**IT STAFFING SERVICES SOLICITATION UNDER
DEPARTMENT OF INFORMATION RESOURCES
IT STAFF AUGMENTATION CONTRACT (ITSAC)**

**CANDIDATE REFERENCE**

|  |  |
| --- | --- |
| Solicitation Number: 212260061 | Title/Level: IT Auditor 2  |
| Candidate Name: | Category: Security |

|  |  |
| --- | --- |
| **Reference Name** (Required): |  |
| **Title:** |  |
| **Company Name** (Required): |  |
|  |  |
| **Phone Number** (Required include area code): |  |
| **E-mail Address:**  |  |
| **Professional Relationship:**  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Peer |  | Co-Worker |  | Supervisor |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Customer |  | End-User |  | Subordinate |

|  |  |
| --- | --- |
| **Reference Name** (Required)**:** |  |
| **Title:** |  |
| **Company Name** (Required)**:** |  |
|  |  |
| **Phone Number** (Required include area code): |  |
| **E-mail Address:**  |  |
| **Professional Relationship:**  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Peer |  | Co-Worker |  | Supervisor |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Customer |  | End-User |  | Subordinate |

|  |  |
| --- | --- |
| **Reference Name** (Required)**:** |  |
| **Title:** |  |
| **Company Name** (Required)**:** |  |
|  |  |
| **Phone Number** (Required include area code): |  |
| **E-mail Address:**  |  |
| **Professional Relationship:**  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Peer |  | Co-Worker |  | Supervisor |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Customer |  | End-User |  | Subordinate |

**NOTE: ONLY INCLUDE THE INFORMATION REQUESTED ON THIS FORM. DO NOT INCLUDE ADDITIONAL INFORMATION.**

**CANDIDATE QUALIFICATIONS**

|  |  |
| --- | --- |
| Solicitation Number: 212260061 | Title/Level: IT Auditor 2  |
| Candidate Name: | Category: Security |

|  |
| --- |
| **Minimum Requirements:** Candidates that do not meet or exceed the **minimum** stated requirements (skills/experience) will be displayed to customers but may not be chosen for this opportunity. |
| ActualYearsExperience | YearsExperienceNeeded | Required/Preferred | Skills/Experience |
|   | 5 | Required | Cybersecurity frameworks and compliance: Proven experience auditing controls against NIST, ISO 27001, PCI-DSS, or SOC 2 standards, with working knowledge of current data protection laws, regulatory compliance, and third-party risk management practices. |
|   | 5 | Required | Technical IT auditing: Strong ability to evaluate security controls such as network protection, identity access management, endpoint security, and incident response across modern IT environments. |
|   | 5 | Required | Communication and reporting: Experienced in drafting audit reports, presenting findings to executive and legal stakeholders, and engaging vendors constructively. |
|   | 5 | Required | Analytical and investigative thinking: Demonstrated ability to identify security gaps, assess risk impact, and make sound, evidence-based recommendations. |
|   | 4 | Required | Third-party/vendor risk auditing: Hands-on experience conducting cybersecurity audits of external vendors, including due diligence, contract compliance, and risk assessments. |
|   | 3 | Required | Policy and documentation review: Skilled at reviewing and validating security documentation, procedures, and control implementation for accuracy and completeness. |
|   | 3 | Preferred | Cloud cybersecurity auditing: Experience auditing vendor environments hosted in AWS, Azure, or Google Cloud, including cloud-native controls and shared responsibility models. |
|   | 3 | Preferred | Incident response and breach assessment: Familiarity with analyzing vendor incident response plans, reviewing past breaches, and evaluating remediation practices. |
|   | 3 | Preferred | Contract interpretation and SLA compliance: Ability to interpret legal and technical language in vendor contracts to ensure proper implementation of SLAs, IT, and cybersecurity obligations. |
|   | 2 | Preferred | Government or regulated industry experience: Background in auditing technology vendors serving courts. |
|   | 2 | Preferred | Presentation to executives: Experience summarizing technical findings for non-technical audiences, including C-suite executives or legal counsel. |
|   | 1 | Preferred | Certifications: At least one relevant certification (CISA, CISSP, CRISC, or ISO 27001 Lead Auditor). |

**CANDIDATE ACKNOWLEDGEMENT**

|  |  |
| --- | --- |
| RFO: 445 Solicitation Number: 212260061 | Title/Level: IT Auditor 2 |
| Candidate Name: | Category: Security |

|  |
| --- |
| I hereby authorize **Innosoul, Inc. dba Innosoul Information Technologies, Inc.** to submit my resume in response to the temporary staffing Solicitation 212260061 for **Office of Court Administration**.I understand that submission of my resume by multiple vendors may result in my disqualification from this opportunity. Customers reserve the right to hire a candidate submitted by multiple vendors.Worker signature:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |