same, manufacturer should be able to generate a temporary username and password for third party to login into Digital Sky and validate information.</td>
</tr>
<tr>
<td></td>
<td>Such login credentials is required to have a pre-defined validity.</td>
</tr>
<tr>
<td>Application Multi Access</td>
<td>In some cases, applications should be allowed to be made on behalf of applicant. For the same, administrative rights can be given to other to undertake the applications. However, such access will be provided based on pre-defined rules that will be shared by AAI from time to time.</td>
</tr>
<tr>
<td></td>
<td>The application should have flexibility to allow such access (without sharing username/password).</td>
</tr>
<tr>
<td>Safety Reporting</td>
<td>Portal should allow people to report safety incidents that should be collated in organized manner.</td>
</tr>
<tr>
<td>Password</td>
<td>1. Define the format for the password based on the standards set by the government (if any) or based on the discussion with the client.</td>
</tr>
<tr>
<td></td>
<td>2. Define a limit of days to change the password to all users based on client’s requirement.</td>
</tr>
<tr>
<td></td>
<td>3. Add the ability to ask the user to enter a new password, once the system detects that expiry password date (Client defined Days to Password Expiration + Last Update Password Date for user) has arrived.</td>
</tr>
<tr>
<td>Automatic data population and validation</td>
<td>All forms are required to be streamlined to remove redundancies in terms of seeking information. Wherever the information can be retrieved from the system will be pre-loaded on the relevant application forms. However, it is required that before submission of pre populated data, stakeholder is provided an option to review the pre populated data.</td>
</tr>
<tr>
<td>Functional Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>For example, current information available at eGCA should be auto populated rather than seeking same information again from the stakeholders. Example, a PPL holder can apply for Drone License. In that case, data should be retrieved from eGCA system. eGCA system is being currently under development at DGCA. Hence, API based information sharing is a requirement. Further, all information that has been previously entered in the system shall be displayed subsequently/not asked in the subsequent forms. E.g. In the approval process for a new flight path for a previously registered UAV, some of the UAV details may not be asked again.</td>
</tr>
<tr>
<td></td>
<td>Formats</td>
</tr>
<tr>
<td></td>
<td>Digital Sky would follow standard structures and templates for various documents messages and alert that are generated within the platform and shared with the users. This module would provide interface for management of templates for all document and alerts (SMS/ Email etc.) in Digital Sky.</td>
</tr>
<tr>
<td></td>
<td>Issuance of Approvals/ Letter</td>
</tr>
<tr>
<td></td>
<td>Standardized templates is required to be developed for issuance of approval letter/certificates digitally wherein, standard text can be added from the database based on the approval. For each relevant service, such approval letters/certificates are required to be designed and integrated into the system for such issuance. However, the template published should be editable such that additional text can be added to the letter.</td>
</tr>
<tr>
<td></td>
<td>Undertakings</td>
</tr>
<tr>
<td></td>
<td>Wherever relevant, digital undertakings can be undertaken by stakeholders for submission of applications. For example, an application is made by drones operators on behalf of drones pilots; hence, pilot can provide a digital undertaking to drones operator to make an application on his/her behalf.</td>
</tr>
<tr>
<td>Service Assignment Workflow Module for Processing Service Requests</td>
<td>There would be some services which will be automated and will not require any intervention from the officials, however, there will be services which cannot be fully automated and require processing by the DGCA/AAI officials. For any service request, there could be 3 key internal stakeholders: - Receiver: The person who receives application once submitted by the stakeholder - Evaluator: The person assigned with task of reviewing the application and - Approver: Approves the Application</td>
</tr>
<tr>
<td></td>
<td>It is required that workflow be designed with flexibility of assigning multiple people for each of the above. Further, the application shall allow for unplanned selection of individuals under each category.</td>
</tr>
<tr>
<td>Functional Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>It is required that a default designation be assigned for each service in each category that can thereon be changed by DGCA/AAI.</td>
<td></td>
</tr>
<tr>
<td>Please note that DGCA/AAI officers with specific administrative rights for the service may be directly allowed to make changes in such default settings.</td>
<td></td>
</tr>
<tr>
<td>There will be two types of file movements for various services in Digital Sky:</td>
<td></td>
</tr>
<tr>
<td><strong>Movement as per process steps:</strong> With application completion and submission, the service owner in AAI/DGCA will have the provision to assign the application to different stakeholders within AAI/DGCA. There will be a provision to search the name of individuals within AAI/DGCA (with defined parameters such as name, designation, region, directorate etc.) and assign particular step of the process to them.</td>
<td></td>
</tr>
<tr>
<td>The assignee will receive a notification (Email + SMS) on the same and it will reflect on their dashboard as well. There will also be an option to <strong>add additional attachments</strong> in addition to the required files.</td>
<td></td>
</tr>
<tr>
<td><strong>Reverse movement in case of clarifications/actions:</strong> In case of any clarification/action is required from the previous step of the process, the same can be sent back by either the applicant/DGCA/AAI along with comments. There will also be provision for <strong>adding attachments</strong> in the reverse flow.</td>
<td></td>
</tr>
<tr>
<td>Both internal and external stakeholders will have the ability to raise queries at any stage of the process of a service with the ability to add or request attachments. This is in continuation to the internal/external file movement.</td>
<td></td>
</tr>
<tr>
<td>All such queries, comments, clarifications are to be associated against the service request.</td>
<td></td>
</tr>
<tr>
<td>It is required that all such communication undertaken related to the service should be traceable at any later stage</td>
<td></td>
</tr>
<tr>
<td>All the actions on the portal such as request/response for query, uploading of documents, data validations, data entry/removal etc. by either internal or external stakeholders will have a time stamp and individual mapping which can be used for tracking and evaluation.</td>
<td></td>
</tr>
<tr>
<td>Time stamps will be an integral part of the system for monitoring adherence to SLAs by AAI/DGCA officials that are promised to stakeholders and also for audit purposes.</td>
<td></td>
</tr>
<tr>
<td>Each request will have a unique transaction ID for tracking and reference. The request ID will be used as a primary key for creating dashboard views, allocation of tasks etc.</td>
<td></td>
</tr>
<tr>
<td>The module allows for assigning specific tasks to individuals and tracks their progress. Such tasks assignment can be automated based on work load on individuals; further, such assignment of tasks can also be manual based on preference and nature of service</td>
<td></td>
</tr>
<tr>
<td>Functional Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance Check</td>
<td>All processes involve generation of various documents at various stages. Digital Sky is expected to make these processes paperless. All documents generated need to be generated in a standard mechanism, with common functionalities like use of templates to be populated, PDF generation, digital signatures etc. All such common functionalities related to generation of any kind of documents would be encapsulated in this components and used by other specific components.</td>
</tr>
<tr>
<td>Document Generation</td>
<td></td>
</tr>
<tr>
<td>Auto Generation of Approval number/Letter No/License No, etc.</td>
<td>All approvals related to a request will have an auto generated number based on pre-defined rules. The rules for the same will be finalized in discussion with DGCA/AAI.</td>
</tr>
<tr>
<td>Photo Attachment and Organization</td>
<td>For certain services, especially, surveillances, incident reporting, photographs may be taken and attached as proofs. Such uploading of photographs should be attached to the service number and file be created in desirable format. Further, the file created should be metadata tagged and automatically named in a pre-defined format.</td>
</tr>
<tr>
<td>Multiple Documents Upload</td>
<td>System should allow for multiple documents to be uploaded simultaneously as per requirements of the application form of a service</td>
</tr>
<tr>
<td>Heavy Files Management (FTP)</td>
<td>For the purpose of heavy files, uploading of the files should be allowed within an FTP server and linkage to the same be provided in the application form rather than uploading the same along with application form.</td>
</tr>
<tr>
<td></td>
<td>The minimum size limit for the same may be decided between MSP and AAI/DGCA.</td>
</tr>
<tr>
<td>Uploaded Documents Management System for Services</td>
<td>All documents uploaded by the stakeholder for purpose of a service should be meta data tagged accordingly. Such uploaded documents should always be tagged with the service for which the documents were uploaded. The system should also allow for a version control mechanism to cater to identification of documents submissions at various stages.</td>
</tr>
<tr>
<td></td>
<td>Further, flexibility of auto archiving of version of documents should exist in certain services based on repetitive submission of documents for a single service request. Such option is to be exercised based on discussion with DGCA on specific services only.</td>
</tr>
<tr>
<td></td>
<td>Applicants should be allowed to upload various format documents as per system requirement.</td>
</tr>
<tr>
<td>Continuous Compliance Check/Validifications</td>
<td>All checks for compliance should be done on real time basis and any unexpected non-compliance be flagged to AAI/DGCA immediately and also to the concerned individual.</td>
</tr>
<tr>
<td></td>
<td>For example, a UAV has has deviated from the approved flight path, such flagging will cause non-compliance which should be flagged to different stakeholders. Based on such non-compliance, the relevant action option should be given to the stakeholders and updating of the same across the system should be done. Further, in case of non-compliance based on other requirements to be maintained by individual, an auto generated warning should be generated for authorities in AAI/DGCA and also to the non-compliant individual.</td>
</tr>
</tbody>
</table>
### APPENDIX 4 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dashboards</strong></td>
<td>Similar action is required for forms filled for service based on pre defined rules.</td>
</tr>
<tr>
<td></td>
<td>Digital Sky will allow the users to prepare their own dashboards based on statistics, documents pending, and documents processed etc. at different levels. This component would allow configuration and management of such dashboards.</td>
</tr>
<tr>
<td></td>
<td>However, there will be default settings for each set of stakeholders wherein, they will be able to view dashboard containing information and services relevant to them. The dashboard view will be as per the access rights of each set of stakeholders. The information sharing on dashboards is to be finalized in consultation with AAI/DGCA.</td>
</tr>
<tr>
<td><strong>Application Fees Payments through BharatKosh or any other Payment Gateway</strong></td>
<td>The application fee for all services are to be stored in a central repository wherein the applicable fee will be automatically populated for displaying the required fee for the services.</td>
</tr>
<tr>
<td></td>
<td>All forms that require submission of fees will have a payment gateway option integrated with the BharatKosh. The payment made through the gateway will be automatically verified and successful payment receipt is to be generated.</td>
</tr>
<tr>
<td></td>
<td>In case, the payments are made directly at BharatKosh, transaction number will be validated from BharatKosh. Further, in case, the DGCA/AAI is required to integrate with any other payments gateway, such integration shall be undertaken with similar functionalities.</td>
</tr>
<tr>
<td></td>
<td>Cart option for multiple application payments are to be made such that fees can be paid one time for multiple applications in single session. The information of all such payments are to be provided to finance team of AAI/DGCA through the portal in formats to be decided by DGCA.</td>
</tr>
<tr>
<td><strong>Automated notification on breach of SLAs</strong></td>
<td>The system will automatically notify the relevant stakeholders in case of breach of SLAs for a service. The breach of SLA will automatically be displayed on the dashboard of all concerned stakeholders including senior management.</td>
</tr>
<tr>
<td><strong>Ability to Send Reminders to stakeholders</strong></td>
<td>DGCA/AAI should be able to send reminders to stakeholders involved towards processing an application. Such reminders shall be associated with the service request and is to be stored for future references.</td>
</tr>
<tr>
<td><strong>Meeting/Activity Scheduling Module</strong></td>
<td>For the purpose of holding multi stakeholder meeting or scheduling a joint task with both internal and external stakeholders, a scheduling module is required to be developed integrated with workflow of each service requiring such feature.</td>
</tr>
<tr>
<td></td>
<td>For stakeholders in DGCA/AAI, their calendars will be synced with the module and their availability will also be displayed before a meeting is schedules. In case of external stakeholders, the applicant will be automatically notified if a meeting request has been made. The platform will also have the functionality to send automated mails/SMS to external stakeholders other than the applicants.</td>
</tr>
<tr>
<td>Functional Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Once the request has been accepted by the recipient, the same will reflect on the dashboard of both the sender and recipient.</td>
</tr>
<tr>
<td></td>
<td>In case of external stakeholders who do not have an entity on the Digital Sky platform, their acceptance of the request will start reflecting on the dashboard of the sender. (A URL will be sent for acceptance by the recipient on mail).</td>
</tr>
<tr>
<td></td>
<td>Confirmation of the request of Digital Sky ID holders same can be done over email/sms/app by individuals.</td>
</tr>
<tr>
<td>Calendar based appointment scheduling</td>
<td>Digital Sky platform would provide a calendar based appointment management system. This component would manage automated scheduling of appointments with AAI/DGCA officers. Additionally, this component may be used by department officials to set up and define their calendars. This component needs to be built with a provision to automate walk-in appointments at various locations.</td>
</tr>
<tr>
<td>Grievance Redressal Module</td>
<td>There will be an in-built GRM module which can be used for resolution of grievances for both internal and external stakeholders. For the same, Digital Sky support team will be first level responders/supporters as per the escalation matrix. The MSP shall, in consultation with the AAI/DGCA, design and implement an escalation matrix for providing resolutions of issues so reported by the stakeholders through any communication channels. For all grievances, ticket number shall be assigned. Further appropriate categorization of the same shall be done to track areas of grievances.</td>
</tr>
<tr>
<td>Information Sourcing</td>
<td>This component will enable the users of eGCA platform to run a query to fetch information related to applications, status and other services.</td>
</tr>
<tr>
<td>Digital Signatures</td>
<td>There will be provision for selected DGCA officials to provide digital signatures in all the applications/requests etc. where they are the approving authority. External stakeholders will also have the provision to digitally sign their applications and approvals etc.</td>
</tr>
<tr>
<td>E Signatures</td>
<td>While digital signatures are applicable for individuals representing DGCA/AAI, individuals such as UAV pilots etc. will be required to have option for e-signatures. The e-signatures may be validated through AADHAR provided the data is shared UAIDAI. In addition to eSign, other forms of DSCs must also be supported (like hardware dongles as authorised by CCA) for digital signing.</td>
</tr>
<tr>
<td>API</td>
<td>System is to be designed to source information available with various stakeholders. The data to be sourced is to be discussed with stakeholders during the course of designing phase of the solution.</td>
</tr>
</tbody>
</table>
### Functional Requirements

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on such data, auto population of information is required at form level. Further, flexibility in design is required to be done such that stakeholders whose information is sourced from other systems have different forms and data requirements for a service, while others that don’t have such source of information from external stakeholders can also apply based on larger requirement of data to be manually submitted.</td>
</tr>
<tr>
<td>The MSP is required to assess all information that can be auto populated from the external agencies through stakeholder interactions. DGCA will support the vendor in arranging such stakeholder consultations, provided at least 7 working day notice is given to DGCA/AAI. Further, it is onus of DGCA/AAI to seek approval and come to an agreement for sourcing of data. MSP is required to provide technical documents and data requirements to DGCA/AAI for undertaking discussion with stakeholders</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Wide Information Symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on any new development (such as enforcement, etc.) related to an Digital Sky ID, the impact of such development will trigger alerts for change required to all other related services to concerned authorities for acceptance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the enforcement done by DGCA /AAI officials will also be tagged in the system with the associated stakeholders. The enforcement actions will be tagged for each stakeholder on the Digital Sky portal for review at any point in time. The access rights will be different for external stakeholders and internal stakeholders. All enforcements will be readily available for access to all stakeholders and any impact of enforcements shall be intimated to each directorate for acceptance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the purpose of renewal/validity, while the standard validity for an approval type is given as per CAR, in some services flexibility of deciding the validity of an approval is to be given</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Agnostic Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>The platform will be accessible through multiple devices such as desktop, laptop, mobile, tablet etc. There will be a web based portal for access by desktop and laptop; and a mobile app for access by mobile and platform available on leading platforms such as Android and iOS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flexible search Database Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to search and validate the individuals, UAVs, etc who are recognized by AAI/DGCA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quick Profile View</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the purpose of quick evaluation of an individual's application or profile, a summary view of key points shall be developed that can be accessed by any officer in AAI/DGCA during review period. The dashboard should include compliance dashboards; further, compliance scorecards be provided any analytics driven insights be given on areas of risks</td>
</tr>
</tbody>
</table>
2. Functional Requirements for Registration at Digital Sky

In this section, the functional requirements specific to certain modules/services are included. It is to be noted that some of the functional requirements listed may be similar to the common functionalities listed in “Common functionalities” Section.

