|  |  |  |
| --- | --- | --- |
| **Vendor Name:** | **Completed by:** | **Date:** |
| **Updated:** |
| **Question** | **Response** |
| **Data Protection** |
| 1 | In what geographic location(s) will DHS data be stored? Specify the timeframe in which DHS will be notified if this changes. |  |
| 2 | How does the vendor detect changes to the integrity of DHS data and what measures are in place to ensure DHS data is not lost, modified or destroyed?  |  |
| 3 | How does the vendor ensure deleted data cannot be recoverable? |  |
| 4 | How does the vendor detect degradation of DHS data? |  |
| 5 | Define a security incident.  |  |
| 6 | Describe the vendor’s incident response and reporting program.  |  |
| **Cloud Service Providers** |
| 7 | Will DHS data be stored in a cloud?  |  |
| 8 | Who is the cloud service provider? |  |
| 9 | Is the cloud service provider FedRAMP authorized and if so, specify the impact level. |  |
| 10 | If not FedRAMP authorized, specify the security framework for which the cloud service provider is certified.  |  |
| 11 | How can DHS be assured cloud service providers meet the same security standards as that of the vendor? |  |
| **Access Control** |
| 12 | Who has access to the systems providing DHS data and services? How is this access controlled? |  |
| 13 | What authentication method is required to access DHS data and applications (e.g. username and password)? |  |
| 14 | Which multi-factor authentication methods does the vendor support? |  |
| 15 | Does the vendor allow the use of personal devices for access to DHS data? |  |
| 16 | Specify the frequency vendor staff access to DHS data is reviewed. |  |
| 17 | Which access control methodology does the vendor support: Role-based access control (RBAC), mandatory access control (MAC), or discretionary access control (DAC)? Define how you meet this methodology. |  |
| **Regulatory Compliance** |
| 18 | Is the vendor a HIPAA covered entity?  |  |
| 19 | Is the vendor a business associate of DHS? If yes, does the vendor have downstream business associate agreements with subcontractors? |  |
| 20 | Define the vendor’s HIPAA training. List the training modules and the time allotted for each module. |  |
| 21 | Is the vendor audited or assessed by a third party? If yes, specify the security framework.  |  |
| 22 | Explain how the vendor performs an information security risk assessment. What is the frequency? |  |
| 23 | Explain how the vendor manages their information security risk assessment program. |  |
| **Business Continuity and Resiliency** |
| 24 | Does the vendor have a business continuity plan?  |  |
| 25 | How often is the business continuity plan tested? |  |
| 26 | How does the vendor ensure DHS can continue doing business at all times, even if there is a permanent catastrophic failure or natural or man-made disaster where DHS data or services are located? |  |
| 27 | What guarantees does the vendor provide for recovery time objectives (RTO) and recovery point objectives (RPO)? |  |
| **Service and Data Integrity** |
| 28 | Is DHS data encrypted in transit? If so, specify the encryption algorithm and cipher strength. Who owns the encryption key? |  |
| 29 | Is DHS data encrypted at rest? Is so, specify the encryption algorithm and cipher strength. Who owns the encryption key? |  |
| 30 | Specify the network security tools used to monitor data flow into the vendor’s network for malware or cyber-attacks. |  |
| 31 | What tools and procedures does the vendor utilize for intrusion detection and at what frequency? How is this capability tested for functionality at the hardware, network, and database levels?  |  |
| **Multi-Tenancy** |
| 32 | How does the vendor separate DHS data and services from those of other clients? |  |
| 33 | In what ways could the vendor’s other client’s affect the quality of the service or service levels provided to DHS? |  |
| 34 | What resources will DHS share with other clients? |  |
| **Infrastructure and Application Security** |
| 35 | Who owns and operates the vendor’s data centers and what physical and environment security measures are in place? |  |
| 36 | What parts of the vendor’s infrastructure are owned and operated by the vendor and what parts are obtained from a colocation service? |  |
| 37 | What standards are followed for hardening network equipment, operating systems, and applications? |  |
| 38 | Specify the tools used to perform vulnerability scans and the frequency. What is the timeframe to re-mediate high and critical findings? |  |
| 39 | Specify the frequency of third party penetration tests to assess infrastructure security. Include the type of third party report received.  |  |
| 40 | What specifications does the vendor follow to purge data when equipment is retired or replaced? How does the vendor purge any resident DHS data? |  |
| 41 | Does the vendor utilize a web application for this service? If so, does the vendor follow the OWASP Top 10 List? |  |
| **Non-production Environment Exposure** |
| 42 | Is DHS data loaded to a test environment? If so, who has access to the test environment? |  |
| 43 | Which copies are de-identified and which are not? |  |
| 44 | Is live DHS data used in testing? |  |