Federal Communications Commission
Broadband Data Collection

Wireless Network Engineering & Consulting Support Services

Performance Work Statement

7 November 2022

Prepared by:
Federal Communications Commission
Office of Economics and Analytics
45 L Street NE
Washington, DC 20554

CONTENTS

Performance Work Statement

1 BACKGROUND

The Broadband DATA Act (BDA), enacted in March 2020, requires the Federal Communications Commission (FCC) to collect more granular and consistent data from broadband internet access service providers on the availability and quality of broadband service. Among other provisions, the BDA requires the FCC to establish processes to evaluate the coverage data collected from fixed and mobile wireless broadband service providers. Pursuant to the BDA, the FCC has implemented a new Broadband Data Collection (BDC). Mobile broadband service providers must submit network coverage maps (voice, 3G, 4G LTE, and 5G-NR) based on standardized requirements, as well as supplemental data about how the maps were generated to support their broadband coverage claims. Similarly, fixed wireless broadband service providers must submit broadband coverage data in the form of either propagation maps and model details or a list of addresses or locations; if the provider submits coverage maps, it must provide additional information with its maps and model details. Moreover, mobile wireless service providers may submit on-the-ground speed test data or infrastructure data (or both), as well as potentially other data, as part of the FCC's mobile challenge and verification processes. ***See Broadband Data Collection Mobile Technical Requirements Order, DA 22-241, Mar. 9, 2022*** *(Mobile Technical Requirements Order).*

The FCC's Broadband Data Task Force (BDTF), together with other FCC Bureau's and Offices, has designed and developed an overarching Broadband Data Collection System (BDC System) to collect, validate, and publish complete, granular, and reliable data on broadband availability. *See* https://www.fcc.gov/BroadbandData. The key outputs of the BDC System will be public-facing broadband maps with granular information helping to pinpoint where broadband service is available and where it is not available. The FCC, other federal agencies, and other stakeholders will use these broadband maps to make decisions about where service is needed and how to fund the expansion of broadband services.

Challenge Process. The BDA requires the FCC to establish a challenge process to enable consumers, governmental entities, and other third parties to challenge, or formally dispute, the accuracy of the broadband coverage maps or other information submitted by a provider regarding the availability of its broadband internet access service.

For mobile challenges, consumers, governmental entities, and other third-party entities must submit the results of speed tests based on specific parameters and include certain metrics. The FCC will aggregate and evaluate—by the testing environment (i.e., outdoor stationary or in-vehicle mobile) and technology type—valid speed tests submitted by challengers. The FCC will apply the methodology adopted in the Mobile Technical Requirement Order to analyze the speed

test data and determine whether the three thresholds for a "cognizable" challenge—geographic, temporal, and testing—have been met and, if so, the geographic boundary of the area subject to the cognizable challenge.

Mobile service providers must either respond to a cognizable challenge or concede and have the challenged area identified on the mobile coverage map removed. Providers may rebut a challenge with on-the-ground test data or, in certain circumstances, infrastructure data, so that the FCC may resolve the challenge.

Verification Process. The BDA also requires the FCC to verify the accuracy and reliability of the broadband Internet access service data that service providers submit. For mobile verification inquiries, FCC staff may request and collect verification data from mobile service providers on a case-by-case basis where staff have a credible basis for requiring verification of a provider's coverage data. Staff will rely upon all available evidence to determine whether there is a credible basis for initiating a verification inquiry. For fixed wireless providers using propagation maps and models to report broadband availability, the FCC requires such filers to provide certain infrastructure parameters and details (e.g., details of their radio network planning tools, base stations, terrain and clutter, customer premise equipment (CPE) antennas, link budgets) to allow FCC staff, members of the public, and government entities and third parties to independently verify the accuracy of the filers' maps and propagation models through audits, investigations, the challenge process, and the crowdsource process.

The FCC will supply mobile providers with a statistically valid sample of an area subject to a verification request (the targeted area). In response to the verification request, a mobile provider must submit either on-the-ground test data or infrastructure information for the specified area(s). The provider may also submit additional data that it believes supports its reported coverage. FCC staff will analyze the information submitted by a provider in response to a verification request to determine whether the provider has successfully demonstrated accurate coverage in the targeted area.

The FCC may also conduct general data quality checks separately from the formal verification process. These general data quality checks would focus on review of the availability data based on submitted supporting data.