<table>
<thead>
<tr>
<th>Functional Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Sky Identification Number</td>
<td>Post registration and validations, a unique eGCA ID is generated for applicants, which will be used for all processes/services.</td>
</tr>
<tr>
<td>Mapping of All ID Nos with eGCA ID</td>
<td>All individual numbers associated with the stakeholder such as pilot license number, Operator Number etc. shall be all mapped to the Digital Sky ID of the applicant. The format of Licence number, Operator Permit number etc. shall be standardised based on the directions from AAI/DGCA.</td>
</tr>
<tr>
<td>Validation of Data by eGCA Support Cell</td>
<td>All data captured through stakeholders/entered manually by vendor, validation for correctness of data is to be undertaken by Vendor’s “eGCA Support Cell” through comparison of scanned copies uploaded.</td>
</tr>
<tr>
<td>Flagging of Validated/Approved Data</td>
<td>Upon validation of data, specific flags are indicated of validation that can thereon be reviewed by AAI/DGCA officials; once AAI/DGCA officials verify the data, it will be considered true data, which is flagged and recognized accordingly by the system.</td>
</tr>
<tr>
<td>Service Level Dashboard</td>
<td>All data entries that were made wrong at source and/or were not been able to be captured during validation stage by vendor shall be separately captured and dashboards of the same shall always be available for AAI/DGCA to track error rate.</td>
</tr>
<tr>
<td>Data Change Process</td>
<td>The data change process shall be included for all data that has been accepted by Digital Sky support cell and AAI/DGCA officers, but is identified to be wrong at later stage. For the same, special approval process shall be followed.</td>
</tr>
<tr>
<td></td>
<td>It is to be noted that such special approval process shall be decided based on discussion between DGCA/AAI and MSP.</td>
</tr>
<tr>
<td>History Traceability</td>
<td>All records w.r.t person validating/changing/approving data w.r.t. to registration process shall always remain in records and be easily accessible</td>
</tr>
<tr>
<td>Data Acceptance for eGCA Processing of Application</td>
<td>The system should recognize the data for application processing only after DGCA/AAI officials have approved the authenticity of data</td>
</tr>
<tr>
<td>DGCA Approval on Data entry</td>
<td>Data Entry for approval should be made available to DGCA/AAI on immediate basis; however, the DGCA/AAI officials may decide to verify data on need basis.</td>
</tr>
</tbody>
</table>
3. Functional Requirements of e-log book (Pilot Log Book, Drones Log Book, etc)

The MSP is required to design 4 elogbooks based on requirements to streamline information requirements from stakeholders and also ensuring data sets available for continuous compliance checks based on analytics. The following provide the functional requirements related to E-Log Books:

<table>
<thead>
<tr>
<th>Functional Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Friendly Log Books</td>
<td>E-Log Book design should be user friendly and not cumbersome. The entry options should be offered on need basis only. For example, if a pilot has undertaken flying in one type of drone, the options for other drones type should not be visible for inputs as such inputs are not required for that particular entry.</td>
</tr>
<tr>
<td>Validation of Entries</td>
<td>E-Log book should allow individuals to certify entries from relevant designated officer, etc. Such validation should be done through digital signatures of designated person. For the same, designated individuals enlisted in Digital Sky shall be selected by individual for submission.</td>
</tr>
<tr>
<td>Supporting Documents as Attachments</td>
<td>The log book should allow individuals to attach supporting documents for validation of entry (in case required)</td>
</tr>
<tr>
<td>Approved Entries</td>
<td>Only validated/approved entries should be made available for auto population of application undertaken by individuals/operators on behalf of individuals</td>
</tr>
<tr>
<td>Relevant Flags Option</td>
<td>E Log Book should allow option to flag entries based on need. For example, if an entry is revised, an auto flag should be created. On the other hand, if an entry is required to be reviewed by AAI/DGCA officer, an designated officer could flag the entry “Attention”. Similarly, multiple flags options should be made available for ease of compliance check.</td>
</tr>
<tr>
<td>Auto Sync Option (API based Auto Population)</td>
<td>Stakeholders could sync their log books with systems of stakeholders for auto population of data. For example, a pilot working with an operator has digital log books maintained by operators. For the purpose of auto population, the pilot could sync their log books with such databases to reduce burden of digital inputs manually.</td>
</tr>
<tr>
<td>Revision</td>
<td>Individuals should have an option of revising log book entries; however, such revision is required to be re-validated by designated authority of DGCA; all changes made post first time validation is required to be logged. Based on regulations, it may be decided that entries beyond a time limit cannot be edited.</td>
</tr>
<tr>
<td>Integration of Log Book with Dashboard</td>
<td>Any action required by individuals should be showcased on the dashboards. Such Dashboards will serve the purpose of information and reminders</td>
</tr>
<tr>
<td>Auto Compliance Check</td>
<td>For the purpose of validation of entry and compliance of individuals to meet requirements as per rules and regulations, e log book should automatically and continuously undertake checks on compliance. In case of non-compliance, intimation of the same shall be given to concerned authorities and suggested actions should be highlighted.</td>
</tr>
</tbody>
</table>
### Functional Requirement Details

<table>
<thead>
<tr>
<th>Functional Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Box Option for Single Step Action on Multiple entries:</td>
<td>Log book should have an option of selecting multiple entries for multiple actions in one single step rather than repeating the same action multiple times for multiple entries.</td>
</tr>
<tr>
<td>Filters</td>
<td>Relevant filters are to be provided to view desired entries based on filters. All summation should be based on filtered entries; it is to be noted that summation of entries in terms of hours etc should be automated.</td>
</tr>
<tr>
<td>Auto Matching of Entries to Avoid Wrong Data Entry</td>
<td>Multiple log book entries should be compared to detect errors/fraudulent entries. For example, entries mismatch of drones log book and pilot should be auto detected.</td>
</tr>
<tr>
<td>E-Log Book Mobile App</td>
<td>An app offering same features should be developed for Android and iOS. The app entries should be integrated with web portal application for E-Log Book. The mobile app should allow for offline entries that can be integrated with database once access to internet is achieved.</td>
</tr>
<tr>
<td>Access Rights</td>
<td>Appropriate rights to various individuals and authorities to be given as per the requirement. For example, DGCA/AAI officer who has been assigned with task to evaluate an application should be automatically given access to log book of applicant.</td>
</tr>
<tr>
<td>Selected Entries as PDF document</td>
<td>Auto generation of selected entries as PDF should be done in order to share entries with external stakeholders.</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>All entries should be validated through digital signatures.</td>
</tr>
<tr>
<td>Time Stamping</td>
<td>All entries should be time stamped and identify the individual who has made entry, validated the entry, edited the entry etc.</td>
</tr>
<tr>
<td>Entries with Access Rights</td>
<td>Certain entries made by DGCA designated individuals should be accessible only to DGCA and not to applicant.</td>
</tr>
<tr>
<td>Email Option</td>
<td>An auto integration of log book should be made with email app to easily send email with specific entries.</td>
</tr>
<tr>
<td>Personalization</td>
<td>Based on the relevance of category, the view of the log book is required to be different. For example, entries for view for pilots will be different than that of the designated officer.</td>
</tr>
<tr>
<td>Integration with Third Party Software for filling pilot log books</td>
<td>The elogbook is auto populated based on integration with log books maintained by third party softwares provided integration is feasible.</td>
</tr>
</tbody>
</table>
4. Functional Requirements for Map Application and Required Analytics Features

The module should have Pre-loaded maps of the country’s airspace with provision to search, select and perform functions on geographical areas.

<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selection of No-Fly/Limited Fly/Free Zone</strong></td>
<td>Ability to plot various areas on map based on selection on map directly or through indication of latitude and longitude. With input of either case, the other should automatically populate. Or they can upload a flight path in complex drawings. Further, plotting based on Time of Day should also be enabled to restrict flights based on time of day. Similarly, any editing of such plotting can be undertaken. A workflow shall be defined in the system for approval for all such activities in consultation with AAI/DGCA.</td>
</tr>
<tr>
<td><strong>Data Layers</strong></td>
<td>Ability to add layers of data on the map for compliance/safety/security checks based on analytics</td>
</tr>
<tr>
<td><strong>Search Option</strong></td>
<td>Ability to search locations/areas based on Geography, Lat/Long, Filters (defined in input layers)</td>
</tr>
</tbody>
</table>
| **Integration/Auto Population of other Data layers** | Ability to auto populate information layers provided by other departments. The Map module should be able to auto translate and reflect data in maps based on information provided by other departments through API or otherwise. Integration envisaged currently are as follows:  
  - AFTN & AMSS for NOTAMs  
  - MET for meteorological data  
  - NOCAS for Building/Structure NOCs Data  
  - ATS Automation System for Air Traffic Data & FIC/ADC Number  
  - Military Operations Centre |
| **Visual Zones** | Clearly identifiable and colour coding should be undertaken on maps based on defined zones |
| **Review Option for plotted areas** | All data/points plotted by individuals should be tagged to their profile and should have an option to review/change the same in user friendly manner. Appropriate approval workflows shall be integrated with such processes. |
| **Analytics based flight path recommendation** | Based on plotted regions, module should also provide recommended flight paths to users while applying for approvals |
| **Selection of Flight Path** | Ability for individuals to mark flight path in complete flexible manner. It should allow for any flight path with variation in direction, area plotting, altitude variation etc. |
| **Flight Tolerance Plotting** | Should have built in flight path tolerance defined on case by case basis (business rules driven). Based on this, approvals should be provided |
## Functional Requirements Details

### 4D Mapping
- Ability to define altitude, latitude, longitude, time of day and mapping of the same along with flight path

### Machine Learning Capability
- Based on various safety, security risks that can be derived from the data captured by the Digital Sky, the system should be able to derive and suggest business rules for further consideration of AAI to improve the functionalities and business rules of the Digital Sky Platform

### Landing Spots Marking and Selection
- It is requirement that applicants mark areas in the flight path on such parameters. The module should have ability to auto analyse the feasibility of marked areas based on image analysis and other layers of data.

### Auto Guidance
- Based on selected flight paths, maps should highlight and indicate non-availability of airspace. This should also consider parameters such as time and date of flight, etc. Further, it should recommend available time, path etc. that can best suit the requirements

### UI
- The UI should be intuitive and map based. All plotted areas should be clearly defined on maps in different colour codes for ease of reference of end user

### Risk Evaluation
- Based on data provided, application should be able to evaluate each application and provide risk score for the same. Elements such as Drones make should also be considered in terms of flight time and capacity of flight time of drones. Similarly, multiple such checks and balances ae to be included for deriving the risk scores.

### Real time Updates
- Ability to auto highlight approvals that should be revised based on new data inputs and thereon, allow for actions accordingly. For example, an approval for flight path has been provided earlier which may thereon be re-defined as no fly zone for a limited period should be highlighted and trigger revision of approvals.

Further, based on risk scorecard, workflow to be initiated.

## Functional Requirements for Approval Certificate, Flight Tracking and Analytics based Compliance Checks

<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Details</th>
</tr>
</thead>
</table>
| Approval Certificate    | The approval certificate should integrate with the Drones to activate the drones operations in the following manner:  
  1. Act as a Geofencing mechanism  
  2. Provide Security key to Drones for undertaking flight  
  3. Emergency/Forced Landing SOPs |
| Pre-Flight Authentication| It is required that during pre-flight (in a pre defined period prior to flight), authentication is undertaken through dial in from Drone. The authentication should have mechanism wherein, specific key based code is provided to Drones to authenticate the validity of the certificate. |
APPENDIX 4 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Live Flight Feed</strong></td>
<td>System design should allow for capturing and processing live feed from Drones and thereon, undertake compliance checks on flight path, altitude etc. This functionality should include Telemetry Engine for capturing streaming of location information from Drone to Digital Sky.</td>
</tr>
<tr>
<td><strong>Post Flight Data Analysis</strong></td>
<td>The system design should undertake all analysis on post flight data uploaded by the pilot/operator and thereon validation of compliance is required to be undertaken on the same.</td>
</tr>
<tr>
<td><strong>Auto Calls</strong></td>
<td>In case of any non-compliance identified, an auto call shall be generated to the pilot and standard messages with details of non-compliance indicated over the call. Similarly, alert messages for the same shall be given to the authorities.</td>
</tr>
</tbody>
</table>

6. Functional Requirements – Registries

- Machine Readable Registries for Certified Registered Flight Modules, Digital Sky Service Providers, etc.
- There should be internal registries (accessible to select stakeholders) and external registries (accessible to public).
- Registry Management should be via UI and APIs. The broad requirements are:
  - Flexible schema definition with complex structures
  - Encryption and masking at attribute level
  - Flexible data visibility classification
  - Owner controlled consented access to service providers
  - Digital signature for trusted data
  - Open APIs for data publishing and registry access
  - Flexible data lifecycle control at attribute level
  - Extensibility hooks to build advanced features
  - Ability to link registry entries within the same registry and across registries using different relationship types
  - Extensible registry persistence model with support for graph based database, key-value stores, and blockchain
  - Ability to attach rules for validations, lifecycle operations, and relationships
  - Existing open source libraries can be leveraged: [https://github.com/project-sunbird/open-saber](https://github.com/project-sunbird/open-saber)

7. Functional Use Cases

<table>
<thead>
<tr>
<th>Functional case</th>
<th>Description</th>
<th>Systems involved / stakeholder</th>
</tr>
</thead>
</table>
| UAS registration | UAS, pilots and operators should be registered in order to be able to be identified in the UTM system. | - UAS pilot/operator  
- UAS registration system  
- UAS  
- UTM service provider  
- UTM system  
- National aviation authorities |
### APPENDIX 4 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

<table>
<thead>
<tr>
<th>Functional use case</th>
<th>Description</th>
<th>Systems / stakeholder involved</th>
</tr>
</thead>
</table>
| **UAS identification** | UAS, pilots and operators should be identified in order to be able to provide dedicated UTM services. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Operation/flight request** | Drone flight plans should be created, changed and deleted to provide the intent to the UTM system. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Authorizations and directives** | Flight permission should be created, changed or rejected either manually or automatically to provide airspace access information to UAS. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Notifications/alerts/warnings** | Notifications, alerts and warnings such as NOTAM, weather alerts, etc. should be shared to improve the awareness of the UAS pilot. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Situational awareness** | Information on UAS positioning and contingency information should be shared to improve situational awareness, warn all other airspace users, and enable certain authorities to act if required. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider  
- Authorities  
- Law enforcement  
- Emergency services  
- Conventional airspace users  
- ATM System(s) |
| **Contingency information** | Information on unplanned flight executions, deviations, and emergencies should be shared to warn all other airspace users. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Real-time positioning** | Real-time positioning information should be shared in order to have an actual overview to improve situational awareness and/or to provide conflict advisories. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider  
- Conventional airspace users |
| **Performance information** | Performance information of UAS should be shared in order to have accurate information on the UAS, which is needed for optimizing route management. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Conflict advisories** | When conflicts (could be other UAS, obstacles, manned aircraft, emergencies, incidents, etc.) are detected by the UTM system, the UTM should share the advisories to resolve the conflict. | - UAS pilot/operator  
- UAS  
- UTM system  
- UTM service provider |
| **Priority constraints** | A priority constraint should be created if, for example, an incident occurs, and it is needed to create a temporary restricted area. | - Law enforcement  
- Emergency services  
- Authorities  
- UTM system  
- UTM service provider |
<table>
<thead>
<tr>
<th>Functional case</th>
<th>Description</th>
<th>Systems / stakeholder involved</th>
</tr>
</thead>
</table>
| Identification  | Aircraft should be identified in order to receive correct information, which can be communicated to UAS pilots/operators to improve situational awareness. | - UTM system  
- UTM service provider  
- Conventional airspace users |
| Aeronautical information | Aeronautical information should be shared to be used in the UTM system to provide UTM services for the UAS pilots/operators | - UTM system  
- UTM service provider  
- ATM system(s) |
| Meteo information | Meteo information should be shared to be used in the UTM system to provide UTM services for the UAS pilots/operators. | - UTM system  
- UTM service provider  
- Meteo sensors |
| Spatial information | Spatial information should be shared to be used in the UTM system to provide UTM services for the UAS pilots/operators. | - UTM system  
- UTM service provider  
- Spatial data infrastructure |
| Surveillance information | Surveillance information of cooperative and non-cooperative traffic should be provided, in order to build a complete situational awareness of UAS positioning. | - UTM system  
- UTM service provider  
- Surveillance sensors |
| Privacy feedback | Information to protect privacy of people shall be shared by, and with, the UTM system. | - UTM system  
- UTM service provider  
- Public user |
Appendix 5 - Guiding Principles for Cloud

The proposed solution should adhere to the following principles

1. Stateless vs Stateful

While designing the application on cloud, the MSP should make sure that the application built are stateless application. While the MSP should ensure that only stateless application are present but if there is a need to have a stateful component for storing of session details the state should be stored in a NoSQL/SQL/In-Memory database available on the cloud platform.

The storing of state on HTTP cookies should be prevented as HTTP cookies can be tampered with at the client side and these are required to be transmitted with every request which can increase the size of the payload and result in unnecessary latency. For storing large state components other shared storage layer should be used.

If at all, there is a requirement for client devices to be connected to a single compute (the design should prevent this), sticky sessions, “session affinity” should be utilized at the load balancer level.

2. Scalability

A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system. To the extent possible for Web and App, scale out or scale horizontal architecture should be utilized, where, depending upon the increase of load another instance should be spawned at run-time.

The MSP has to decide and explain whether they would be deploying the application on a container or an OS instance and accordingly should handle the scalability.

3. IaaS/PaaS

The MSP can size the solution on an Infrastructure as a Service(IaaS) Model or Platform as a Service Model(PaaS) or a combination of IaaS and PaaS. IaaS and PaaS are defined as below:

**Infrastructure as a Service Model** the CSP would provide infrastructure up till the Virtualization layer along with administering them and MSP providing and administering infrastructure from Operating System and above. The Operating System in IaaS can also be provided by the CSP.
Platform as a Service (PaaS) The CSP would provide and administer infrastructure stack up till Runtime with MSP Providing and Managing layers above it.

<table>
<thead>
<tr>
<th>Infrastructure As a Service</th>
<th>Platform As a Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>OS</td>
<td>OS</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>

Division of Responsibility between the CSP and the MSP

Please note that containers based solution can also be provided on either IaaS or a PaaS model or a mix of IaaS and PaaS. Container Orchestration Solution would also need to be provisioned to manage the containers

4. On Demand Vs Fixed Billing Instances

One of the advantage that Public Cloud offers is that there is no need to size the resources in advance and can be provisioned on demand as per the requirement. The cloud should offer both on-demand and fixed-billing (paying upfront for a determined usage) instances.

The MSP should do a proper profiling of all the services and should determine what would make more economic sense: on-Demand or Fixed-Billing services.

Typically, the workloads which are slated to run 24x7 should run on Fixed-Billing instances and other instances should run on on-demand instances. However, the MSP should also keep in account the duration of the project and accordingly select the tenure of the fixed billing period. Care should also be taken while sizing during the first 4-6 months of the project implementation where many of the services can change basis customer feedback and hence “on-demand” service should be utilized during this period.
However from AAI/DGCA perspective, the billing would be done quarterly irrespective of Fixed/On-Demand model with the Cloud Service Provider.

5. Microservices Architecture

Microservices architecture is an architecture style that structures an application as a collection of loosely coupled services which enables continuous delivery/deployment of large complex application. IT should be designed to reduce interdependencies so that failure in one component of the system should not affect other components and each and every component should be independently deployable in case of change without deploying the entire application. Microservices architecture is recommended when there are many consumers of atomic unit of functionality. When there is one consumer of tightly-coupled functionality, microservices add overhead without any benefit.

The architecture should adhere to the following:

1. Use of technology agnostic services like REST for the communication between various components.
2. IP addresses should not be hardcoded and should be discovered using a service discovery service.
3. Wherever it is deemed fit use of asynchronous integration services available on the cloud should be utilized.
4. The component failure should be handled in a graceful way.

