ATTACHMENT A – KEY PERSONNEL REQUIREMENTS
List of Tables

1 KEY PERSONNEL REQUIREMENTS

1.1 General

The Contractor shall provide candidate names for each Key Personnel Profile. Subcontractor personnel may be identified as Key Personnel. All candidate Key Personnel shall meet the mandatory requirements for the proposed position.

The Contractor shall present a Key Personnel Profile Summary for each Key Personnel candidate. All Key Personnel Summary Profiles shall be identically structured in format and layout for content.

1.1.1 Key Personnel Profile Completion Information

The underlined text serves as the Key Personnel Profile Summary completion guidelines.

1. *Candidate Professional References*: Contractor shall provide at least three professional references per proposed candidate. Less than three professional references must be explained. The State may reject the candidate if less than three professional references are submitted.
2. *Education and Training:* Contractor shall list the relevant education and training of the proposed candidate and demonstrate, in detail, how a candidate's education and training relates to their ability to perform the intended duties and obligations properly and successfully in this RFP.
3. *Required Experience and Qualifications:* The Contractor shall complete this section to show how the proposed candidate meets the experience requirements for the position.

   For each proposed candidate, the Contractor must provide the following profile information:
   - Full Name of project or engagement
   - Contact Information
   - Date(s) of Experience
   - Description of Duties
4. *Résumé:* The résumé must support the candidate's education, training, experience, and qualifications outlined in the Key Personnel Profile section above.

1.1.2 Additional Completion Guidelines

1.1.2.1 Professional References

The Contractor shall provide the following information for each candidate's professional references:

1. Contact name, including title
2. Phone number
3. Email address

4. Company name
5. Mailing address

The proposed candidate's reference shall be an individual within the client's organization having proper authority on the referenced account or Product project, not a co-worker or a contact within the Contractor's organization, subsidiaries, partnerships, and so forth.

1.1.2.2 Experience Dates

The Contractor shall provide a beginning month and year and an ending month and year; specific to the time that the candidate performed in the position title or category of experience being described, technical or otherwise. It is not sufficient to only provide the length of time the proposed candidate worked for the client or the Contractor Company in general terms.

The State will not consider overlapping months of experience for a candidate as meeting or exceeding the Key Personnel Summary Profile "Mandatory Experience." It is acceptable to the State that the Contractor's proposed candidates for this RFP collectively meet or exceed the "Mandatory Experience" outlined in the tables below. If the Contractor fails to submit a candidate as Key Personnel that can fulfill the Mandatory Experience, the Contractor's Proposal may be rejected as non-responsive.

1.1.2.3 Description of Duties

The Contractor shall customize the description to substantiate the proposed candidate's qualifications. Relevant experience should be clearly described.

The State will not assume that all skill set attribute or requirement descriptions provided relate identically to every technical skill set requirement. The candidate's work experience must be listed separately and completely each time it is referenced regardless. Failure to provide this information or providing information that is inaccurate or out of date, or a client experience that is not applicable, may result in the State not including the proposed candidate's client reference in the evaluation process or rejecting the Contractor's Proposal altogether.

1.1.2.4 Résumé

The Contractor must provide a Curriculum vita (CV) or résumé for all individuals proposed as Key Personnel. The State is not imposing a format for the resume or CV; however, the it must be no more than three (3) pages long, and in the same font size as that used for the body of the technical proposal.

1.1.2.5 Exclusion of Sensitive Personal Information

It is the affirmative responsibility of the Contractor submitting a Proposal to remove all personal confidential information (such as home addresses and social security numbers) of Contractor staff and/or of any Sub-Vendor and Sub-Vendor staff from résumés or any other part of the Technical Response Packet.

Following submission to the State, all Proposals submitted become part of the public record.

All personnel assigned by the Contractor to the performance of services under this RFP shall be fully qualified to perform all duties listed in the RFP and this attachment for the proposed position.

2 KEY PERSONNEL POSITIONS

The State identified a set of key personnel to be associated with this Contract. The positions described in this section are required. Due to the importance of these positions, the State must approve in writing the assignment of a specific resource to these positions. The Contractor shall not reassign or replace a named individual from a key position without the approval of the State.

Key Personnel positions that become vacant shall have a temporary replacement in place within fourteen (14) calendar days after the position becomes vacant. The State must approve all permanent replacements.

The State requires that key personnel be available throughout the life of the Contract, as needed.

2.1 Project/Program Manager

The Project/Program Manager is responsible for the following:

1. Managing the Security project
2. Acting as the principal liaison for the Security Vendor with the State, the AME PMO, CMS, and other System Module Vendors
3. Scheduling and provisioning resources
4. Presenting all formal communication and correspondence to the State
5. Addressing any issues that cannot be resolved with Security and Privacy Controls Project Manager
6. Managing all subcontractor relationship accounts

The list above generalizes the responsibilities of the Project/Program Manager and is not intended to be all-inclusive. Table 1 details the specific qualifications that are required of the individual assigned to the Project / Program Manager position.

