# [FBOP Proposed Attestation]

**[BOP RRC, CMS & Credit Reporting Contracts: To Address ATU concerns]**

The vendor affirms that they have security controls in place to protect DOJ information when that data is being stored, transmitted, processed, or displayed on the vendor's information technologies. Applicable security controls include certifications indicating compliance with: state licensure requirements, SOC 2, ISO 27001, Payment Card Industry, HIPAA as applicable or other environment certifications that would be applicable (to be specified by the vendor). **Vendor has attached documentation of said certifications as part of this affirmation.**

The vendor affirms that internal controls are in place to identify and remediate vulnerabilities within any IT system in which DOJ information is stored and that DOJ data will be stored exclusively within the boundaries of the United States and that only US citizens have access to DOJ's data. The vendor affirms that any DOJ information made available to vendor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. The vendor shall neither reproduce nor release such information to any third-party at any time, including during or after performance of the contract, without prior written permission of the CO or COR.

The vendor agrees to report any actual or suspected breach of DOJ Information within one hour of discovery of an actual breach, and within 24 hours of a suspected breach if vendor has not yet been able to determine whether a breach has occurred. A "breach" is an incident or occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses DOJ Information or (2) an authorized user accesses or potentially accesses DOJ Information for an other than authorized purpose. The report of a breach must be made to the CO or COR; if neither can be reached, the vendor must report the breach to the DOJ Security Operations Center (jsoc@usdoj.gov, 202-357-7000) and FBOP's Information Security Program Office; the COR; and the Contracting Officer within one (1) hour of the initial discovery. The vendor should not disclose any details of the potential or confirmed breach to any individual not involved in responding to the breach. The vendor agrees to cooperate with DOJ's inquiry into the incident and efforts to minimize risks to DOJ or individuals. Such cooperation includes, but is not limited to, providing to DOJ full access to any facility and/or Information System affected or potentially affected the breah or potential breach, and to undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. The vendor further agrees that it shall be responsible for all costs and related resource allocations that DOJ deems required for all such response activities related to any breach.

## A. Vendor Information Types Questions

| Yes | No | N/A | Description |
|---|---|---|---|
| | | | Is the data sensitive (as defined by NIST)? |
| | | | Does the data contain Personally Identifiable Information (PII)? |
| | | | Does the data contain Federal Tax Information (FTI)? |
| | | | Does the data contain Protected Health Information (PHI)? |
| | | | Does the data contain other Limited Official Use Information:<br>Legal Privilege Legal Strategy Grand Jury Title III Information<br>Protected Materials Privacy Act Procurement Sensitive Intellectual Property<br>Law Enforcement Sensitive Infrastructure Sensitive |
| | | | Approximately how many records will be transmitted to the vendor during the contract period? |

## B. Vendor Information Security Questions

| Yes | No | N/A | Description |
|---|---|---|---|
| | | | Is Multi Factor Authentication (MFA) used to access DOJ data? |
| | | | Describe implementation:<br>Explain N/A: |
| | | | Is the principle of least privilege employed for access management? |
| | | | Describe implementation:<br>Explain N/A: |
| | | | Is sensitive data encrypted at rest and/or in transit (e.g., sensitive Personally Identifiable Information (PII), Federal Tax Information (FTI), health information (HIPAA))? |
| | | | Describe implementation:<br>Explain N/A: |
| | | | Do portable devices require mobile device management tools before allowing access to corporate data, including email? |
| | | | Describe implementation:<br>Explain N/A: |
| | | | Is there a formal cyber security program which includes policy enforcement? |
| | | | Describe implementation:<br>Explain N/A: |
| | | | Are routine vulnerability scans of all system assets and endpoints performed? |

| Yes | No | N/A | Description |
|---|---|---|---|
| | | | Describe implementation:<br>Explain N/A: |
| ☐ | ☐ | ☐ | Are internal and external penetration tests conducted? |
| | | | Describe implementation:<br>Explain N/A: |
| ☐ | ☐ | ☐ | Are known vulnerabilities mitigated or remediated within 30 for critical and high risk, and 90 days for medium risks? |
| | | | Describe implementation:<br>Explain N/A:<br>o Critical Patch - to be installed within 30 days or sooner if possible<br>o High Risk Patch - to be installed within 60 days or sooner if possible<br>o Medium Risk Patch - to be installed within 90 days or sooner if possible<br>o Low Risk Patch - to be installed within the normal patching rotation, but within at least a year. |
| ☐ | ☐ | ☐ | Are monitoring services employed which will notify resources as needed 24x7x365 to support incident response? |
| | | | Describe implementation:<br>Explain N/A: |
| ☐ | ☐ | ☐ | If sub-contractors are used, describe questionnaire and other requirements of sub-contractors:<br>Describe implementation:<br>Explain N/A: |

## C. Data Owners

| Role | Responsible Party | Responsibilities |
|---|---|---|
| Data Steward | | Entity who is responsible for the categorization, protection, usage, and quality of the data. |
| Data Steward | | Entity who is responsible for the confidentiality, integrity, and availability of the data on a day-to-day basis. |
| Data Steward | | Entity who is responsible for the confidentiality, integrity, and availability of data on a day-to-day basis. |

## D. Vendor Signature

| | |
|---|---|
| | As the vendor representative, I attest that the information in sections A and B are accurate, and I accept the responsibility of protecting and ensuring the confidentiality, integrity, and availability of DOJ data on a day-to-day basis when it is on the vendor or subcontracted vendor networks. |