6. Interoperability

The MSP should make sure that there is no vendor lock-in with the underlying Public Cloud provider and should devise a framework to evaluate how much is the cloud version interoperable with any other cloud and how easy would it be for DGCA/AAI to port their applications and their data and bring to another cloud or back to on-premise data center. The following factors should be part of the framework:

<table>
<thead>
<tr>
<th>Interoperability</th>
<th>Portability between providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Migration into/out of the cloud to Cloud/On-premise</td>
<td>a. Service portability</td>
</tr>
<tr>
<td>b. Ability to integrate into on-premise IT</td>
<td>b. Data portability</td>
</tr>
<tr>
<td>c. Cloud federation</td>
<td></td>
</tr>
</tbody>
</table>
7. Backup & Disaster Recovery

Data and information are resources that are extremely valuable for the organization; hence data management processes must be in place to maintain the data.

While it is important to transform Storage, it is also more important to ensure all the services are getting properly backed up. For the same, it is important to establish proper policies, by assessing and analyzing the environment and ensuring that the data for which backup is not required is either purged or archived depending upon criticality of data. On cloud, the MSP should ensure either from a SaaS based solution/ Backup Softwares deployed on Cloud VMs managed by MSP or native cloud provider solution that services are backed up.

It is important to have a DR site where the services can failover in case of a disaster and business can continue. Keeping in mind that a modern cloud is to be built which has to be future ready and at the same time should ensure that at time of disaster all the services fail over within RTOs and RPOs defined. The DR should also be available as a service from the cloud service provider. The MSP should make sure that storage replication is taken care of either through a SaaS based software/Software Deployed on Cloud VM managed by MSP or native cloud based data replication service For the compute, depending on the RTO, criticality and architecture instances should be sized on the DR site.

8. Database

The MSP should also do a detailed study and advice on the type of databases to be used for each component (SQL or NoSQL). Each of the database has a specific use case and accordingly each might be utilized. The database instances can be provisioned as a Database as a Service or on IaaS basis with high availability ensured. In case of SQL, it should be provisioned preferably in two separate zones/fault domains/update domains/PODS with synchronous replication to ensure that in case of failure of even a zone/fault domain/update domains/PODS, there is no Data loss and service can be provisioned instantly from the other zones/fault domains/PODS.

The MSP should make sure that storage replication is taken care of either through a SaaS based software/Software Deployed on Cloud VM managed by MSP or native cloud based data replication service.

For SQL (Relational) databases, the MSP should also design the data model of the application with partitioning where the logical data elements should breakup into multiple entities to have more availability, performance and maintainability.

Horizontal partitioning (or Sharding) is preferable where replica of the schema is created and division of data is stored on each shard basis shard key.

9. High Availability

All production, UAT instances should be highly available.

Development instances are not required to be highly available.

However, for the purpose of sizing Production, UAT and Development environment should be sized relative to the number of users. If such figures are not available, all UAT instances should
be sized at 20% of the production instance and should be in High availability. All Development instance should be sized at 10% of the Production instance size and are not required to be in High Availability.

For sizing of DR, MSP should ensure that the DR should be available at time of disaster at DC within defined RTOs and RPOs. MSP should size DR environment in order to meet the RPO and RTO and SLA. In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.

10. **DevOps framework**

The MSP should ensure that for application and infrastructure release deployment DevOps framework should be utilized. Tools for Continuous integration of changes, Continuous Deployment, Automated testing of the deployed changes, and ensuring zero or minimal downtime, code versioning should be utilized wherever necessary.
## APPENDIX 6: Digital Sky Cloud Services Requirements

### 1.1 General Requirements

1. The MSP should architect an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) or both IaaS and PaaS on Virtual Private Cloud (VPC) /Government Community Cloud (GCC) deployment model (As per MEITY) of a MEITY Empaneled Cloud Service Provider. In case of GCC model also, Digital Sky application and infrastructure stack should be logically segregated from the other Government clients.

2. MSP shall assess the infrastructure requirements (including OS Instances, Storage, Networking, Security etc.) for hosting and maintaining all required applications/services. The MSP shall provide the services in conformance with the SLAs as described in the RFP.

3. The MSP should ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.

4. AAI will not be responsible if the MSP has not provisioned some components, sub components, assemblies, and sub-assemblies as part of bill of material in the bid. The MSP will have to provision the same to meet the solution requirements at no additional cost and time implications to AAI.

5. The Virtual Private Cloud services of the CSP should be available on pay as per usage model and Fixed-Billing model and should be sized by MSP basis the Guiding principles of IT infrastructure design section (On-Demand vs Fixed Billing). However from AAI perspective, the billing would be done quarterly irrespective of Fixed/On-Demand model with the Cloud Service Provider.

6. The MSP should use Open Source Solution (Enterprise Edition) for any application software that MSP would be deploying on Virtual Private Cloud/ Government Community Cloud of CSP. In case there is a need to purchase COTS (Commercial-off-the-Shelf) license, the same should be flagged and justified; additionally, any purchase of any license or support should be in the name of AAI or its nominated government agency.

7. The CSP should specify DC and DR locations. AAI may, at any point of time, require audit of the provisioned DC / DR environment; MSP/CSP is required to facilitate such timely audits.

8. Digital Sky Solution and Cloud services should be accessible via internet

9. DC & DR should be provided by the same CSP.

10. The solution should have ability to automatically provision services via a Web Portal (Self Provisioning), provide metering and billing to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota and show-back information is essential for the virtual private cloud platform to be offered.
### General Requirements

11. MSP, in alliance with the CSP, should ensure seamless migration in case the underlying processor architecture is upgraded.

12. The Virtual Private Cloud Services/Government Community Cloud Services of CSP should provide data migration services (both egress and ingress).

13. It is expected that the MSP will provide an integrated solution, after due consideration to the compatibility issues between various components. If there is a problem with compatibility between components, the MSP should replace the components with an equivalent or better component (that is acceptable to AAI) at no additional cost to AAI and without any project delays.

14. The Virtual Private Cloud Services of CSP should provide REST based API for each of the services for automation along with SDKs for platforms like Microsoft .net, Java/JavaScript, Python, PHP or Ruby. The MSP should be able to utilize these API's to set up routine jobs such as backup on an automated schedule wherever necessary.

   The Virtual Private Cloud Services of CSP should also provide API Gateway services to create, host, monitor API services that may be required as part of the solution.

### Policy Requirements

1. The MSP/CSP should confirm that data will reside in India and should not be accessed by any entity outside the control of AAI.

2. The “Digital Sky Data” and “Virtual Private Cloud Services/Government Community Cloud Services of CSP Infrastructure” must be maintained ONLY at the declared hosting site of CSP which should be communicated as part of the solution document.

3. The CSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of the Government Department.
### 1.3 Logical Partitions

1. All the applications would follow a three-tier architecture with clear separation of database tier/layer from application and web layers. For micro services based architecture, MSP should deploy Presentation, Logic and Database category of micro services on different VM's/Containers.

2. The Web layer for applications accessed via Internet shall be hosted in the DMZ zone/Subnet; the application layer should be hosted in the Militarized Zone or a separate subnet.

3. The Database nodes (RDBMS) should be in a separate zone with higher security.

4. All management servers which are not directly accessible through the internet will be kept in Management Zone. Active directory, Different modules of Enterprise Management Servers (including network, server, database, helpdesk etc), Single-Sign-On, access and identity management server, Security Operations Centre, etc., will be a part of this management layer.

5. There will be separate VLANs/Subnets created for various environment as per RFP to segregate development and testing traffics from the production. Appropriate firewall policies can be implemented to have further security between different zones.

6. For the purpose of sizing, the MSP would size the solution on various environments listed in Tender document – Scope of work. Please refer to “High Availability” Guiding principle for sizing guidelines. Those guidelines should be used for sizing and pricing the solution. However, the solution should be scalable and sized on cloud knowing that these guidelines can change in the future depending upon the requirement.

### 1.4 Configuration

1. Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput and hence once provisioned it should be possible to configure the IOs.

2. The CSP should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

3. The MSP shall ensure that identity solution are utilized and use best practices like least privilege, changing of passwords regularly, enable Multi Factor Authentication for Privileged user or for Secure Delete are utilized.
4. Cloud service should support parameterization for specific configuration.

## 1.5 Services

1. The CSP should own and offer services like Database as a service, DNS, Data warehouse Analytics, Message queuing; such services is preferred to be managed from a single console.

2. The MSP/CSP should offer support at any time, 24 hours a day, 7 days a week, and 365 days per year via phone, chat, and email.

3. The CSP should provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud.

4. Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines.

5. Provide Audit logs of the account activity to enable security analysis, resource change tracking, and compliance auditing.

6. Provide data migration services either with the help of a Cloud Native or SaaS/Third Party Software Deployed on VM solution for moving data of all types and sizes into and out of cloud.
## 1.6 Compute

1. The system must be Scalable, Reliable, Highly Available & should provision to upgrade/downgrade virtual machine configuration (vCPU, vRAM, storage) parameters seamlessly based on demand with zero downtime (Using architectural patterns such as rolling or blue/green deployment).

2. The IaaS/PaaS service should have the ability to Auto-Scale (Horizontal) on demand. The service should support automatically launching or terminating instances based on parameters such as CPU utilization or other factors basis the demand. The solution should also be able to do continuous monitoring and optimization of auto-scaling rules and limits. The Cloud service should have self-service provisioning where there is zero dependency on CSP and MSP should be able to provision the service in an agile manner without any intervention from CSP.

3. Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.

4. The MSP shall ensure that the database layer for the applications in production shall be deployed in N+N High availability mode. The Web and Application layer for the applications in production shall be deployed in N+1 high availability mode (Active-Active). However the choice of Active-Active at Application layer is upon the MSP.

5. The MSP shall ensure that the services that are deployed on partitions/virtual images and are required in cluster and/or load-balancing mode, shall be deployed in such a manner that the load sharing/failover is across the OS instances and NOT amongst partitions of the same OS instance. In case of a hardware or software component failure in one partition, other partitions must not be shut down or rebooted.

6. Please remark on the core: vCPU ratio that would be used while giving out the VMs

7. Please confirm that for production instances no burstable vCPU /shared vCPU would be used

## 1.7 Networking

1. Cloud service should entail use of Virtual Private cloud which would ensure logical isolation of the infrastructure.

2. Cloud service should be able to support multiple (primary and additional) network interfaces. Cloud service should be able to support multiple IP addresses per instance.

3. Cloud service/MSP should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
### 1.7 Networking

4. The CSP should provide mechanisms to establish private connectivity between the cloud environment and a stakeholder data center, office, or colocation environment. In case of Digital Sky,

   a) the MSP would provide site-site VPN to Digi Sky Offices, (IPSec)
   b) for work from home users, Point to Site VPN should also be provided.

   For MSP team for Operations management only site-site VPN(IPSec) should be provisioned.

5. Cloud service should support capabilities such as single root I/O virtualization for the isolation of PCI Express resources for manageability and higher performance.

6. Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.

7. The CSP must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.

8. Cloud service should support a Hardware/Software based VPN connection from the cloud DC/DR to DIGITAL SKY office & MSP premises.

9. Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.

10. Cloud service should support Load balancing (both local and Global) of instances across multiple host servers.

11. Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.

12. Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.

13. Cloud service should support an internal load balancer that routes traffic to instances within private subnets.

14. The CSP should be able to provide a 10Gbps network connectivity between the server if required.

15. The internet bandwidth shall be clean with DDOS protection and active monitoring to be provided by the ISP or by the CSP.

16. The Virtual Private Cloud /Government Community Cloud Services of CSP should have the following service available
   - IPv4, IPv6
## 1.7 Networking

- DHCP
- Ipsec VPN Tunnel Creation
- SSL VPN
- DNS services
- Geo load Balancer (Balancing between multiple sites).
- L4 and L7 Load Balancer.
- At least L3,4,6,7 Anti-DDoS solution

## 1.8 Storage

### 1.8.1 Block

1. The CSP should offer block storage volumes greater than 1 TB in size.

2. Cloud compute service should support local storage for transient block storage requirements.

3. Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies. There should be an option to choose the media type with respect to the type of environment. All production instances storage should be SSD backed. Other environments need not be on SSD.

4. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

### 1.8.2 Object

1. The CSP should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data on demand.

2. The CSP should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.

3. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).
### 1.8.2 Object

4. Cloud Service should support lifecycle management configuration

5. The place where the objects would be stored should be configurable and all objects should stay in India.

6. Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).

7. Cloud service should be able to provide audit logs on object storage buckets/ container which should include details about access request and error code.

### 1.8.3 File Storage

1. The CSP should offer a simple scalable file storage service to use with compute instances in the cloud.

2. Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS/SMB connections.

3. Cloud service should support scalable IOPS and throughput performance at any scale.

4. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

### 1.9 Backup

1. The CSP should offer a service with ability to take regular and scheduled backup.

2. The MSP should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.

3. Low cost Object Storage should be utilized as the backup target. If there is need to use the block based storage for backup target for staging or as a whole, the same should be flagged and explained.
1.9 Backup

4. The MSP/CSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications

- An Initial Full Backup
- Daily Incremental with 15 days retention
- Weekly full with 30 days retention
- Monthly Full with 30 days retention on Object Storage and 12 months retention on Long Term storage
- Yearly Full with 30 days retention on Object storage and 7 Years retention on Long term storage
- For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
- Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Digital Sky that require such a service.
- Different Tiers of Backup storage should be chosen depending upon the reads/restore that would be required
- Restoration Policies:
  - Backups taken in last 2 months: Once in a month
  - Backups taken in last 6 months: Once in a Quarter
  - Backups taken in last 1 Year: Once in Half Year
  - The restoration would be performed on a random basis and would be done against a ticket logged in the ITSM tool.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Backup Type</th>
<th>Backup Frequency</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Object Storage</td>
</tr>
<tr>
<td>1</td>
<td>Daily Backup</td>
<td>Daily Incremental</td>
<td>15 days</td>
</tr>
<tr>
<td>2</td>
<td>Weekly Backups</td>
<td>Weekly Full</td>
<td>30 days</td>
</tr>
<tr>
<td>3</td>
<td>Monthly Backup</td>
<td>Monthly Full</td>
<td>30 days</td>
</tr>
<tr>
<td>4</td>
<td>Yearly Backup</td>
<td>Yearly Full</td>
<td>30 days</td>
</tr>
</tbody>
</table>

5. Any data requested from Long Term Storage should be retrievable within a time span of 12 hours.

6. The Long Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.

7. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).
1.11 Security Guidelines

1. The Virtual Private Cloud Services of the CSP shall be fully secure with no scope of data breach/leaks/thefts/data mining/privacy breach etc. It would be MSP responsibility that for the layers where MSP is managing (For example, for the layers, OS and above in case of IaaS or Data and above in case of PaaS) all the relevant security layers are deployed. MSP should also ensure that CSP is also fulfilling all its responsibility (for the layers, OS and above in case of IaaS or Data and above in case of PaaS. Refer Section 4 in Scope of Work - Appendix 5 - Digital Sky - Cloud Service - Guiding Principle for Cloud).

2. The security services / tools should be dedicated (virtual / physical) to the Digital Sky solution

3. The MSP shall be responsible for ensuring security of Digital Sky applications and infrastructure from any threats and vulnerabilities. The MSP shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules.
### 1.11 Security Guidelines

4. The CSP should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.

5. Cloud service should offer a secure way to login (like public and private keys) and should have audit details which should tell about the keys last use details support reporting a user’s access keys last use details.

6. Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.

7. Cloud service should support a policy validator to automatically examine non-compliant access control policies.

8. Cloud service should support features such as user and group management.

9. Cloud service should allow users to reset their password in a self-service manner.

10. The CSP should offer dedicated HSM modules. A hardware security module (HSM) is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware module.

The CSP should offer a service to create and control the encryption keys used to encrypt user data.

11. Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 or equivalent cryptographic algorithm. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

12. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.

13. Cloud Service should also provide for Database Activity Monitoring

14. The MSP shall be responsible for ensuring security of Digital Sky applications and infrastructure from any threats and vulnerabilities. The MSP shall provision and monitor the following security layers

   - Layer 4 Firewall
   - Layer 7 Firewall (WAF)
   - Intrusion prevention/ detection (Network and Host level)
   - Content filtering and blocking
   - Virus protection
   - Event logging & correlation
### 1.11 Security Guidelines

- Vulnerability protection through implementation of proper patches and rules.
- Vulnerability Assessment and Penetration testing before go-live of any module
- Database Activity Monitoring
- Hardware Security Module
- 2 Factor Authentication
- Web Gateway with Content Filtering and Proxy Solution
- Anti-Advanced Persistent Threat
- Anti-DDoS
- Anti-Virus
- Data Leakage Prevention
- SSL VPN
- Email Gateway
- Privilege Identity Management
### 1.12 Data Security & Information Lifecycle Management

1. Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

2. Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

3. Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:
   - Established policies and procedures
   - Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance
   - Compliance with legal, statutory, and regulatory compliance obligations
### 1.13 Identity and Access Management

1. The Virtual Private Cloud/Government Community Cloud Services of CSP should provide Identity and Access Management service for the layer managed by CSP and MSP should bring in identity and access management solution (3rd Party or Cloud Native) for the layer that would be managed by them. (For example, for the layers, OS and above in case of IaaS or Data and above in case of PaaS, MSP should bring in respective tools). The solution should ensure that features like Multi-factor Authentication (Physical token based or Virtual Token Based), enforceable password policies, defining of roles both for resources and users, federation capabilities with other 3rd party Directory Services are present.

2. User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components.

3. Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.
### 1.14 Incident Response

1. The MSP/CSP should have policies and procedures in place for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The MSP/CSP must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures.

2. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.

3. The MSP must bring in an ITSM tool through which the tickets can be logged in.

4. The MSP/CSP should have proper forensic procedures defined and implemented, including chain of custody, required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.

5. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

### 1.15 Governance & Risk Assessment

1. The MSP/CSP should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.

2. Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.

3. Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.

4. Solution shall have an audit and compliance features which enables the Client agency to monitor the provisioned resources, performance, resource utilization, and security compliance. It shall have the following functionalities:
5. The solution should have automated security assessment service that should provide the following: a. vulnerabilities assessment services b. Penetration Testing services c. deviations from best practices such as password policy, unnecessary opened firewall ports, storage access policy, suggestion of data to archive

6. The system should have ability to set up alarms basis resource usage and the ability to define actions on triggering of those alarms(For example, ability to send an email when storage utilization has crossed x% or archive a storage section depending upon data type when it has crossed x% utilization)

7. Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.

8. The solution should provide a dashboard that would list the details of any planned maintenance scheduled as well as any unplanned downtime faced in the recent past(past 3 months at least).

9. MSP/ CSP should provide dashboard for monitoring RPO and RTO of each application and database. The Dashboard should clearly show data replication process and any lag/ failure in data replication that should be notified through alerts to respective authorities.

10. The solution should be able to log all account and resource access into the account and resources (which might be resources logging into the account using API call or root/admin users or other users logging into the account).

11. The solution should be able to discover all provisioned resources in the Virtual Private Cloud Services/Government Community Cloud of the CSP and provide details such as configuration items inventory, history of changes to such configuration items, snapshot of resource inventory at a single point in past, set-up of policies to track provision of resources within a client defined rulesets and auto - notifications each time a configuration changes

12. The solution should be able to suggest best practices to optimize overall cost of resources.

**1.16 Compliance**

1. The MSP/CSP should understand and incorporate the different types of laws and regulations that impose security and privacy obligations on the organization. Especially those pertaining to data location, privacy and security controls, records management and electronic discovery requirements.

2. The MSP/CSP should ensure that independent reviews and assessments are conducted at least annually to ensure that the organization addresses nonconformities with the established policies, standards, procedures, and compliance obligations.
### 1.17 Business Continuity Planning

1. MSP shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning”; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.

2. The CSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.

3. The CSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.

4. Incident response plans should be developed by the CSP which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

### 1.18 Monitoring Solution

1. DIGITAL SKY intends to monitor operational activities to have a holistic view of the provisioned cloud services and their configurations to ascertain required features have been appropriately implemented. In this view, the MSP shall provision monitoring tools (third party or cloud native) for measuring the service levels and application/server/storage/network performance & utilization. Basis the inputs of Monitoring Solution, the cloud services should be configurable with auto-change in provisioned resources as per the monitoring inputs.

2. The monitoring tool should publish (on portal) real-time status (of all the services) that is refreshed with at least 5 min frequency; further, the tool should publish all historical parameters for a period of minimum 3 months. The tool shall be capable of generating per day/month/quarter utilization reports.

3. The Monitoring System should have the following components:

   a) Cloud Dashboards: Collect and track metrics, collect and monitor log files, and set alarms to gain system-wide visibility into resource utilisation, application performance, and operational health. Overall, monitoring platform should provide End to End monitoring of complete IT Infrastructure

      - Server Monitoring: Should monitor heterogeneous operating systems for both dedicated & virtual instances on CSP OS layer including (but not limited to) Windows 32/64 bit, all major flavours of Linux, etc.
1.18 Monitoring Solution

- Application Monitoring: To perform infrastructure aware application triage, i.e. pinpoint network issues causing application degradation. The MSP should also deploy polling tools at the end user site/DIGITAL SKY offices to measure performance SLAs (with Synthetic User Monitoring and Real User Monitoring).

- Database Monitoring: Monitor multiple database servers and versions being proposed on each server

- Storage Monitoring: Monitor IOPS, Latency etc.

- Network Monitoring: Should provide capability to monitor any device based on SNMP v1, v2c & 3

- SLA Monitoring: Support Service Level Agreements, Lifecycle Management including Version Control, Status Control and Audit Trail

  b) Audit Trail: Provide logs of all user activity. The recorded information should include (but not limited to) identity/source IP of API caller, time of API call, the request parameters, and the response elements.

  c) Security Compliance: Monitors cloud resources and provides alerts in regards to security gaps such as overly permissive access to certain ports, minimal use of role segregation using IAM, and weak password policies.

  d) Configuration Management: Discovery of configuration items and their relationships and generate detailed, predefined custom report of configuration items and their configuration

  e) Systems Manager: Provides a unified user interface to view operational data and automate operational tasks across cloud resources.

  f) Personal Health Dashboard: Provides a personalised view into the performance and availability of the services customers are using, as well as alerts that are automatically triggered by changes in the health of those services.

  g) End User Experience Monitoring: To measure end users’ experiences based on transactions without the need to install agents on user desktops.

  h) Asset Management: To keep track of licences life cycle from procurement to disposal and auto discovery and management of software inventory deployed on network.

4. Dashboard for views for all the above monitoring layers and can provide proactive notifications and alerts on actions that should be taken to prevent a failure

5. The department may insist on the following regular reporting during the contract:

  a. Availability of the cloud services being used
1.18 Monitoring Solution

b. Summary of event-based alerts, providing proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources

c. Reports providing system-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources

d. Auto-scaling rules and limits

e. Report of all of the provisioned resources and view the configuration of each.

f. Summary of notifications, triggered each time a configuration changes

g. Incident Analysis in case of any un-authorized configuration changes.

h. Summary of alerts with respect to security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies

i. Summary of security assessment report that identifies the possible improvements (prioritized by the severity) to the security and compliance of applications deployed on cloud

j. Report on upcoming planned changes to provisioning, either possible optimizations, if any, indicating how the underutilized services can be reduced to optimize the overall spend, or required enhancements (e.g., upgrade to additional storage) to meet the service levels defined in the RFP.

6. The User / Admin Portal (User Profile Management, Trouble Management) should also be part of the solution.
### Parameters

1. The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface.

2. The web interface console would also offer power-users tips.

3. The proposed helpdesk solution must provide seamless integration to log incident automatically via system and network management.

4. The proposed helpdesk solution must provide classification to differentiate requests basis priority/severity to address the most critical ones first.

5. The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.

6. Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming.

7. The escalation policy would allow flexibility of associating with different criteria like device/ asset/ system, category of incident, priority level, organization and contact.

8. The proposed helpdesk solution must provide web-based knowledge database to store useful history incident resolution.

9. The proposed helpdesk solution must have a strong Business Objects based reporting module built in it.

10. The proposed helpdesk solution must integrate with monitoring, event management and support automatic problem registration, based on predefined policies.

11. The proposed helpdesk solution must be able to log and escalate user interactions and requests.

12. The proposed helpdesk solution must provide status of registered calls to end-users over email and through web.

13. The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

14. The proposed helpdesk solution must have the ability to track work history of calls to facilitate troubleshooting.

15. The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.

16. The proposed helpdesk solution must support request management, problem management, configuration management and change order management.

17. The proposed helpdesk solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.

18. Knowledge tools and Configuration Management Data Base (CMDB) should be integral built-in components of Helpdesk and should be accessible from the same login window to enable seamless access.

19. The proposed helpdesk solution must allow the IT team to see the Configuration Items (CI) relationships in pictorial format, with a specified number of relationships on single window.

20. Workflow must provide the ability of being Non-linear workflow with decision based branching and the ability to perform parallel processing. It should also have a graphical workflow designer with drag & drop feature for workflow creation and updation.
APPENDIX 7 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>21. The proposed helpdesk solution must have an integrated CMDB for better configuration management &amp; change management process. CMDB should have been able to scale as per the requirements of the project for creation of CI families, CI Classes and CI Relationship Types out of the box. Both helpdesk &amp; CMDB should have same login window for seamless access.</td>
</tr>
<tr>
<td>22. The proposed helpdesk solution must have a top management dashboard for viewing the helpdesk KPI in graph &amp; chart formats.</td>
</tr>
<tr>
<td>23. The proposed helpdesk solution must support remote management for end-user &amp; allow analysts to do the desktop sharing for any system located anywhere, just connected to internet/intranet.</td>
</tr>
<tr>
<td>24. The proposed helpdesk solution must allow IT teams to create solution &amp; make them available on the end – user login window for the most common requests.</td>
</tr>
<tr>
<td>25. The proposed helpdesk solution should be able to integrate with the CSP helpdesk solution and should provide one unified portal to the user</td>
</tr>
<tr>
<td>26. The proposed helpdesk should also offer a Knowledge Management portal where frequently logged tickets and their solution would be mentioned</td>
</tr>
</tbody>
</table>
Annexure 8: Digital Sky Technology Architecture

To overcome the challenges of approval and compliance to be undertaken by the stakeholders, Digital Sky has been conceptualized to be a one-stop approval/compliance platform for stakeholders related to Drones usage in India. The platform has been conceptualized to minimize human interventions in the process for approval/compliance related to Drones.

This section focuses on how the Digital Sky solution architecture should look like. The contents of the section are logically structured so as to make enhancements to this section as and when there is opportunity, based on additional learning, to mature it to the higher level. The section provides the expected technical architecture of Digital Sky system. It was necessary to orient the section based on adopted international standards. The Open Group Architecture Framework (TOGAF®) is a framework for enterprise architecture, which provides a comprehensive approach for designing, planning, implementation, and governance of enterprise information architecture. This section has been structured taking inspiration from publicly available information about the framework.

1.1.1 Design Considerations

Digital Sky system shall be built following the below design considerations:

1.1.1.1 Ecosystem Approach

The motive of the technological enhancements is to integrate all the key stakeholders and bring them to a common platform so as to work in prefect synchronization with each other. The key stakeholders in this computerization effort have been highlighted in the RFP. Stakeholders will interface with Digital Sky System via portal or via mobile app provided applications for activities such as registration, flight approvals, post flight data sharing, etc.

1.1.1.2 Continuous adoption of rapidly evolving Technology

Technology evolves too fast and projects similar to Digital Sky with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changes, new RFP (Request for Proposal), etc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment.

1.1.1.3 Provision of a Sustainable, Scalable Solution

The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 10 years from Go-Live. The solution would be done keeping in mind the scalability of the system. The simplified approval processes related to Drones application and ease of compliance is expected to lead to huge growth in contract’s base. Every component of Digital Sky System needs to scale horizontally to very large volume of data.
1.1.1.4 Distributed Access and Multi-channel service delivery

With High penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that all e-Gov applications provide multiple channels of service delivery to constituents. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that an ecosystem of integrated apps also evolves. One of the design considerations is to provide multiple channels/interfaces to stakeholder to interact with Digital Sky System. The aim is to reduce load on portal layer.

1.1.1.5 API Approach and Use of India Stack

The aim of the project is to reuse the already built in API components which are available free with GOI such as India Stack. India Stack is a complete set of API for developers and includes the Aadhaar for Authentication (Aadhaar already covers over 940 million people and will quickly cover the population of the entire nation), e-KYC documents (safe deposit locker for issue, storage and use of documents), e-Sign (Digital Signature/ e-Sign acceptable under the laws), unified payment interface (for financial transactions) and privacy-protected data sharing within the stack of API.

1.1.1.6 Security & Privacy

Security and privacy of data should be fundamental in design of the system without sacrificing utility of the state procurement system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.

1.1.1.7 Business Rule Driven Approach

All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior.

Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.

There should be a central interface for managing the configurability by authorized user group.

1.1.1.8 SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the organization and provide timely analysis of data as well as
monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

1.1.1.9 Data Distribution Service

As a future roadmap, it is envisaged that the functionalities provided by the Digital Sky 2.0 system should allow for value adds by industry overall on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers).

1.1.2 Guiding Architectural Principles

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

The overall system will be build based of the following architectural principles which will be the backbone of the overall system architecture:
Digital Sky system would be built on the following core principles:

1.1.2.1 Platform Approach

The Digital Sky system is envisaged as a faceless system with 100% API driven architecture at the core of it. Digital Sky portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing stakeholder and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

1.1.2.2 Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

a) Modular design to distribute the appropriate system functions on web and app server
b) Increase in-memory Operations (use static operations)
c) Reduce number of I/O operations and N/w calls using selective caching
d) Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.

1.1.2.3 Preference to Open Source & Vendor Neutrality

While proposing a solution major emphasis has been given to Open Source Software. While finalizing the solution architecture for Digital Sky system, policy of Government of India on adoption of open source software issued by MeitY vide F. No. 1(3)/2014-EG II has been considered. Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/MSP pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.
1.1.2.4 Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

a) The application functions to be divided logically and developed as Modular solution.

b) The system should be able to scale horizontally & vertically.

c) **User Base estimated volume—**

   a. 10 lacs active UIN (active registered drones). Estimated current volume is 40,000 drones. Please note that estimated active UIN means that at a given time, the number of active drones is not estimated to cross this number. This is with view that drones have short lifespan and hence, a number of drones is the duration shall also be retiring (leading to reduction in active UIN) while new drones shall be registering (leading to increase in number of active UIN)

   b. 5 lac pilots in the duration of the contract

   c. 1000 manufacturers in the duration of the contract

   d. 1 lac drones operators in the duration of the contract

d) **Data Volume** – Ability to support projected volume growth in content post system implementation & content migration.

e) **Functionality** – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.

Scalability could be achieved by adhering to the following architectural principles

a) Loose coupling through layered modular design and messaging

The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more services are provided through the Digital Sky System. Each of the logical layers would be loosely coupled with its adjacent layers

b) Data partitioning and parallel processing

c) Horizontal scale for compute, Network and storage
1.1.2.5 Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system will ensure data confidentiality and data integrity.

The application system should have the following

a) Data security policies and standards to be developed and adopted across the departments and systems

b) In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.

c) Role based access for all the stake holders envisaged to access and use the system

d) Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.

e) Ability to adopt other authentication mechanism such as Electronic Signature Certificates

f) Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized

g) Data should be visible only to the authorized entity

h) Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided. (E.g. Logging of IP Address etc.)

i) Data alterations etc. through unauthorized channel should be prevented.

j) Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

1.1.2.6 Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following
a) Prevent processing of duplicate incoming files /data

b) Unauthorized alteration to the Data uploaded in the Digital Sky system should be prevented

c) Ensure minimum data loss

1.1.2.7 Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using people manually managing it.

1.1.2.8 Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the following availability requirements

a) Load Balanced across two or more Web Server avoiding single point of failure

b) Deployment of multiple application instances should be possible

c) Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.

1.1.2.9 Reconstruction of truth

System should not allow database /system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of invoices and final returns) could be used to reconstruct derived data such as ledgers and system generated returns. System should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.

1.1.3 Architecture Overview

1. The Digital Sky systems architecture consists of the following high-level components:

   a) It is aimed to save data in a single location in their information systems to adhere to the principle of ‘Store once and multiple uses”. This data may then be accessed across the organisation by different departments and for different uses. The aim is to hold a single copy of basic registration information on people, addresses/buildings, land, companies/institutions, etc.).
b) The Digital Sky core system (i.e. system without user interface- Digital Sky portal) is a faceless system consisting of a set of services exposed via APIs for storing and processing all the relevant data. It includes all the business and functional services. It is optimized for reliability, scalability and performance. Other components can access the core system only through its APIs.

c) API Layer: Digital Sky system exposes two sets of distinct APIs, one for consumption by stakeholders via various application interfaces and one for consumption by government agencies. The APIs are RESTful, JSON or XML-based and stateless services. For security reasons, the production API end points should be consumed via MPLS lines or secured VPN. All APIs should be only accessible via HTTPS protocol.

d) The Platform of the IT applications stack contains the Data processing and data mining applications which provide an analytics backbone and trend analysis capability.

e) Digital Sky system landscape also includes a web portal for direct, browser-based access by stakeholder or government employees. The UI and access functionalities for stakeholder and the government authorities should be different. The web portal access the functionality of the system through the exact/same set of APIs as any other external application.

f) In the Digital Sky system landscape the solution should also be available through mobile device.

g) Digital Sky system APIs are meant to be consumed by a variety of applications and platforms, including mobile devices, Drones Equipment, etc.

h) When an organization like DGCA/AAI wish to offer effective and efficient services – whether they are electronic or not to its stakeholders related to Drones, it is important that it has service management capabilities in place. This requirement is highlighted using the concept of a Service Oriented Enterprise (SOE). A holistic view is essential and must be applied from the highest level of management down through the entire organisation.

### 1.1.4 Solution Architecture

The section below shows the solution Architecture of the envisaged Digital Sky application. It includes layer wise different business services, external integration, MIS reporting, analytics workflow implementation, and notification services.

The logical layers identified for the proposed architecture are as follows –

1. Client Layer
2. Presentation Layer
3. Business Layer
4. Data Storage Layer

5. Data Analytics Layer

6. Integration Layer

1. **Client Layer**

This layer represents the users or stakeholders who will be using the Digital Sky system, either collecting information for decision support or viewing reports/dashboards or monitoring operations or submitting data or applying for specific service requests. Besides the front-end users there will be back-end users who will be acting on the service request raised, verify and approve or reject application accordingly. The users are overall listed in the RFP

2. **Presentation Layer**

The presentation layer is catered for the DigSky portal, it encapsulates all presentation logics required to service the users that access the system. This layer intercepts all client http requests, authenticates the users, conducts session management, controls access to business services, constructs the response and delivers the http response back to the client.

As depicted in the above solution architecture diagram, this layer will cater to the following key services –

- MVC Framework Services
- Security Services
- Business Presentation (UI) Services
- Caching Services
- User Personalization & Dashboard Services
- Admin Services
- Report UI Services
- Calendar Services
- Communication Services

a) **MVC Framework Service**

Based on static and dynamic requirements of the presentation services, there can be the client side and server side components in this layer.

i. *Client Components*: These are static components required for rendering the UI pages and include HTML, Java scripts, style sheets, image, icons etc.
II. **Server Component:** These are the dynamic components that are required for processing of client request. Popular MVC framework can be used and leverage the framework’s rich tag libraries and MVC (Model-View-Controller) capability.

b) Portal Services

The DigSky portal is an interface to the end-users for all services in DigSky system (either on the same portal or using sub-domain). Every user needs to pass through strong authentication before serving him his own personal ‘Dashboard’ as home page, the contents of which are dynamically decided based on the accesses permitted to the users. In no case, a user shall be allowed multiple logins from any device(s).