Audit Process. The BDA requires the FCC to conduct regular audits of information submitted by providers. FCC staff may randomly conduct audits of a provider's coverage area to verify coverage and request and collect data in conjunction with such audits. Audit tools will include field surveys, investigations, and annual random audits to verify data accuracy. In addition, audits may be initiated based on an unusual number of crowdsource complaints.

Crowdsource Process. The BDA requires the FCC to "develop a process through which entities or individuals . . . may submit specific information about the deployment and availability of broadband internet access service . . . on an ongoing basis . . . to verify and supplement information provided by providers." Various entities, as well as consumers, may submit

crowdsource data to the FCC. Mobile crowdsource data are evaluated through a combination of automated processing and further review by FCC staff. The automated process identifies areas for further review. Staff then review the identified potential targeted areas and any other relevant data to determine whether the data presents a credible basis to warrant verification.

Propagation Modeling Tool. To augment the analytical capability of the BDC system and effectively evaluate and verify broadband maps, the FCC has licensed Forsk's propagation modeling tool, Atoll/Naos, an industry-leading software solution/automation platform (hereinafter referred to as the "Propagation Modeling Tool" or "PMT"). In general, the PMT provides capability to conduct propagation modeling for commercial wireless services, including access to various geographic data (GeoData) sources as inputs to the PMT. The vendor that is awarded this contract (hereinafter "Contractor") is expected to be proficient in propagation modeling tools and techniques. Experience with the Forsk Atoll/Naos platform is preferred, but not required.

2 OBJECTIVES

The FCC has established a biannual schedule for the collection of information on broadband service availability and quality of service. Mobile wireless providers are required to submit propagation maps reflecting technology-specific user download and upload speeds given prescribed minimum cell edge probabilities, cell loading factors, and modeling resolution. In addition to maps, mobile wireless providers are required to disclose to the FCC details of their propagation models and the link budgets that they use for modeling cell edge network throughput. Fixed wireless service providers that choose to submit availability data using propagation maps and modeling details must similarly provide the FCC with details of how they generated their propagation maps and models, including details about their radio network planning tool(s), base stations, terrain and clutter, link budgets and other parameters, and receiver and customer premises equipment antennas. Complete details of the data to be submitted biannually can be found in the Data Specification for Biannual Submission of Subscription, Availability, and Supporting Data document published by the FCC.[1]

To support implementation of the BDA requirements, the FCC requires wireless engineering, analytical, and consulting advisory support and services for ongoing review and analysis of data submitted by fixed wireless and mobile wireless service providers (including coverage maps, propagation modeling results, link budgets, network monitoring results, infrastructure data, and

[1] The data required from, and submitted by, providers include certain contact information, which the FCC considers to be personally identifiable information (PII), subject to applicable Federal laws and requirements. Because these data will be shared with Contractor, Contractor is responsible for maintaining and processing such data in a manner consistent with Federal laws and requirements, as set forth in greater detail in Section 10. PII is defined as information that can be used to distinguish or trace an individual's identity, alone or when combined with other information that is linked or linkable to a specific individual.

methodology details), public and anonymized challenge and crowdsource data from various entities and stakeholders,[2] and data related to the challenge, verification, and audit processes. Support of these tasks may require engagement with fixed wireless and mobile wireless service providers and other stakeholders to clarify, analyze, and validate all required data and reporting. Through this support, the FCC is seeking to:

- Enhance the FCC's ability to accurately assess and verify fixed wireless and mobile wireless coverage maps and related supporting data submitted by service providers as part of the BDC availability, challenge, verification, crowdsource, and audit processes;
- Obtain support for review and analysis of biannual coverage maps and supporting data, including infrastructure data, link budgets, wireless providers' propagation models, and clutter data, which could include engagement, as necessary, with fixed wireless and mobile wireless service providers for clarification of supporting data;
- Produce and analyze outputs of the PMT under different conditions based on the fixed wireless and mobile wireless providers' supporting data (e.g., traffic load, link budget, infrastructure data) and transmit the results to the FCC's BDC system for comparison with submitted coverage maps;
- Review and evaluate the results produced by the BDC system of the comparison of the PMT with the submitted coverage maps;
- Develop and review plans for the FCC to conduct on-the-ground (OTG) mobile speed tests as necessary to support the audits of coverage maps, and evaluate test results;
- Create documentation such as recommendations to support the evaluation of the data and coverage maps that can be shared within FCC, with challengers, and/or with service providers;
- Communicate and engage with service providers as necessary regarding the assessment of coverage maps and resolve any potential issues; and
- Establish and continuously improve BDC propagation modeling, challenge, verification, crowdsourcing, and audit processes to effectively and efficiently meet BDA requirements.