Table 1: Project/Program Manager Qualifications

Project/Program Manager Qualifications
1. Bachelor's degree in information technology, computer science, finance, or a related field is required 2. Minimum of five (5) years of Project Management experience where their firm has conducted independent and impartial Security and Privacy Assessments 3. Project Management Professional (PMP) certification 4. Previously managed at least one project of similar scope and size 5. Must have excellent communication skills, writing skills, small group facilitation skills, and formal presentation skills 6. Minimum of ten (10) years of relevant experience in professional services, development, client support, or project management 7. Must be able to work up to 10% of the time on-site. 8. Must have a combination of privacy and security experience and relevant assessment certifications. Examples of acceptable privacy and security experience may include, but are not limited to: • HIPAA security standards • Most current NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or the most current NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations • Minimal Acceptable Risk Standards for Exchange (MARS-E) • Federal Information Security Management Act • Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization

Project/Program Manager Qualifications
• Statement on Standards for Attestation Engagements • Center for Internet Security (CIS) benchmarks • Open Web Application Security Project (OWASP)

2.2 Security and Privacy Controls Lead

The list below generalizes the responsibilities of the Security and Privacy Controls Lead and is not intended to be all-inclusive. The Security and Privacy Controls Lead is responsible for the following:

1. Managing all subcontractor relationships, if applicable
2. Managing the engagement and serving as the chief liaison for DHS for all aspects of Independent Assessment of Security and Privacy Controls activities
3. Scheduling all work and coordinating between DHS and the Contractor
4. Ensuring alignment of all Independent Assessment of Security and Privacy Controls with State and federal expectations
5. Managing Independent Assessment of Security and Privacy Controls activities (e.g., scope, schedule, budget, resources) and providing reports
6. Executing and delegating all tasks and deliverables specified within this RFP
7. Ensuring all Independent Assessment of Security and Privacy Controls deliverables meet the required quality standards
8. Facilitating the engagement by using the project management processes, organizing the engagement, and managing the teamwork activities consistent with the approved Independent Assessment of Security and Privacy Controls Plan
9. Delivering briefings to Project team leadership with support from the Contractor team as needed

Table 2 identifies the specific qualifications required of the Security and Privacy Controls Lead.

Table 2: Security and Privacy Controls Lead Qualifications

Security and Privacy Controls Lead Qualifications
1. Bachelor's degree in information technology, computer science, finance, or a related field is required 2. Minimum of three (3) years' experience in a leadership role on an Independent Assessment of Security and Privacy Controls project for a health and/or human services system 3. Minimum of five (5) years' experience with the technical aspects of security and privacy 4. DHS requires that the Security and Privacy Controls Lead possess a combination of privacy and security experience, and relevant assessment certifications. Examples of acceptable privacy and security experience or certification include, but are not limited to: • HIPAA security standards

Security and Privacy Controls Lead Qualifications
• Most current NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or the most current NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations • Minimal Acceptable Risk Standards for Exchange (MARS-E) • Federal Information Security Management Act • Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization • Statement on Standards for Attestation Engagements • Center for Internet Security (CIS) benchmarks • Open Web Application Security Project (OWASP) 5. Hold an active certification as a Certified Information System Security Professional (CISSP) 6. Have at least one of the following relevant auditing certifications. Examples of relevant auditing certifications include: • Certified Information Systems Auditor (preferred) • Certified Internal Auditor (preferred) • Certified Information Privacy Professional • Certified Information Privacy Manager • Fellow of Information Privacy • HealthCare Information Security and Privacy Practitioner • Certified Risk Management Professional • Certified Government Auditing Professional • Certified Expert HIPAA Professional

2.3 Senior Penetration Testing Lead

The list below generalizes the responsibilities of the Senior Penetration Testing Lead and is not intended to be all-inclusive. The Security Penetration Testing Lead is responsible for the following:

1. Managing all subcontractor relationships, if applicable
2. Managing the engagement and serving as the chief liaison for DHS for all aspects of Penetration Testing activities
3. Coordinating with the Security and Privacy Controls Lead as necessary
4. Scheduling work and coordinating between DHS and the Contractor
5. Managing Penetration Testing activities (e.g., scope, schedule, budget, resources) and providing reports
6. Executing and delegating all tasks and deliverables specified within this RFP
7. Ensuring all Penetration Testing deliverables meet the required quality standards
8. Facilitating the engagement by using the project management processes, organizing the engagement, and managing the teamwork activities consistent with the approved Security and Privacy Assessment Plan (SAP).
9. Delivering briefings to Project team leadership with support from the Contractor team as needed

Table 3 identifies the specific qualifications required of the Senior Penetration Testing Lead.

Table 3: Senior Penetration Testing Lead Qualifications

Senior Penetration Testing Lead Qualifications
1. Bachelor's degree in information technology, computer science, finance, or a related field is required 2. Minimum of three (3) years' experience in a leadership role in penetration testing for a health and/or human services system 3. Minimum of five (5) years' experience with the technical aspects of security and privacy 4. DHS requires that the Senior Penetration Testing Lead possess a combination of privacy and security experience, and relevant assessment certifications Examples of acceptable penetration testing, privacy, and security experience or certifications may include, but are not limited to: • HIPAA security standards • Most current NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or the most current NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations • Minimal Acceptable Risk Standards for Exchange (MARS-E) • Federal Information Security Management Act • Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization • Statement on Standards for Attestation Engagements • Center for Internet Security (CIS) benchmarks • Open Web Application Security Project (OWASP) 5. Hold an active certification as a Certified Information System Security Professional (CISSP) 6. Have at least one of the following relevant penetration testing certifications: • CompTIA PenTest+ • EC-Council Certified Ethical Hacker (CEH) • Certified Penetration Tester (CPT) • Certified Expert Penetration Tester (CEPT) • Certified Cloud Penetration Tester (CCPT) • Certified Mobile and Web Application Penetration Tester (CMWAPT) • Certified Red Team Operations Professional (CRTOP) • EC-Council Licensed Penetration Tester (LPT) Master • Global Information Assurance Certification (GIAC) Penetration Tester (GPEN) Offensive Security Certified Professional (OSCP)