Some of the specifications of the web portal are provided below:

a) UI layer should not have its data

b) The portal should not allow concurrent sessions for same user. The system should automatically log out a customer in case of session breakdowns (e.g., communication failure, high inactivity period - these should be parameterized)

c) The portal should support workflows

d) The portal should implement security features, such as password complexity, automatic blocking (temporary/permanent) of user logins after given number of unsuccessful login attempts (should be parameterized), controlled access to content stored on the portal and logging of security incidents. It should by its own or through an integrated Identity Management solution and should be capable of managing security rights and privileges by individual, group and role.

e) Portal should support HTTPS protocol on Secure Socket Layer (SSL).

f) The portal should support the leading browsers such as Internet Explorer, Firefox, and Chrome etc.

g) The portal should be able to expose /publish functional applications seamlessly

h) The portal should provide search engine with advanced full-text search capabilities. The search engine should be able to search for requests within the portal.

   i. Should provide support for comprehensive audit trail features such as:

   ii. Daily activities log should be merged into the history log files

   iii. Date, time and user-stamped transaction checklist should be on-line generated for different transactions

   iv. All transaction screens should display system information
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

v. Daily activity reports should be provided to highlight all the transactions being processed during the day

vi. Unsuccessful attempts to log-in to the system should be recorded

i) Portal should be compatible to popular mobile devices Operating systems

j) Portal should be interoperable with industry standard databases

k) In addition the portal should provide the following capabilities

i. Should have multilingual capabilities with regional, localization and Unicode support.

ii. Should be able to integrate with common office application

iii. Should authenticate users from Active Directory/LDAP, claim based authentication

iv. Should support virtualization

v. Should support customization of look and feel of the portal

vi. Should support a broad range of standards, preferably open standards. Some examples are DOM 1.0, HTML 5, HTTP, HTTPS, MathML, ODBC, ODF (IS26300), Open XML (IS29500), OpenSearch, OpenType, PDF 1.7, PDF/A, RTF, RSS, ATOM, SOAP, SVG, REST, UDDI, Unicode, URI/URN, W3C XML Schema, WCAG 2.0, WebDAV, WSDL, WSRP, XHTML, XML, XML Web Services, XMLDSig, XPATH, XPS, XSLT

a) Should integrate with standard email services

b) Should integrate with instant messaging services

c) Should integrate with any other portal products through open standards such as HTML, XML, RSS, web services, and WSRP.

d) Should support encryption and compression features

e) Should support multiple roles with associated access controls.

f) Should support upload, store, organize and share documents

g) Should provide multi-channel output capabilities

h) Users should be able to upload documents in multiple formats

i) Users should be able to upload multiple files at the same time

j) Should support version control, change tracking and comments in these documents

   i. Should support document linking capabilities (static, dynamic, and/or other)
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

ii. Should support the import of content into the repository

iii. Should support document and text indexing capabilities

iv. Should support image indexing capabilities

v. Should be able to support to store and manage documents in the same repository

vi. Should Support Managed Metadata

vii. Should support content archiving capabilities

viii. Should provide offline support for forms

ix. Should support creation of ad hoc query by users

x. Upload document will be in XML, CSV and excel. Scanned document will be in PDF and images in JPEG, PNG.

xi. While uploading bulk data it should also tell for errors if it encounters any.

a) Mobility Services

The mobility layer encapsulates the mobile enablement framework, which deals with both rendering the web pages in mobile devices through necessary UI components as well as making available native mobile apps of individual services, developed using native mobile components and data security considerations in latest Android and Apple iOS platforms. The mobile apps will be capable of offline data capture and can be installed and used by all the stakeholders as well as government officials.

Some of the key requirements related to Mobile application, but not limited to, are mentioned below:

i. The Mobile Application should provide an intuitive and user friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.

ii. It should enable ease of configuration and changes to existing GUIs, and support the introduction of new screens.

iii. It should provide on screen tips and online help to aid users while interacting with it.

iv. Should make use of data available in the existing database and reduce duplicate data entry

v. Incorporate analytics into mobile app, to track and identify users experience and actions.

vi. Apps should be easily customizable and easy to Administer data in the DigSky database

vii. Network level security, traffic should be encrypted using secured connectivity
viii. Should structure overall content with proper tagging to make them screen reader friendly.

ix. Application should ensure Compatibility with all platforms such as Android & iOS.

x. Solution should develop resolution independent design structure i.e. Mobile Application should adjust itself automatically as per the screen resolution of the Mobile

xi. Mobile Apps should work flawlessly across different platforms

xii. There should be minimum use flash contents so that home page should be loaded quickly

xiii. It should not occupy excess client’s Mobile RAM.

xiv. Should provide Role Based Access control

xv. Should come with mobile threat prevention and recovery system

xvi. Should support authentication using Digital Signature/ e-Sign

xvii. Should have facility to download and upload files, including eForms, Drones Data Files

b) Security Services

The security service will provide the following security control features -

User Registration & User Profile Management

System Administrators can administer the application security through a web interface that will allow them to register and create user profiles for users who will access the DigSky applications.

User Registration service will allow administrators to perform activities like registration and login features, creation/editing/deletion of user profiles and groups, assigning roles to users, assigning users to groups etc.

User Profile Management Service describes how to customize the self-registration process for creating user accounts, and how users edit their account profiles in the DigSky applications.

User Authentication

Highly configurable web security services provided by the HTTP Server like Apache will be leveraged, which adds a comprehensive set of Web single sign-on services, and extends them further with centralized user provisioning that is available in any open LDAP, version 3-compliant directory service. End users logging on to the system will be authenticated against the user name/password credentials and all documents will be authenticated against Digital Signature/ e-Sign.

In addition, the application server’s underlying authentication provider services for enterprise application security to authenticate user identity can be utilized. Refer to the security architecture section below in this document.
User Authorization

Users, groups, roles and security policies will be defined to prevent unauthorized access to specific DigSky application services. The application server’s underlying authorization provider service can be availed to authorize user access.

a) Business Presentation (UI) Services

These are the presentation services that present the web user interface to the end users to avail the various services offering of the DigSky applications.

These services can make use of forms, style sheets, tiles and tag libraries and the view component of the MVC framework to render the UI page.

b) Caching Services

This service leverages the powerful caching techniques of the underlying application server caching services. The Application Server Web Cache will make use of state-of-the-art caching and compression technologies to optimize portal performance and more efficiently utilize low-cost, existing hardware resources. The built-in workload management features of the application server ensure application reliability and help maintain quality of service under heavy loads. The caching services can be static, dynamic as well as distributed.

c) User Personalization & Dashboard Services

These are presentation layer services that provide user personalization services allowing users to maintain their own specific profiles. Each user will be presented with a centralized dashboard view specific to each user profile that will display key information in a summarized manner and will allow top officials to monitor the status of the department specific service requests and performance as well as the KPIs for the department.

d) Report UI Services

This service will present the user interface to the end users to provide reporting criteria, complex querying and view MIS/Custom/Analytics reports generated by the business layer MIS and Analytics reporting components.

e) Calendar Services

This custom service will provide the Calendar functionality in the DigSky application. This component will be custom built leveraging the MVC framework components. The service will display the date and time of all events scheduled in a standard monthly calendar format.

f) Business Layer

The business layer will manage the DigSky business services for its stakeholders. All business processing for the application will be centralized in this layer. It receives requests from the presentation tier, processes the business logic based on the requests, and mediates access to
the other underlying layer (data access/storage layer or integration layer) resources. Additionally, this layer will handle content management services, database connection management, session management, email and SMS notifications, interfacing with payment gateway and SMS gateway, integration with other Govt. applications and third party solutions.

The following services will be provided by the business layer:

- **Business Services & Service Request Common Components**
- **Workflow & Business Rule Services**
- **Notification & Messaging Services**
- **Payment Services**
- **MIS/Custom Reporting Services**
- **Analytics Tools**
- **Server Administration & Management Services**
- **Support Services**
- **Maps Application**

**Business Services & Service Request Common Components**

These are the DigSky business layer components that will provide the business logic and rules to achieve the desired functionality. It will handle the requests coming from the presentation layer business presentation services and process the business logic based on the request. These services can in turn call common service components, workflow process engines, notification service or content services based on the type of processing requested by the presentation layer. It mediates access to the data access and storage layer to retrieve data from the data store or persist data in the data store.

**Workflow & BPM Services**

The proposed solution architecture will make use of open standard workflow services to cater to the approval/rejection workflow cycle. These workflow services is capable of automating and streamlining business processes. The workflow engine deployed in the business layer will take care of routing approval request to the respective users and decisions triggered the process for completion.

The flexible architecture of the Workflow Services will allow users to model and automate sophisticated business processes. One can define processes that loop, branch into parallel flows and rendezvous, decompose into sub-flows, and branch on task results, time out, and more. Expressing business rules in the process model enables model-driven integration. Workflow Services acting as a system integration hub can apply the business rules
to control and route objects between applications and systems with minimal intrusion into those applications and systems.

Few features (minimum requirements) that should be kept in mind while implementing Workflow Management Framework are:

a) Support easy workflow configuration, its maintenance, and need based modification, addition alteration of the steps.

b) Support process modelling based on BPMN2 notation standard

c) Facility to simulate a process before launching it so that appropriate changes can be made based on findings.

d) Provide business rule engine and a management platform. Users shall be able to modify the business rules online without any need of deployment. System shall also have business rule connector so that it can talk to any 3rd party business rule engine

e) Allow saving custom BPM templates so that end user can tailor a business process based on any of the custom template.

f) Offer performance monitoring features for the business processes. The system shall be capable of identifying, reporting inefficient processes and operations and/or those with high level of error and omission

g) Expose W3C standard web services and REST based web services so that it can communicate to any other technology layer seamlessly.

h) Have capabilities which will enable business activity monitoring and capture audit trail of all transactions as well. Web based dashboard shall be made available for accessing all reports.

i) Provide dashboard view for showing multiple reports. Dashboard view and content can be customized for individuals.

Business Rules

Business rules would be needed in multiple scenarios as highlighted in RFP

- **Notification & Messaging Services**

The Notification Services will let the DigSky application users perform simple email functions, such as view, create and delete messages, automatically create messages as part of the business flow with attachments and reply to or forward an existing mail. It simply enables users to use mail, manually or automatically, in a single collaborative environment. The Notification Services expose data from an existing mail server based on IMAP4 and SMTP protocol.
Notification Services also include services which will send emails & SMS alerts and notifications to the stakeholders based on specific business process event that occurs during the service request life cycle. The flexible architecture of Notification Services will eliminate the pains of implementing features such as polling events, scheduling, formatting and delivery of notifications.

The trigger for sending the SMS can be event-driven as well as time-driven. There are two typical scenarios for SMS communication (i.e. sending and receiving SMS) that will cater to the DigSky functional requirements of (i) alerting users through SMS notification and (ii) receiving SMS request from stakeholders to get service request update information. The SMS application will expose java API to initiate the SMS broadcasting or alert notification.

Following are some of the key requirements for the SMS services through the solution:

i. The gateway must be as per prevailing TRAI/DoT norms

ii. Should contain required details /information and targeted to the applicant or designated officers and other stakeholders

iii. Support automated alerts that allows to set up triggers that will automatically send out reminders

iv. Resend the SMS in case of failure of the message

v. Should be instantaneous with almost no waiting time.

vi. Must have common features like non-acceptance of landline nos., unacceptable mobile nos. etc.

vii. Should Support for Long text messages

viii. The message shall be sent through command line interface/API, Web Interface provided by the Service Provider.

ix. The vendor shall maintain DND controls.

x. Should provide standard reports like success/failure report on current as well as historical/cumulative basis.

It is to be noted that for any activities where mobile application notification can serve the purpose of notification, SMS intimation will not be required to be undertaken for such activities especially related to drones flight approvals.

- Payment Services

The Payment Services will conduct payments for applications by stakeholders. Some of the key features of payment gateway are mentioned below:

a) Should support secure integration with Payment Service Providers
b) Should support a unified interface to integrate with all Payment Service Providers

c) Should support integration with Payment Service Providers using web services over secured protocols such as HTTP/S

d) Should manage messages exchange between UI and payment service providers

e) Should support beneficiary’s payment transactions tracking against various services

f) Should support bank accounts reconciliation

g) Should provide and preserve all logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers

h) Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country

i) Should support redundant Payment Discovery

j) Should submit Periodic Reconciliation Report

k) Should support transaction reports to monitor and track payments

l) Should support real-time online credit card authorization for merchants

m) Should support compliance with emerging trends and multiple payment options such as debit card, credit card, cash cards and other payment mechanisms

n) Should provide fraud screening features, alert mechanism

o) Should support browser based remote administration

p) Should support processing of one-time or recurring transactions using tokenization

q) Should support real-time integration with SMS and emails

r) Should be compliant to standards like PCI DSS

- **MIS/Custom Reporting Services**

Generation of MIS/Custom Reports at various levels is one of the important service requirements of the DigSky application. Considering the various levels and types of reporting services that the monitoring component of the application will have to provide, the proposed solution architecture will make use of open standard reporting framework compatible with the technology platform.

Major features of the reporting tool are as follows:
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

a) It includes JDBC-wrapped data providers for Relational Databases (RDBMS), JavaBeans (EJB, Hibernate), plain old Java objects (POJO), and XML data sources

b) Conditional Parameters can be passed from the web application

c) Parameters would be simple to implement and very powerful, allowing to qualify, restrict, or enhance the data that is delivered to users based on run-time conditions.

d) Pixel-perfect page-oriented or continuous output for web or print

e) Dashboards, tables, crosstabs, charts and gauges

f) Web-based and pixel-perfect reports

g) Report output in PDF, XML, HTML, CSV, XLS, RTF, TXT

h) Sub-reports easily handle highly complex layouts

i) Visual text rotation

j) Drill-through /hypertext links, including support for PDF bookmarks

k) No limit to report size

l) Conditional printing

m) Multiple data sources of multiple kinds in one report

• Analytics Tools

Use of Analytics is considered to be the most important aspect of the DigSky system, in terms of getting intelligent insights out of the streaming data received real-time and theron taking decisions. The system should be perform predictive analysis, operational analysis, risk modelling, statistical analysis for taking informed decisions as highlighted in RFP. The proposed solution architecture will make use of the open standards framework compatible with the technology. Further, the tool should have robust visualizations such as graphs, charts, and histograms for reporting purposes.

i. The reporting tool should have slicing and dicing features facilitating ad-hoc management reporting on the fly.

ii. The reporting tool should have basic statistical modelling properties, so that users can create clusters, regression analysis, and other modelling techniques dynamically.

iii. The reporting tool should output data in various formats.

iv. The Reports generated by the system should be made accessible through API or an interface (for portal) to be viewed by the authorized users. The tool should enable
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

different types of users to perform analysis on data across the Enterprise without the
need to Subset/sample/create multiple views of data. The interface for the authorized
users should be simple with user friendly features such as drop down list, drag and
drop utilities etc., and should be built with focus on users with elementary statistical
knowledge.

v. DBAs and end users to use a web-based portal to evaluate and understand the state
of their system

vi. The management console should be Web based and should not require any client
installation.

vii. The solution shall provide a common management console to monitor multiple
systems in Test, Development, production systems across multiple instances and
across locations

viii. Proposed solution should be capable of seamless integration with leading Office tools
both for import and export of data and reports in multiple formats. The solution should
allow data to be accessed from any industry standard data source using native
connectors. It should also allow data load jobs to be scheduled to automate the
process of loading data into the system for Analysis

ix. Data Visualization tool capable of interactive visualizations. Preference would be
given to tools with auto charting facilities.

x. The analytics and reporting solution should integrate a market leading Data
Visualization tool capable of interactive visualizations. Preference would be given to
tools with auto charting facilities.

xi. Solution should be capable of generating highly formatted, interactive
reports/dashboards with or without parameters. Should also have strong ad hoc report
generating capabilities.

xii. The solution should have the ability to format (page size, row, columns, fonts, colours,
tables etc.), allow data manipulation (slice & dice multidimensional data on the fly,
pivoting, sorting, ranking, rearranging columns, etc.). The solution should have drill-
down capabilities (ability to drill down to various levels of a hierarchy).

xiii. The solution should have the capability of raising exception alarms (e.g. email
notification). Should provide for exception reporting (ability to set certain thresholds).

xiv. The solution should have user friendly GUI to allow easy generation of reports and
exporting capabilities (ability to export resulting data to other applications such as
Excel, Notes, CSV.).
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

xv. The solution should have integration capabilities e.g. ability to integrate in existing portal. The solution should be able to publish all the reports on the portal and have the ability to archive reports.

xvi. The solution should be able to distribute reports and also have the ability to save data for later use or to a local PC/laptop or for other users to view. It should support offline viewing. It should be able to send reports electronically to other users.

xvii. The solution should be able to sort/filter without re-querying.

xviii. The solution should have the ability to schedule reports.

xix. The solution should provide for a browser based interface to view reports.

- **SLA Monitoring, Server Administration & Management Services**

These are the SLA monitoring services, server monitoring & administration services provided by the underlying web and application server container.

**SLA Monitoring**

Designated Solution should be used for SLA Monitoring of servers. SLA solution watches nodes and services that we will specify, alerting admin when things go bad and again when they get better. It also can gather performance and utilization statistics, trending and alerting on thresholds.

**Web Server Load Monitoring**

The system administrator needs to closely monitor the responses of the web servers to make the system highly available. The HTTP Server dashboard should help system administrator monitor the load of HTTP servers.

**Application Server Administration & Monitoring**

Server administration would include a wide range of tasks from creating Server domains, deploying applications, migrating domains from development environments to production environments, monitoring and managing the performance of the run-time system and diagnosing and troubleshooting problems.

System administrators should be able to easily perform all the Server management tasks without having to learn the APIs or the underlying management architecture.

- **Support Services**

These services will provide support functionalities like audit trail, error & exception handling, logging to the business components of the Digital Sky application.