[2] As discussed at greater length below, the FCC will disclose to Contractor—or limit Contractor's access to—only challenge and crowdsource data elements that are anonymized or otherwise have been made public.

3 SCOPE

As further detailed in Section 4, the FCC requires support in three primary task areas:

1. **Task 1: Program Management Support** – Includes overall workload planning and management, assessment and triage of all BDC fixed wireless and mobile wireless requests or inquiries from the FCC to assist the FCC in prioritizing, sequencing, and executing the required analyses, and all general program management activities, including, but not limited to, staffing, project management, contract financial management, status and progress reporting, quality control, risk management, and support for a range of stakeholder communications and briefings.

2. **Task 2: Fixed Wireless and Mobile Wireless Engineering Support** – Includes a broad range of technical engineering and analytical services required to support the BDC processes described above.

3. **Task 3: Special Projects (Optional Task)** – At the FCC's discretion during any performance period, but only upon the Contracting Officer's written authorization to proceed, the Contractor shall support Special Projects related to the task areas above. Refer to Section 4.3 for additional details.

4 DETAILED REQUIREMENTS

Specific requirements for each of the three tasks defined in Section 3 are further detailed below.

4.1 TASK 1: PROGRAM MANAGEMENT

The FCC requires a range of program management support to manage the workload allocation, staffing, quality control, reporting, and administration of all activities under this support contract.

4.1.1 Assessment & Triage of BDC Inquiries

The Contractor shall support the intake, review, assessment, and triage of the BDC inquiries from FCC staff and other sources identified by the FCC, which will assist FCC personnel in prioritizing, sequencing, and executing the required analyses and reporting within specified timeframes. The Contractor shall also provide higher-tier technical assistance with BDC inquiries from FCC stakeholders and the public, specifically the review, analysis, and recommended resolution of certain trouble tickets received through the BDC Help Center.

4.1.2 Program / Project Management & Administration

The Contractor shall provide a range of Program and Project Management support activities, including, but not limited to, staffing and workload planning and management, project management, contract financial management, status and progress reporting, quality control, risk management, and support for a range of stakeholder communications and briefings. As further described in Section 5 Deliverables, the Contractor shall work with the FCC to develop agreed upon templates to be used in providing weekly status reports and executive briefings upon request.

The Contractor shall develop an overall Program Management Plan, as defined below, by documenting a comprehensive approach to meeting the objectives and requirements outlined in the PWS. As described in Section 5 Deliverables, the Contractor shall work with FCC post award to finalize the draft Program Management Plan and its components submitted with its proposal. The overall Program Management Plan shall include, at a minimum, the following elements:

- **Project Management Plan** including key activities, milestones, and government review/approval points throughout the period of performance;
- **Staffing Plan** documenting personnel to be utilized on the effort and their qualifications, as well as the overall approach to ensuring availability of qualified personnel on an ongoing basis
    - If sub-contracting any portion of the work, please provide the name(s) and address(es) of all subcontractor(s) (if applicable) and a description of their planned subcontracting effort;
    - See PWS Section 10 and Clause LOCAL-27 Security Requirements Suitability and Security Processing for additional personnel requirements;
    - ***See PWS Section 9 for additional requirements for the Staffing Plan***;
- **Quality Assurance Plan** documenting the approach to be used to ensure high-quality and on-time delivery of the end product, including proposed key performance indicators (KPIs);
- **Communications Plan** including approach to engaging with FCC leadership, technical personnel, fixed and mobile wireless broadband service providers, and other external stakeholders (as needed) to support the requirements of the PWS and provide progress updates as required. Additionally, the communications plan shall document the communications channels and escalation path within the Contractor's organization for resolution of any critical issues unable to be resolved through the Contractor's Project Manager; and

- **Training and Documentation Plan** outlining the approach to training and codification of key processes and analyses to support process improvement and execution efficiency gains over time.

The FCC will work with the selected Contractor in the week following award to review, update, and finalize the draft plans submitted in the Contractor's proposal.

4.2 TASK 2: FIXED WIRELESS AND MOBILE WIRELESS ENGINEERING SUPPORT

The Contractor shall provide wireless engineering, analytical, and advisory services to support the FCC's challenge, verification, crowdsourcing, and audit processes and related coverage analyses and process improvement activities, as described below.

The task areas detailed in this section represent the types of analytical and advisory support anticipated to be required and the general skills and experience necessary to provide the support but should not be considered an exhaustive list of all required support. As various challenge, verification, audit, and other BDC processes are rolled-out for the first time, there will necessarily be a period of process review and refinement that may require additional types of related analysis and advisory support. Additional details of the requirements related to FCC's mobile challenge and verification processes are provided in the Mobile Technical Requirements Order.

4.2.1 Review of Biannual Coverage Maps and Supporting Data

To support the review of the BDC coverage data submitted by fixed wireless and mobile wireless providers biannually, the Contractor shall provide a range of analytical and advisory services at the direction of the FCC, including, but not limited to:

- Link Budget Review and Quality Control
    - Review and understand the specifications for Fixed and Mobile Broadband Supporting Data published in sections 7 and 9 of the BDC availability data specifications (https://us-fcc.app.box.com/v/bdc-availability-spec)
    - Identify potential issues with a provider's link budget when comparing it to the provider's coverage map for a particular technology (e.g., 3G, 4G, or 5G)
    - Identify patterns and potential issues across link budget submissions from multiple service providers (large range of value for similar link budget parameters, unexplained gains or losses, certain values resulting in an overstatement of coverage or a relatively large number of cognizable challenges, etc.)

- Propagation Model Review and Quality Control
  - Review and understand the specifications for propagation modeling information published in sections 7 and 9 of the BDC availability data specifications (https://us-fcc.app.box.com/v/bdc-availability-spec)
  - Compare propagation model types and parameters across providers and with coverage areas to identify patterns or potential issues

Deliverables

Sample outputs and deliverables required under this task may include, but are not limited to:

- Report summarizing the results of link budget and propagation model reviews
- In the event deficiencies, anomalies, deviations from industry standards or engineering best practices, or other issues are identified, documentation describing the issue(s) and any recommended actions

4.2.2 Verification, Challenge, Crowdsource & Audit Support

The FCC has established several primary methods by which staff can assess and confirm the accuracy of wireless provider coverage maps:

- **Verification Inquiries:** On a case-by-case basis, FCC staff can initiate a coverage verification inquiry where staff has a credible basis for questioning the accuracy of a provider's coverage maps.
- **Challenges:** Consumers may submit OTG test data collected with the FCC Speed Test App or an approved FCC App to indicate that a mobile wireless broadband provider has submitted inaccurate or incomplete coverage maps. Additionally, governmental entities, third parties, and other mobile providers may submit OTG mobile test data collected with an approved FCC App or collected using their own hardware and software, provided the submitted data meet the FCC-required set of metrics.[3] OTG data will be aggregated to create challenges to mobile provider coverage data.
- **Crowdsource Data:** Consumers and third parties may submit crowdsource data to provide information to the FCC about deployment and availability of both fixed and mobile broadband service at specific locations. Mobile crowdsource data are evaluated through a combination of automated processing and further review by FCC staff. Fixed

[3] Challenge and crowdsource data include data elements that are, or could reveal, PII. The FCC will disclose to Contractor—or limit Contractor's access to—only challenge and crowdsource data elements that are anonymized or otherwise have been made public, the latter of which, under the BDC Third Report and Order, include the location that is the subject of a challenge. *Establishing the Digital Opportunity Data Collection; Modernizing the FCC Form 477 Data Program*, WC Docket Nos. 11-10 and 19-195, Third Report and Order, 36 FCC Rcd 1126, 1174, para. 125 (2021). The FCC will not disclose to Contractor—or provide Contractor access to—any other challenge or crowdsource data elements that include or could reveal PII, such as contact_name, contact_email, contact_phone, server_timestamp, server_source_ip_address, server_source_port, device_imei, device_id.

crowdsource data are evaluated by FCC staff to identify individual instances or patterns of potentially inaccurate or incomplete availability data that warrant further investigation or review.

- **Audits:** FCC staff may initiate an audit of a wireless provider's coverage map, which may include the collection of OTG test data.

The Contractor shall provide support for each of these processes as further described below.

4.2.2.a Verification Process Support

Based on the challenge, crowdsource, or other data submitted in the BDC system, the FCC will determine from the BDC system areas of a mobile provider's coverage map that require additional data to support the mobile provider's coverage claims. Mobile providers may submit infrastructure data and/or OTG measurement data to support their coverage maps in the area(s) targeted for verification (and may also include transmitter monitoring software data as a supplement to OTG or infrastructure data).