**Audit Trail Services**
There is a design need to verify that transactions in Application are being processed correctly. Audit Trail Services will maintain a historical record of transactions that have been applied to an object or set of objects. The record should contain enough detail to determine how the objects affected by the transactions reached their current state.

Implementation of Audit Trail Services in Application can follow two basic approaches -

a) Using the java artefacts following the Prototype design pattern

b) Using database functionalities like trigger or stored procedures

**Exception, Error Handling & Logging Services**

A robust and reliable application error handling mechanism should be part of the basic infrastructure which will handle normal situation as well as unexpected application error.

Error detection, error handling, propagation of error information and error logging capabilities will be considered to make the application robust.

Logger will be used to log the system debug activities, errors and exceptions with different severity level. All errors would be logged with error code, error level and error message along with timestamp. Log 4j may be used for logging mechanism. It is an open source, popular logging package in Java and allows the developer to control which log statements are output with arbitrary granularity.

- **Data Storage Layer**

This layer is responsible for communicating with external source system and data stores. All access to the underlying DigSky system databases will be through this layer. Typically the business layer is coupled with the data storage layer whenever the business services requires data or services that resides in the Data Storage layer. All DigSky application data access objects will reside in this layer and use JDBC technology to connect to the databases. An Object Relationship Mapping (ORM) framework steps in to fill this gap providing an easy to use and powerful object-relational persistence framework. The ORM Data Access Services will provide persistence to the DigSky Application data in enterprise database and facilitate creation, update and deletion of entities and relations. All the persistent records like business transaction details, workflow information, user information, emails are stored in this persistence layer in different format. Transaction details and workflow information would be stored in RDBMS while emails are stored in email server. User information would be stored in Directory server for faster authentication. The application framework will authenticate the users against LDAP server.

In other words the database layer will hold repositories for:

- User information
- Authentication information
- Business information including all audit logs
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

- Content information
- Mail information
- Workflow information

Suggested specification of the proposed RDBMS is mentioned below:

i. All the applications implemented should have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented should also optimize the duration of connection to the database by using techniques like session time out.

ii. Database should have perpetual and enterprise wide/subscription based licenses. They should have proven scalability credentials to cater to any system load.

iii. It should provide Unicode support.

iv. It should support User-defined Data Types & User-defined Functions.

v. Database should support advanced data compression, self-healing and deployment in various cluster topology.

vi. The database platform should support enhanced configuration and management of audits.

vii. The database platform should support Failover Clustering and disaster recovery solutions.

viii. It should support online indexing operations and parallel indexing operations

ix. Database should support Schemas, Roles Based Privileges & Authentication.

x. The data platform should support policy-based system for managing one or more instances across enterprise

xi. It should provide a scripting shell that lets administrators and developers automate server administration

xii. The database should have enterprise level DB- support center with a 24*7 helpdesk support.

xiii. Other than built in database access logic in application, a separate database security layer will be required to control direct access to database server by any unauthorized user.

xiv. The database platform should support defining resource limits and priorities for different workloads, which enables concurrent workloads to provide consistent performance

xv. Database security should provide different layers of database users with overall control of database security administrator, only authorized database administration users with assigned privilege should be allowed to access database.
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

xvi. A separate audit trail should be maintained for any direct modification, deletion and addition in RDBMS database in database structure or records. User, even the database administrator should not be allowed to tamper with audit log. Database server should support most granular column encryption to encrypt sensitive data.

xvii. The selected RDBMS should have abilities for fault tolerance, linear scalability, mixed workload capability.

xviii. Database should support option of different partitioning schemes within the database to split large volumes of data into separate pieces or partitions, which can be managed independently. It should support physical columns. The partitioning should enhance the performance, manage huge volumes of data and should provide foundation for Information Life Cycle Management.

xix. The RDBMS should preferably provide options for Automated/manual performance analysis with diagnosis of the cause of performance related issues with possible resolutions.

xx. RDBMS licenses should be unrestricted and full use licenses (read, write and modify). RDBMS should allow storing scanned images, text documents, XML, multimedia inside the tables. It should be part of the basic database distribution without any additional cost to the organization.

xxi. RDBMS should support the separation of security functionality from application functionality and database administration functionality.

xxii. Any proprietary OEM specific functionality of RDBMS should not be used.

• Data Analytics Layer

This layer is responsible for receiving the structured, semi-structured and unstructured data from the different data stores and performing analytics of the same for generating insights for application driven decision. There will be two separate data analytics engine, one for the business intelligence and dashboard and the other for applying intelligent algorithms and analytics to interpret and provide utility to the data and getting outputs of tangible values, insights or recommendations.

The intelligence engine is highly application-specific and generates real intelligence that can be used to make decisions.

The system design should have Virtual Data Room for access to anonymized data and Public Data for publishing of aggregate statistics.

• Integration Layer
All interfacing with external/internal systems will take place through this layer. External systems will not have direct access to the Digital Sky database, but instead will be calling the relevant business services in the business layer for availing the information. An ESB infrastructure shall be in place along with the API gateway that will provide standard interface to integrate with heterogeneous application making use of XML/JSON based standard protocol and mechanism for data exchange.
1.1.5 Integration Architecture

Envisioned API Enabled Architecture

All the integration that are indicated with DSP will also be required to be undertaken directly with Digital Sky Platform. In this regards, MSP is required to consider direct integration to platform of all the corresponding systems indicated in the diagram above.

The various technologies that would be required to achieve integration between the different applications and external systems are described below

1.1.5.1 Integration with External System

Many external systems would need to be integrated with Digital Sky and use of API's/Web services that are provided by various external systems. The external systems that may be integrated (Not limited to) are

- AFTN & AMSS for NOTAMs
- MET for meteorological data
• NOCAS for Building/Structure NOCs Data
• ATS Automation System for Air Traffic Data & FIC/ADC Number
• Military Operations Centre
• BharatKosh
• MHA
• CBEC
• eGCA
• Data.gov.in
• Any other government agencies.

1.1.5.2 API Gateway Services

• It is expected that the communication of the Digital Sky system with external interface will happen through an API layer. An API gateway should be used to manage the API communication with the external interfaces.

• Following are some of the expected gateway features for API management
  o API layer would not be exposed to untrusted connection
  o All APIs level access either to department systems or to app providers servers (for users accessing the system through the APPs) should be secure and through either of the below mode of connectivity:
    ▪ MPLS or
    ▪ VPN over internet
  o All data transfer to happen through APIs, File transfer mechanism is not encouraged
  o App signature authentication will be through the license key + time stamp + app version and other meta data
  o All the APIs would be stateless in nature, thus easy to load balance, even if hit through portal is very high and this requires high end processing.
  o The API Platform should be allowed to manage all your enterprise initiatives from a single solution:
  o The API platform should support existing APIs and developer preferences and provide the following transformations: and developer preferences
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

- The API Platform should provide clustering and ensure reliability, scalability and single point of administration:
- The API Platform should provide for enterprise grade encryption:
- The API platform should provide secure access to all APIs and provide ALL the following forms of authentication, access control and certificate/credential support:
- The API platform should provide comprehensive threat protection for all API traffic.

1.1.5.3 ESB component

Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rule-based routing, and policy-based routing, as applicable in various business cases.
- The solution should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable.
- The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality
- ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.
- ESB should support all industry standards interfaces for interoperability between different systems
- ESB should support the following integration security standards:
  - Authentication
  - Authorization
  - Encryption
  - Secure Conversation
  - Non-repudiation
  - XML Firewalls
  - Security standards support
  - WS-Security 1.1
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

- WS-Trust 1.3
- WS-Secure Conversations 1.3
- WS-Basic Security Profile
  - The solution should support routing to all internal & external systems.
  - The solution should have comprehensive auditing capabilities to support any internal or external audits.
  - The solution should provide configurable logging feature for supporting error handling.
  - The solution should include feature of service registry for managing all services.
  - The solution should support Business Activity Monitoring. One should be able to do a real time analysis of the data flowing within the ESB. One should be also able to monitor Key Performance Indicators.
  - The solution should be able to interoperate and connect with applications deployed on a number of platforms including, AIX, HP-UX, Sun Solaris, Windows, Linux etc.
  - The solution should support a whole suite of adapters such as Data Handler for XML, Exchange, Lotus Domino, industry standard packaged solutions etc.
  - The solution should support various messaging patterns e.g. synchronous, asynchronous, pub/sub, multicast, etc.
  - The solution should support SQL access to relational databases. Integration capabilities with NoSQL databases would be also advised.
  - The proposed ESB should support Time Control and Notification for messaging
  - The ESB should have an capabilities of Routing, Enrichment, Update, Transformation Processing
  - The ESB should support for Message Expiry configuration

1.1.5.4 SMS Gateway

SMS services are envisaged to be made available as part of the solution design. SMS services can be used for OTP authentication and as well as informing the users about their registration status, payment alert, return update etc. The service provider may integrate the solution with MSDG, and use the services available through it, or deploy SMS Gateway services developed by it for Digital Sky or integrate with other sms gateways provided by service providers, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be
available as part of the solution. For outbound message SMS gateway can be developed. Specification related to SMS has been provided in the Notification & messaging section above.

1.1.5.5 Email Services

Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support antispam features.

1.1.5.6 Integration with SSDG, NSDG, National Portal and MSDG

It is envisaged that the Digital Sky solution could be required to integrate with State/National/Mobile e-Governance Service Delivery Gateway (SSDG/NSDG/MSDG) and National Portal respectively, as per NeGP guidelines and DeitY, GoI vision for all government applications. APIs are required to be built for connectivity with 3rd party gateway. There could be HTTP based API as well as SMTP protocol based API. It is mandatory that the requirements of 'Integration' and 'Scalability' must be taken into account while developing /customizing the application so that any change is easily addressed as and when these systems are implemented at the state and national level.

1.1.5.7 Security Architecture

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of Digital Sky security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders. A diagrammatic representation of the security framework for the envisaged Digital Sky system is provided below. The architecture shall be mainly based on cryptography overall as indicated in RFP
Some of the key security principles are explained below.

### 1.1.5.8 Application Security

a. Digital Sky system must comply with the Application Security Plan and security guidelines of Government of India as applicable

b. Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities.

c. Validation checks should be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.

d. Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

e. Should implement secure error handling practices in the application.
f. Digital Sky system should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following

g. Prevent SQL Injection Vulnerabilities for attack on database

h. Prevent XSS Vulnerabilities to extract user name password (Escape All Untrusted Data in HTML Contexts and Use Positive Input Validation)

i. Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS

j. Prevent Security Misconfiguration Vulnerabilities (Automated scanners shall be used for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc. maintain Audits for updates)

k. Prevent Insecure Cryptographic Storage Vulnerabilities (by encrypt off-site backups, ensure proper key storage and management to protect keys and passwords, using a strong algorithm)

l. Prevent Failure to Restrict URL Access Vulnerabilities (By providing authentication and authorization for each sensitive page, use role-based authentication and authorization and make authentication and authorization policies configurable

m. Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections)

n. Prevent Id Redirects and Forwards Vulnerabilities

o. For effective prevention of SQL injection vulnerabilities, Solution should have monitoring feature of database activity and should have reporting mechanism to restrict or allow the traffic based on defined policies.

1.1.5.9 Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Digital Sky applications. Consider use of at least two of the following forms of authentication mechanism:

1. Something you know, such as a password, PIN etc

2. Something you have, such as a smart card, hardware security token etc

3. Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.
1. For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data.

2. For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defence is the password conforming to the password complexity rules'. Along with the password next user has to provide a one-time password which varies for each session. One time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

Centralized Identity and Access Management Model

It is recommended to adopt an enterprise level centralized authentication model that is secured and ensures that user has a single credential to access the all the services.

In this model there will a centralized authentication services with provision for centralized user registration and user credential store. A centralized user repository (directory services) for the storage of user credentials will also store the authorization information for the user which will be used in different application.

The proposed centralized Identity and Access Management solution is depicted below –

1. Central Access Management Service
   a. This service will provide the central authentication service for the users/groups created by verification of the user credentials against the central LDAP user repository. When a user tries to login to any centralized application e.g. single window portal, departmental sub-, the user credentials will be validated through the central authentication service.
   b. Single Sign-On service will centrally maintain user session thus preventing user from multiple login when trying to access multiple applications.

2. Central Identity Management Service
   a. This service will handle user life cycle management that will enable Digital Sky to manage the lifespan of the user account from its initial stage of provisioning to the end stage of de-provisioning. Typically user provisioning and de-provisioning is workflow driven that will require approval.
   b. User management service will cover user administrative functionalities like creation, propagation and maintenance of user identity and privileges.
   c. Self Service feature will allow end users (e.g. members) to maintain their user identity account including self-password reset which will significantly reduce helpdesk/admin effort to handle password reset requests.
d. The central user repository will store the user identity data and deliver it to other services (e.g. central authentication service) for credential verification. Adherence to LDAP v3 standard has been the dominant standard for central user repository.

e. Enforce a robust and strong password policies that will allow users to change/reset password with password expiry and account lockout features, define and implement complex password rules and session timeout policies.

Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list:

- Establish groups of users based on similar functions and similar access privilege.
- Identify the owner of each group
- Establish the degree of access to be provided to each group

1.1.5.10 Data Security

Traditional Structured Enterprise Data

Department should protect Digital Sky System information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defences against possible security vulnerabilities and threats, allowing errors to be corrected and system misuse to be minimized.

The implications for adhering to an effective data security and integrity guideline related to the Digital Sky System are the following –

1. Data security policies and standards to be developed and adopted in the Digital Sky application

2. Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.

3. In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.

4. Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
5. **Audit Capabilities:** The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.

6. **Maintaining Date /Time Stamp and User Id:** Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.

7. **Access Log:** The Digital Sky System should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

### 1.1.5.11 Data Integrity

Data in transit (from external systems or between internal systems) or data at rest must be protected from tampering. The risk is from both external users and internal users (such as Database Administrators) who are close to the data at all times.

To handle the risks of data being tampered by the external users and during transit, API design must ensure checksum features and Digital Signature/ e-Sign to validate the data is secured. The API documents explain these features in detail and all the sensitive data must adhere to these principles. Digital Sky system shall ensure to validate integrity using the checksum and Digital Signature/ e-Sign validations before processing the data.

To handle the risks of data being tampered by the internal users such as Database Administrators who have access to data, Digital Sky application shall be designed with the below principles:

1. All the data access must be enabled only through internal API /modules.

2. Each subject area can be packages into a persistence module that exposes domain specific methods to read, insert, update or delete the records

3. Persistence module shall abstract the underlying data base technologies, physical data models

4. Based on the current proposals, underlying technology used to store data could be in one of the possible ways:
   a. RDBMS store
   b. HBase column based store
   c. File store (e.g HDFS, XFS)
   d. Object store

   a. **RDBMS store:**
      i. RDBMS store shall be accessed using industry standard Hibernate ORM layer, which is widely adopted and is open source/open standard
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

ii. Every database (related to a subject area) that is identified to have sensitive information shall have one additional data column in each of the tables to track the checksum value

iii. The columns and the order in which the columns shall be sequenced is tracked as a version number

iv. This version number used followed by a delimiter and then the computed checksum value shall be stored in the above 'integrity' column

v. When the data read, the persistence module shall compute the checksum and validate the data integrity before returning the data

vi. All the insert, update calls shall also do the same logic to compute the checksum and update the new value as part of these transactions

vii. One possible implementation of the above security requirement can be done using hibernate interceptors and triggered 'On Save' or alternatively using the standard OOD patterns by extending the base platform level class across all the entities in Digital Sky system

viii. In the persistence module layer, the checksum retrieved can be validated and appropriate exceptions can be thrown to the callers

ix. Tracking the version number for each row, shall enable the design to be scalable for any future table level alternations that can happen

b. NoSQL based store:

If NoSQL store is used then also data integrity can also be achieved in similar fashion and instead of ORM interceptor, here custom code in the persistence module can be considered.

c. File store:

The Digital Sky system shall store all the xml request files received from external systems as-is. Since XML APIs have in built in security features related to checksum and Digital Signature/ e-Sign validations, any re-use of these files by the internal systems must ensure these checks are done before using this data.

1.1.5.12 Data Confidentiality

To ensure data is secured to access only by required teams and applications, the following principles are to be adhered:

1. All the databases must be accessed by individual user accounts and user accounts cannot be shared by multiple persons or as a team based accounts.
2. All the databases/systems must be integrated with the Identity Access Management system for centralized control. This will also enable disabling of user accounts when a person leaves the organization.

3. For reporting purposes, the data MUST be anonymized (e.g. user level id and details are to be masked - mobile number can be stored as a hash value etc.) before publishing to the BI reporting system.
   a. Any ID must be stored by a UUID value that cannot be easily guessed.
   b. The mapping of such critical id's can be stored as master information in main databases.
   c. Any other sensitive information must be hashed and stored in BI system

4. For sharing of identity data between systems, OAuth 2.0 must be used.

5. Sensitive data stored in the main RDBMS tables must be encrypted so that Database administrators do not have direct access to this information for misuse
   a. Encryption must be done on similar lines of data integrity. However to ensure no significant performance loss, the Hardware security modules must be used to encrypt and decrypt the data while persisting and reading the data.
   b. All applications reading the data must use the common persistence modules designed for each subject area to abstract the implementation complexity and expose the solution as a re-usable component.
   c. The keys used to encrypt the data shall be critical information that must be protected at all times.
   d. The column type for all encrypt able columns must be sized large enough to store the encrypted information. Additionally the column type is set to string type and persistence module for each of the databases must ensure to do the required translation from string to appropriate data type. For e.g. numeric column such as year of establishment may be stored as string in table but converted to the integer by the persistence module.

1.1.5.13 Message Protection and Integrity

The Request message XMLs would be protected using HMAC. The MAC would be used to simultaneously verify both the data integrity and the authentication of a message.

1.1.5.14 Digitally signed requests

In some cases the Request XMLs would be digitally signed that would help in the non-repudiation of the requests. Digital Sky system would also send digitally signed XMLs as response for specific cases. The XML message received as input for some of the message can be validated with configuration.
1.1.6 Enterprise Manageability Architecture

The enterprise manageability and operations architecture is shown in the figure below:

Enterprise manageability and operations architecture

The above figure depicts the operations architecture of the Digital Sky system. The architecture can be divided into mainly the following components:

- **ITSM Tools and Practices:**

  It is strongly recommended to use the ITIL best practices for the IT service management of Digital Sky. The key areas that are recommended to be setup for management of day to day operations of Digital Sky as per ITIL best practices are

  **Event Management:** Any events that are captured in the application monitoring tools such as info, warnings and alerts need to be captured, correlated and processed by event management tools. Based on the result of correlation, tools can pinpoint to root cause of error/failure conditions and such events can be sent to incident management tools to create incident tickets.
Incident management: Incidents refer to conditions of errors, breakdowns etc. which need support for corrections. Incidents can be manually created or created automatically by event management tools, or by application monitoring tools. The best recommended architecture is where all applications are monitored by a combination of infrastructure, security and application performance monitoring tools. These tools on generation of any kind of events create incidents of priority depending on severity of alerts.

Problem Management: In case incidents are closed with a workaround without a permanent resolution, deep dive investigations is followed up by opening of a problem record. Problem record documents the ongoing investigations and workaround available till the permanent resolution is achieved.

Release and Deployment management: Deployment of applications or application changes/components etc. in a complex enterprise such as Digital Sky needs a seasoned deployment management process and tools. It is recommended to also use advanced capabilities such as DevOps which has capabilities such as continuous integration and continuous deployment to reduce the time it takes to commit a change in development and move the change to production.

Access Management: Access to grant authorized users is controlled using the access management process. Access management needs to be managed in a controlled manner and hence identity and access management suite is part of the Enterprise architecture of Digital Sky. A clear definition of privileges associated with different roles needs to be defined where access to different application components, workflows etc. is well documented and maintained in the identity and access management system. A clear policy of upgrade and removal of identities needs to be also defined. Audit trails of any change in privileges need to be maintained in identity management system.

IT Change management: Any change to the system needs to be done via the regular change management process of ITIL. Change management requires the creation of a change management board who would be the different process/application owners. Periodic meeting of change request board would approve, reject all the changes to be carried out to any system after a detailed impact analysis and making sure all stakeholders are aware of their roles and responsibilities in carrying out their changes.

Performance management: A regular performance management process needs to be established where performance of key applications (customer facing and internal) needs to be regularly reviewed and any changes needed to ensure the scalability of the applications evaluated and recommended for change requests.

- Application/infrastructure monitoring tools and practices

It is strongly recommended to have application monitoring in place for all applications where application performance is continuously recorded and evaluated. Application monitoring would enable quick troubleshooting of any issues related to application performance and also give a continuous end user experience measurement. End user experience measurement is extremely
critical to ensure any issues in application are caught and handled early before stakeholders starts noticing them and complaining.

It is also recommended to have infrastructure level monitoring in place to keep a vigil on the health of the infrastructure on which the various application architecture layers are deployed.

- **Security management and tools:**

It is extremely important to have a set of IT security management processes and tools to ensure IT security of Digital Sky is always maintained. It is recommended that an IT security policy, framework and operational guidelines be maintained by the Managed Service Provider (MSP) and Cloud service provider (CSP) as an overall guideline to all forms of IT security – Physical, application, data, network and cloud.

The IT systems maintained should be regularly audited and subject to different IT security testing. The system should also maintain regular detailed audit records of all data changes made to critical systems, procurement transactions. There should be tools to mine these audit records and gather intelligence from these tools to not only alert MSP and CSP of any breaches but also predict of any security mishaps that can occur. Latest security tools like IPS, IDS, Malware protection, Data loss protection, DB change audit observation kits etc. need to be in place. All the security management processes, tools and usage should be well documented in a Digital Sky security policy and guide the security processes to be followed to maintain IT security of Digital Sky system.

### 1.1.7 Solution Component

It is preferable to deploy open source solutions to build Digital Sky system which is modular, scalable and portable across platforms. All the platforms and solutions proposed for Digital Sky system should be vendor neutral and AAI/DGCA can replace any platform without any constraint.

An indicative list of solution component has been provided below. The Solution Components in the list have been identified as Core and Non-Core. For each solution component, the requirement in terms of Open Source / Bespoke / Proprietary is also given in the table below. For certain Open Source products, enterprise support in India, from respective OEM is required.

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>Type</th>
<th>Type of component (Open Source / Bespoke / Proprietary)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>Web Portal</td>
<td>Core</td>
<td>Bespoke / Open Source product</td>
</tr>
<tr>
<td>Mobile Solution</td>
<td>Core</td>
<td>Bespoke / Open Source product</td>
</tr>
<tr>
<td>Web Server</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>Application Server</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
</tbody>
</table>
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

<table>
<thead>
<tr>
<th></th>
<th>Non Core</th>
<th>Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learning management</td>
<td></td>
<td>Bespoke/ Open Source product/Proprietary</td>
</tr>
<tr>
<td>Grievance Management</td>
<td>Core</td>
<td>Bespoke/ Open Source product/Proprietary</td>
</tr>
<tr>
<td>Core Map/GIS Tool</td>
<td>Core</td>
<td>Open Source</td>
</tr>
<tr>
<td>GIS Visualization</td>
<td>Non Core</td>
<td>Open Source product/ Proprietary</td>
</tr>
<tr>
<td>ESB</td>
<td>Core</td>
<td>Bespoke/ Open Source product</td>
</tr>
<tr>
<td>Work Flow Management</td>
<td>Core</td>
<td>Bespoke/ Open Source product</td>
</tr>
<tr>
<td>Rule Engine</td>
<td>Core</td>
<td>Bespoke/ Open Source product</td>
</tr>
<tr>
<td>Queue-based Messaging</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>MIS Reporting</td>
<td>Core</td>
<td>Open Source product/ Proprietary</td>
</tr>
<tr>
<td>BI Tool</td>
<td>Non-Core</td>
<td>Open Source product/Proprietary</td>
</tr>
<tr>
<td>Analytics Tool</td>
<td>Non-Core</td>
<td>Open Source product/ Proprietary</td>
</tr>
<tr>
<td>API Gateway</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>In Memory-Caching</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>Build Management</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>Source Control</td>
<td>Core</td>
<td>Open Source product</td>
</tr>
<tr>
<td>Map Visualization</td>
<td>Core</td>
<td>Open Source product/ Proprietary</td>
</tr>
</tbody>
</table>

All non-core components should adhere to the architectural principle stated in RFP

** Any bespoke development must be done on an open source programming language.

It should be noted the selected MSP will be responsible for the overall support and maintenance of the Digital Sky solution till the end of the O&M phase.

1.1.8 Software Development Lifecycle

1.1.8.1 Continuous Build

The Digital Sky system development should be highly modular and parallel development should be carried out for faster execution using industry’s best Software Development Lifecycle practices. All application modules within the same technology platform should follow a standardized build and deployment process.

A dedicated ‘development /customization’ environment should be proposed and setup. The MSP must provision separate development and testing environment for application development and
testing. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking tool is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

### 1.1.8.2 Container Architecture

MSP should follow micro service deployment approach. MSP should use a Container Architecture tool for entire development life cycle e.g. developing, shipping, and running applications. With container Architecture, the developer teams can separate the applications from the infrastructure and treat the infrastructure like a managed application. It can also help to ship code faster, test faster, deploy faster, and shorten the cycle between writing code and running code. It allows the developers to develop on local containers that contain the applications and services. It can then integrate into a continuous integration and deployment workflow.

Following objectives can be achieved by a Container Architecture:

- Faster delivery of the applications
- Easy Deployment and scaling
- Achieving higher density and running more workloads

[Container Architecture Diagram]

*An illustration of Container Architecture*
1.1.9 QUALITY ASSURANCE

A thorough quality check is proposed for the Digital Sky system and its modules, as per standard Software Development Life Cycle (SDLC). MSP is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by AAI. MSP is required to incorporate all suggestions/feedback provided after the elaborate testing of the AAI, within a pre-defined, mutually agreed timeline. MSP must undertake the following:

a. Outline the methodology that will be used for testing the system.

b. Define the various levels or types of testing that will be performed for system.

c. Provide necessary checklist/documentation that will be required for testing the system.

d. Describe any technique that will be used for testing the system.

e. Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.

f. Indicate/demonstrate to AAI that all applications installed in the system have been tested.

1.1.9.1 Automated Testing

MSP is expected to perform automated testing with following features:

a. Should support multi-layer test scenarios with a single solution.

b. Should support and execute testing on GUI and UI-Less (standard Web Services, non-SOAP Web Services, such as REST, etc.) Components.

c. Should allow version control of tests and test assets providing ability to compare versions and identify changes.

d. Should allow centralized storage and management of tests and test assets including external resources used by tests.

e. Should have an IDE environment for QA engineers which should be configurable.

f. Should provide local system monitoring to test and validate performance issues including memory leakage, CPU overload and network overload to determine if specific business scenarios exceed desired performance thresholds.

g. Should provide Auto-documentation while creating of automated tests.
h. Should generate reports that can diagnose defects and can be exported to (PDF, XML, Html) (mandatory) and doc (optional) formats.

i. Report with summary data, pie charts and statistics for both the current and previous runs needs to be provided.

j. Should enable thorough validation of applications through a full complement of checkpoints such as GUI object, database, XML, XPath, etc.

k. Should provide Unicode support for multilingual application testing.

l. Should be able to record the test Execution into a video file for viewing later.

m. Should provide facility to parameterize tests to generate/assign test case output values automatically during runtime.

1.1.9.2 Performance and Load Testing

The MSP is expected to implement performance and load testing with following features:

a. Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.

b. Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.

c. MSP should perform the load testing of Digital Sky application for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.

d. Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.

e. Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator as applicable while introducing configurable latency/jitter/packet loss etc.

f. Should eliminate manual data manipulation and enable ease of creating data-driven tests.

g. Should provide capability to emulate true concurrent transactions.

h. Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM

i. Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.

j. Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components

k. Should correlate response times and system performance metrics to provide quick insights into root cause of performance issues.

l. Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.

m. Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.
APPENDIX 8 – TENDER FOR DEVELOPMENT, HOSTING AND MAINTENANCE OF DIGITAL SKY PLATFORM
Appendix 9: Service Level Agreements

1.1 Introduction

i. This document details the expected service levels for various services to be provided by the MSP. Performance of the Managed Service Provider (MSP) services shall be measured against the Service Level Agreements as explained and detailed in this document.

ii. The service level targets define the levels of service to be provided by Managed Service Provider to AAI for the duration of this contract or until the stated SLA targets are amended.

iii. The objectives of SLA governance model are to:
   a. Provide clear reference to service ownership, accountability, roles and/or responsibilities.
   b. Present a clear, concise and measurable description of service provisioning at each level.
   c. Match perceptions of expected service provisioning with actual service support and delivery.

iv. The SLAs are intended to:
   a. Make explicit the expectations that AAI has for performance
   b. Help AAI control and ensure the planned levels and performance of services
   c. Trigger a process that brings AAI and Managed Service Provider’s management attention to some aspect of performance when that aspect drops below an agreed upon threshold or target.

1.2 SLA Philosophy and Principles

This section details the overall philosophy and principles that have been adopted in preparing the SLA

Framework for MSP.

i. Uniform approach to interpretation of SLAs has been adopted and it will be based on coherent reading of SLAs which appear in many sections of the RFP document.

ii. Levels of SLAs which the MSP should follow post GO-LIVE. SLA applicable for Pre Go Live (timelines driven) defined in tender document

iii. Any change in the SLAs would be governed by the SLA change control mechanism.
iv. MSP would be responsible for SLAs for the work undertaken by the sub-contractors. Sub-contractors' SLA would not be separate from the MSP’s SLAs. MSP would be responsible for the overall SLAs for delivery of services (as defined in the RFP).

v. MSP shall deploy automated and transparent tools for measurement and reporting of SLAs.

vi. MSP’s role shall be limited to development, deployment and maintenance of the SLA reporting tool. Control of the tool shall be with AAI or its appointed agency. All aspects of the reporting tool including code and implementation shall be subject to review/audit by AAI or its appointed agency. MSP is required to provide periodic SLA reports which may be audited by AAI nominated agency from time to time.

1.3 Definitions

i. Below are definitions specific to this SLA document.

a. Non-working days = All Sundays and Public Holidays as declared by AAI

b. "Downtime" is measured from the time the application becomes unavailable (due to any reasons whatsoever attributable to the MSP) for business processing to the end user to the time it becomes fully available for the above stated business processes. Any scheduled outages planned in advance and are not attributable to MSP shall be excluded from SLA calculation. Such Downtime shall be undertaken only after prior approval from AAI. It is to be noted that for each time downtime request, a written consent will have to be taken by MSP under category of “non-attributable” to MSP.

c. "Helpdesk Support" shall mean the helpdesk center which shall handle Fault reporting, Trouble Ticketing and technical related enquiries during this contract. Further, the helpdesk mean business support provided as per scope of work

d. “Tickets” refers to the request generated in the Service desk describing the issue or problem the user is facing.

e. “Incident” refers to any event/abnormalities in the functioning of the Digital Sky Services that may lead to disruption or lower performance in normal operations of the Digital Sky services.

1.4 Administration of Service Level Agreements

1.4.1 Responsibilities of Parties

1.4.1.1 Responsibilities of AAI

AAI is responsible for providing early warning of any organizational, functional or technical changes that might affect Managed Service Provider’s ability to deliver the services described in the SLAs.
1.4.1.2 Responsibilities of the Managed Services Provider

i. Managed Services Provider is responsible for delivering the services described in Scope of Work document to the performance targets detailed in this document.

ii. Additionally, Managed Services Provider is responsible for:
   - Reporting problems to AAI Management as soon as possible
   - Providing early warning of any organizational, functional or technical changes that might affect Managed Services Provider’s ability to deliver the services described in the SLA

iii. Immediate action to identify problems and follow up with appropriate action to fix them as quickly as possible.

1.4.2 Reporting procedures

i. SLA reporting should be done using an automated tool that should provide reports on a Weekly, Monthly, Quarterly basis

ii. To the extent possible SLA reporting should be based on automated logs with minimal manual intervention.

iii. Well-defined processes should be implemented for those SLAs that require manual intervention for measurement and reporting. In such cases, the SLA measurement methodology should be discussed and agreed upon with AAI

iv. The SLA performance reports in an agreed upon format should be made available on-line.

v. The reports will include “actual versus target” SLA performance, a variance analysis and discussion of appropriate issues or significant events.

vi. SLA reports will be distributed to authorized Management personnel as directed by AAI.

1.5 SLA Change Control

1.5.1 General

i. It is acknowledged that the SLAs may change as AAI’s business needs evolve over the course of the contract period.

ii. This document defines the following Management procedures:
   a. A process for negotiating changes to the SLA.
   b. An issue Management process for documenting and resolving particularly difficult issues.
c. AAI and Managed Services Provider’s Management escalation process (to be defined later by AAI) to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of Management.

iii. Any changes to the levels of service provided during the term of this Agreement will be requested, documented and negotiated in good faith by AAI and Managed Services Provider.

iv. AAI or the Managed Service Provider can request a change in SLAs.

v. Changes will be documented as an addendum to this document and, consequently, the Contract.

vi. If there is any confusion or conflict between the Contract and this document, the Tender and its addendums, the Contract will supersede.

1.5.2 SLA Change Process

i. The parties may amend this SLA by mutual agreement in accordance with the process described below.

ii. Changes can be proposed by either party.

iii. The Managed Service Provider’s representative will initiate an SLA review at least bi-annually. Normally, the forum for negotiating SLA changes will be AAI’s monthly meetings. AAI and MSP will review the Service Levels and mutually agree whether to:

   a. Add to, delete or change the Services to be measured and the corresponding Service Levels to reflect changes in AAI’s business operations; and

   b. Improve the existing Service Levels, where warranted, to reflect operational or technical improvements.

iv. Unresolved issues will be addressed using the issue Management process.

v. The Managed Service Provider’s representative will maintain and distribute current copies of the SLA document as directed by AAI. Additional copies of the current SLA will be available at all times to authorized parties.

1.5.3 Service Levels for a New Service, Optional Service or Additional Services

i. With respect to a New Service, Optional Service or Additional Services, MSP and AAI will establish initial Service Levels following full implementation of such Services which will apply during the initial 90-day period of MSP providing such New Service, Optional Service or Additional Services.

ii. To the extent appropriate, such initial Service Levels will be the same as or similar to existing Service Levels for the same or similar Services.
iii. During such 90 days, MSP and AAI will conduct a process for **Measurement and Validation of Service Levels** to validate the initial Service Levels and agree upon the actual Service Levels. AAI shall be final authority to decide on the SLA and shall be binding on MSP.

iv. The finalized service levels shall be documented and implemented in adherence with the SLA version control process.

### 1.5.4 SLA Version Control

i. All negotiated SLA changes will require changing the version control number.

ii. SLAs shall be documented for new services, optional services and additional services following the completion of measurement and validation for those SLAs.

iii. As appropriate, minor changes may be accumulated for periodic release (e.g. every quarter) or for release when a critical threshold of change has occurred.
1.6 Application of Liquidated Damages

i. SLA shall be measured and applied post 3 months of Go-Live of various phases. Any operational SLA breach (excluding the Go-Live related timelines mentioned in tender document) during the implementation phase for services Go-Live of Phase 1 & 2 shall be applied on the quarterly payment as base (as per payment schedule) and shall be deducted from the next due payment to MSP.

ii. All payment adjustments for breach of SLA in the O&M phase shall be adjusted against the quarterly payments.

iii. A maximum level of performance Liquidated Damages are established and described below.

iv. The framework for performance Liquidated Damages as a result of not meeting the Service Level Targets are detailed below.

v. A quarterly performance evaluation will be conducted using the three monthly reporting periods of that quarter.

vi. Where SLA measurement is done on a monthly basis, sum of Liquidated Damages associated with each month shall apply for the quarter.

vii. Performance Liquidated Damages shall be levied for not meeting each SLA.

viii. Breach of SLAs target shall result in various severity level based on the business impact the component causes to MSP services.

ix. The severity levels of SLAs and the associated financial Liquidated Damages are defined as per the following table:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Liquidated Damages as a percentage of Quarterly payment applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Event of default and termination as per the RFP document and the corresponding consequences shall follow</td>
</tr>
<tr>
<td>8</td>
<td>5.0 %</td>
</tr>
<tr>
<td>7</td>
<td>4.0 %</td>
</tr>
<tr>
<td>6</td>
<td>2.0 %</td>
</tr>
<tr>
<td>5</td>
<td>1.0 %</td>
</tr>
<tr>
<td>4</td>
<td>0.5 %</td>
</tr>
<tr>
<td>3</td>
<td>0.4 %</td>
</tr>
<tr>
<td>2</td>
<td>0.2%</td>
</tr>
<tr>
<td>1</td>
<td>0.1%</td>
</tr>
</tbody>
</table>
i. If on Performance evaluation it is found that the MSP has not met a measurement parameter for two consecutive quarters the same shall result in doubling the Liquidated Damages percentage of that measurement parameter.

ii. Cumulative Liquidated Damages for each quarter after Go-live shall under no circumstance exceed 25% of the fee payable for that quarter. The Cumulative Liquidated Damages for the entire project under no circumstance will exceed 10% of total Contract Value.

iii. If liquidated damages calculations exceed 15% of the quarterly payment for two consecutive quarters, then AAI can take appropriate action including termination of the contract and forfeiting of Performance Bank Guarantee.

iv. Notwithstanding anything contained herein, if the MSP fails to achieve Go-Live within 6 months of the planned date, due to reasons attributable to the MSP, then AAI will have the right to terminate the contract for default.
1.7 Operations & Maintenance Phase SLAs (After Go-Live of Digital Sky System including O&M undertaken prior to Go-Live of all Phases)

1.7.1 Digital Sky Availability SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Digital Sky Web Portal/App including all functionalities and services.</td>
<td>Availability</td>
<td>Metric: % of Uptime for any of the parameters (Digital Sky Web Portal, all functionalities and/or services) &lt;br&gt;Formula: Uptime % = (1 - \left(\frac{\text{Total Downtime}}{\text{Total Time} - \text{Planned Downtime}}\right)) *100 &lt;br&gt;Total Downtime - Total cumulative time of any of the parameters defined above. &lt;br&gt;Planned Downtime - Total maintenance time as defined and agreed upon by MSP and AAI and not attributable to MSP. &lt;br&gt;Total Time - 24 X 7 measured over a period of month. &lt;br&gt;Period of Measurement: Monthly &lt;br&gt;For each additional drop of upto 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages. For example, a drop to 97.3% will be levied with additional 0.5% LD, while a drop to 96.3% will be levied an additional 1% LD</td>
<td>&gt;=99.9%</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;99.9% and &gt;= 99.5%</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;99.5% and &gt;= 99.0%</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;99% and &gt;= 98.5%</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;98.5% and &gt;= 98.0%</td>
<td>7</td>
</tr>
</tbody>
</table>
### Digital Sky API Availability SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
</table>
| 1       | Digital Sky API availability. | Availability | Metric: % of Uptime for all APIs  
Formula: Uptime % = (1−{(Total Downtime) / (Total Time – Planned Downtime)}) *100  

Total Downtime - Total cumulative time of any of the parameters defined above.  

Planned Downtime - Total maintenance time as defined and agreed upon by MSP and AAI and not attributable to MSP.  

Total Time - 24 X 7 measured over a period of month.  

Period of Measurement: Monthly  

For each additional drop of upto 1% in performance below 98%, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages. For example, a drop to 97.3% will be levied with additional 0.5% LD, while a drop to 96.3% will be levied an additional 1% LD. | >=99.9% | 0 |
|          |                    |             |            | <99.9% and >= 99.5% | 5 |
|          |                    |             |            | <99.5% and >= 99.0% | 6 |
|          |                    |             |            | <99% and >= 98.5%  | 7 |
|          |                    |             |            | <98.5% and >= 98.0% | 8 |
### 1.7.2 Digital Sky Performance SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Average page loading time for all services at AAI offices</td>
<td>In seconds</td>
<td>Page loading time measured monthly.</td>
<td>95% within the limit of 2 seconds</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Transaction response time except the transactions mentioned in 1.3 below at AAI offices</td>
<td>In seconds</td>
<td>Response time of services measured monthly</td>
<td>95% within the limit of 2 seconds</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>Transaction response time involving uploading/ downloading of documents (avg. size 2 MB) at AAI offices</td>
<td>In seconds</td>
<td>Response time of services measured monthly</td>
<td>95% within the limit of 5 seconds</td>
<td>2</td>
</tr>
</tbody>
</table>

Note: The above time should be captured at AAI offices. The MSP should deploy tools at the location to allow for measurement of performance. Please note that network delay caused shall be accordingly adjusted in the measurement of performance.

### 1.7.3 Cloud Services/Network SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RTO</td>
<td>Time in Hours</td>
<td>Based on the successful operations from DR Site and restoring the services back. This is applicable for both production environment and during DR Drills</td>
<td>&lt; 15 Min</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;=15 to &lt;45 Mins</td>
<td>5</td>
</tr>
</tbody>
</table>
### APPENDIX 9 – QUALIFICATION AND SELECTION CITERIA FOR DIGITAL SKY – SERVICE LEVEL AGREEMENT

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
</table>
|         |                     |                | **RPO**<br>Time in Minutes<br>Based on the successful operations from DR Site and restoring the services back with no data loss. This is applicable for both production environment and during DR Drills<br>For delay of each additional 10 minutes or part thereof after 20 minutes, additional 0.5% of the Quarterly Payment shall be levied as additional Liquidated Damages. | >=5 Mins: 0  
>5 to <10 Mins: 5  
>=10 to <20 Mins: 7  
>= 20 Mins: 8 |                |
| 2       | RPO                 |                | <5 Mins 0  
>5 to <10 Mins 5  
>=10 to <20 Mins 7  
>= 20 Mins 8 |                     |                |
|         |                     |                | **DR Drill**<br>Two Drills (once every 6 months) in a year (based on successful operations from the DR site and restoring services back with no data loss).<br>This will be measured every 6 months and the Liquidated Damages will be levied in the quarter following the end of the six month period.<br>Exception: Where the Drill is impacted or delayed due to reasons not attributable to the MSP, and the MSP has informed AAI about the same with proper evidences and RCA (whenever applicable). | 2 Drills: 0  
1 Drill: 5  
0 Drill: 6 |                |
| 4       | DR Drill            |                | >1 day & <= 10 days 0.05% of Quarterly payment |                     |                |
| 5       | Timely upgrades and updates | All components of Digital Sky | MSP shall ensure that all the components in the DIGITAL SKY are within supported versions. Upgrades need to be executed for all components on a regular basis. MSP shall in discussion | >1 day & <= 10 days: 0.05% of Quarterly payment |                |
### Cloud Service SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>application run on supported versions</td>
<td></td>
<td>with AAI decide on timelines for updates. The SLA is applicable on delay beyond the decided timelines between AAI and MSP. Note: It shall be MSP’s responsibility to trigger timely requests for upgrade of the various components. These requests should be accompanied by relevant technical literature, OEM whitepapers etc. These should also be accompanied by MSP’s own technical analysis of impact on other components in the System and dependency on other vendors in AAI’s landscape. AAI may reserve the right to defer an upgrade, and the MSP will be exempted from the corresponding penalty. For delay of each additional week or part thereof after 25 days, 0.2% of implementation phase contract value shall be levied as additional Liquidated Damages.</td>
<td></td>
<td>&gt; 10 days &amp; &lt;= 20 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For every component in the DIGITAL SKY application (in any environment) which is not on the OEM supported version, 10% of Quarterly Payment will be levied as penalty per component per default quarter. Shall be evoked even if a component has been in an unsupported version for one day in a Quarter. Identification of such incidents can also be evaluated for breach of contract.</td>
<td></td>
<td>&gt; 20 days &amp; &lt;= 25 days</td>
</tr>
</tbody>
</table>

6 Adherence to Backup Policy | Backups | Based on the backup policy indicated in the RFP | Target:  
- 100% backups taken on time as per the RFP  
- 100% backups tiered to Long term storage on schedule in accordance to the Backup Policy | < 100% backups taken on time as per the Backup Policy defined in RFP | 5 |
|                           |         |                                              | < 100% backups tiered to Long term solution on | 4 |
### Cloud Service SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>100% backup restoration testing on time in accordance to the Backup Policy</td>
<td>schedule in accordance to the Backup Policy in the RFP</td>
<td>3</td>
</tr>
</tbody>
</table>

### 1.7.4 SLAs on Audits

<table>
<thead>
<tr>
<th>#</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outcome of Half Yearly IT Security Audit</td>
<td></td>
<td>The third party auditor shall rate the performance of the MSP / CSP on IT Security implementation. The three ratings for the performance shall be: Satisfactory, Requires Improvement, and Unsatisfactory</td>
<td>Satisfactory</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Requires Improvement rating</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unsatisfactory rating</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Implementation of recommendations of previous IT Security audits</td>
<td></td>
<td>Implementation of recommendations given by the IT Security auditor and which have been agreed upon to be implemented by the MSP &amp; AAI</td>
<td>100% on time</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt; 100 %</td>
<td>5</td>
</tr>
</tbody>
</table>
100% on time, for the recommendations agreed upon with AAI, to be implemented in the said quarter

1.7.5 Helpdesk SLAs

<table>
<thead>
<tr>
<th>#</th>
<th>SLA Parameter</th>
<th>Definition &amp; Target</th>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
</table>
| 1. | Availability of each Toll-Free Lines at Help Desk Location | Uptime = \{1 - [(Toll Free Line downtime) / (Total Time)]\}  
Total Time shall be measured as defined in RFP  
Downtime shall be measured from the time the Toll Free Line at a help desk becomes unavailable to the respective users to the time it becomes available  
**Target:** Minimum 95% up time measured on a Monthly basis per toll-free line  
For each additional drop of 1% in performance below 95%, liquidated damages of 1% will be levied as additional liquidated damages. | 100% of the toll-free lines should meet the Target  
>= 99.0% to < 100% of the toll-free lines meeting the target  
>= 97.0% to < 99 % of the toll-free lines meeting the target  
>= 95.0% to < 97 % of the toll-free lines meeting the target | Nil  
3  
4  
5 |
| 2. | Call Queue Waiting time | Measured as % of calls where ‘call queue waiting time’ is less than 2 minutes. | >=95%  
>=94% and <95% meeting the target | Nil  
1 |
<table>
<thead>
<tr>
<th>#</th>
<th>SLA Parameter</th>
<th>Definition &amp; Target</th>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Call queue waiting time</td>
<td>Call queue waiting time is the waiting time in Automatic Call Distributor (ACD) queue after pressing prescribed digit to talk to the agent but before being answered by the agent.</td>
<td>&gt;=93% and &lt;94% meeting the target</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Target:</strong> 95% Calls</td>
<td>&gt;=92% and &lt;93% meeting the target</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each additional drop of 1% in performance below 91%, liquidated damages of 1% will be levied as additional liquidated damages</td>
<td>&gt;=91% and &lt;92% meeting the target</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;91%</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Helpdesk ticket/ Incident Response</td>
<td>Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.</td>
<td>100% within the defined target</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td><strong>Target:</strong> 15 Minutes</td>
<td>&gt;=99% and &lt;100% meeting the target</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each additional drop of 1% in performance below 95%, liquidated damages of 1% will be levied as additional liquidated damages.</td>
<td>&gt;=97% and &lt;99% meeting the target</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&gt;=95% and &lt;97% meeting the target</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Time to Resolve – Severity 1</td>
<td>Time taken to resolve the reported problem.</td>
<td>100% within the defined target</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Target:</strong> 100% of the incidents should be resolved within 120 minutes of problem reporting</td>
<td>&gt;=99% and &lt;100% meeting the target</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level as defined in Tender Document</td>
<td>&gt;=98% and &lt;99% meeting the target</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&gt;=97% and &lt;98% meeting the target</td>
<td>8</td>
</tr>
</tbody>
</table>
## APPENDIX 9 – QUALIFICATION AND SELECTION CRITERIA FOR DIGITAL SKY – SERVICE LEVEL AGREEMENT

<table>
<thead>
<tr>
<th>#</th>
<th>SLA Parameter</th>
<th>Definition &amp; Target</th>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>For each additional drop of 1% in performance below 97%, liquidated damages of 1% will be levied as additional liquidated damages.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Time to Resolve – Severity 2</td>
<td>Time taken to resolve the reported problem.</td>
<td>100% within the defined target</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Target</strong>: 100% of the incidents should be resolved within 6 hours of problem reporting</td>
<td>&gt;=99% and &lt;100% meeting the target</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level as defined in Tender Document</td>
<td>&gt;=98% and &lt;99% meeting the target</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each additional drop of 1% in performance below 97%, liquidated damages of 1% will be levied as additional liquidated damages.</td>
<td>&gt;=97% and &lt;98% meeting the target</td>
<td>7</td>
</tr>
<tr>
<td>6.</td>
<td>Time to Resolve – Severity 3</td>
<td>Time taken to resolve the reported problem.</td>
<td>100% within the defined target</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Target</strong>: 100% of the incidents should be resolved within 16 hours of problem reporting</td>
<td>&gt;=99% and &lt;100% meeting the target</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level as defined in Tender Document</td>
<td>&gt;=98% and &lt;99% meeting the target</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each additional drop of 1% in performance below 97%, liquidated damages of 1% will be levied as additional liquidated damages.</td>
<td>&gt;=97% and &lt;98% meeting the target</td>
<td>4</td>
</tr>
<tr>
<td>7.</td>
<td>Submission of Root Cause Analysis (RCA) reports</td>
<td>For all Level 1 Severity incidents resolved during the quarter, SI to submit RCA reports.</td>
<td>&lt;=5 Working days</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&gt;5 and &lt;=7 Working days</td>
<td>3</td>
</tr>
</tbody>
</table>
### Security SLAs

<table>
<thead>
<tr>
<th>#</th>
<th>SLA Parameter</th>
<th>Definition &amp; Target</th>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Security reporting</td>
<td>MIS report to be submitted on quarterly basis within pre-defined timelines</td>
<td>On time</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100% reporting of the security KPI’s (defined during project start)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Target:</strong> 100% on time reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 1 day &amp; &lt;= 5 days delay</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 5 days &amp; &lt;= 10 days delay</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 10 days &amp; &lt;= 15 days</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 15 days delay</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Patch updates</td>
<td>Availability of latest patches on the system components.</td>
<td>&gt;=98%</td>
<td>Nil</td>
</tr>
</tbody>
</table>
### APPENDIX 9 – QUALIFICATION AND SELECTION CRITERIA FOR DIGITAL SKY – SERVICE LEVEL AGREEMENT

<table>
<thead>
<tr>
<th>#</th>
<th>SLA Parameter</th>
<th>Definition &amp; Target</th>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Target:</strong> All patches released, to be</td>
<td>All patches released, to be installed on at least 98% of all applicable components</td>
<td>&gt;= 97% &amp; &lt; 98%</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>installed on at least 98% of all</td>
<td>within 48 hours</td>
<td>&gt;= 96% &amp; &lt; 97%</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>applicable components within 48 hours</td>
<td></td>
<td>&gt;= 95% &amp; &lt; 96%</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;95%</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td><strong>Target:</strong> Latest AV signature to be</td>
<td>Availability of latest AV signature on the system components.</td>
<td>&gt;=98%</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td>installed on at least 98% of all</td>
<td></td>
<td>&gt;= 97% &amp; &lt; 98%</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>applicable components within 24 hours</td>
<td></td>
<td>&gt;= 96% &amp; &lt; 97%</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&gt;= 95% &amp; &lt; 96%</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;95%</td>
<td>7</td>
</tr>
<tr>
<td>3.</td>
<td>Anti-virus (AV) signature update</td>
<td>Vulnerability Assessment for all systems / sub systems / network devices shall be</td>
<td>&lt;=10 days</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td>performed once every six months and all detected vulnerabilities closed within the</td>
<td>&gt;10 and &lt;=20 days</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cycle.</td>
<td>&gt;20 and &lt;=30 days</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&gt;30 and &lt;=35 days</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td><strong>Target:</strong> No delay</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Page 18 of 20
### Penetration Testing

Penetration Testing (external) will be conducted once every year. All detected vulnerabilities to be closed within the year.

<table>
<thead>
<tr>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=10 days</td>
<td>Nil</td>
</tr>
<tr>
<td>&gt;10 and &lt;=30 days</td>
<td>4</td>
</tr>
<tr>
<td>&gt;30 and &lt;=40 days</td>
<td>5</td>
</tr>
<tr>
<td>&gt;40 and &lt;=45 days</td>
<td>6</td>
</tr>
<tr>
<td>&gt;45 days</td>
<td>7</td>
</tr>
</tbody>
</table>

For each additional hour after 1 hour, liquidated damages of 0.05% will be levied as additional liquidated damages.

### Reporting of Security Incidents

**Target:** Detecting and reporting within 15 minutes.

<table>
<thead>
<tr>
<th>Service Level</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;15 Minutes</td>
<td>Nil</td>
</tr>
<tr>
<td>&gt;15 Minutes &amp; &lt;=30 Minutes</td>
<td>4</td>
</tr>
<tr>
<td>&gt;30 Minutes &amp; &lt;=1 Hour</td>
<td>5</td>
</tr>
</tbody>
</table>
### Project Management SLAs

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Category/ Component</th>
<th>Metric Type</th>
<th>Definition</th>
<th>Target</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reporting</td>
<td>Scheduled Reporting</td>
<td>100% adherence to time lines specified in project planning</td>
<td>100% adherence</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;100% adherence</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Reporting</td>
<td>Monitoring of the systems</td>
<td><strong>Metric:</strong> Availability of a dashboard to track and monitor 100% of the SLAs and KPIs</td>
<td>99.9%</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>How:</strong> Availability of dashboard and generation of reports in prescribed format</td>
<td>&lt; 99.9%</td>
<td>3</td>
</tr>
</tbody>
</table>