In supporting the requirements of the Verification Process, the Contractor shall provide engineering, analytical, and advisory services, including, but not limited to:

- Review and confirm the areas flagged in the BDC system for verification.
- Use the Forsk product suite (Atoll/Naos), accessible via the BDC system, to generate "core coverage" areas (as defined in the Mobile Technical Requirements Order), compare the newly created "core coverage" map results to the service provider's submitted coverage maps, and make sound determinations on the accuracy of the submitted coverage maps and verification responses.
- If the service provider submits infrastructure data in response to a verification request:
    - Review the infrastructure data to ensure consistency with the relevant data specification.
    - Using the biannual data submitted by mobile and some fixed wireless providers (link budget, clutter information, propagation model), prepare and submit a core coverage analysis request to the PMT.
    - Review and analyze the BDC system's comparison of provider-submitted coverage maps with the PMT-generated coverage maps. Document any PMT parameter settings that could cause differing results.
- If the service provider submits OTG data in response to a verification request:
    - Review submission and confirm that all the required fields are consistent with the relevant data specification.
    - Support submission of the measurement data to the BDC system for comparison with the service provider's maps.

- Support, as needed, to respond to any service provider appeals of adverse BDC verification results, including, but not limited to:
    - Additional supporting analysis or documentation development.
    - Supporting engagement and communications with service providers to gather or verify additional information related to the appeal.

Deliverables

Deliverables required under this task may include, but are not limited to:

- Document all parameter settings used in the PMT analysis. All PMT analyses should be reproducible.
- Document any findings with respect to completeness and compliance with the relevant data specifications of the infrastructure or OTG data submissions from the provider. Identify possible amendments to the data specifications that would enhance the efficiency of the BDC system (for example the removal of unnecessary fields from the data specification, the addition of newly identified useful fields to the data specifications, or the optimization of the allowed value ranges of the fields in the published data specifications).
- Higher tier technical support, including, for example, providing guidance and support on escalated BDC technical parameter questions from mobile providers.

4.2.2.b Challenge Process Support

Based on challenge data submitted by consumers, governmental entities, third parties, or other service providers (collectively "challengers"), the system will identify H3 hexagon grid areas that are subject to challenge. In rebuttal of a challenge, mobile providers may submit infrastructure data to identify tests within the challenger speed test data set that the provider claims are non-representative of network performance in six circumstances; 1) extenuating circumstances at the time/location of a given test, 2) mobile device was not capable of using or connecting to the technology or spectrum band that the provider models for service in the challenged area, 3) test was taken during an uncommon special event, 4) test was taken during a period of abnormally high network loading, 5) mobile device used a data plan that could result in slower service, and 6) mobile device was either roaming or using Mobile Virtual Network Operator (MVNO) at the time of the test. Otherwise, the wireless provider should submit OTG measured data in rebuttal of a challenge.

In supporting the requirements of the Challenge Process, the Contractor shall provide a range of analytical and advisory services, including, but not limited to:

- Review and adjudication of provider responses to challenges.
- If the service provider submits infrastructure data:
    - Review submission for completeness and document any deficiencies in the data.

  - Review the explanation of why the provider has submitted infrastructure data. The circumstances include, but are not limited to:
    - Review the network loading factor at the time of the OTG test result (as submitted by the provider) and compare it to the information included in the link budget used to create the filer's coverage map.
    - Confirmation that an uncommon special event occurring within the location of the challenge could have impacted the OTG test results, including initiating PMT analysis of area, if warranted.
    - Review capabilities of testing device and confirm that it cannot connect to the network under challenge due to technology or frequency bands
    - Determine if the infrastructure data matches the OTG data metadata (Cell ID/PCI, frequency band). If not, does the service provider offer a satisfactory explanation?
    - Review OSS based Key Performance Reports submitted by service providers and determine if the cell loading criteria was satisfied.

- If the service provider submits OTG measurement data:
  - Review data (spreadsheets, tables, charts, datasheets, etc.) and detailed system specifications submitted by mobile service providers, governmental entities, and third-party challengers that choose to use their own software and hardware to collect OTG test data for mobile challenges and ensure the systems used meet FCC requirements and specifications.
  - If during the challenge rebuttal process additional supporting or non-supporting measurement data are submitted to the BDC, the Contractor shall support review of the rebuttal results in light of the additional data and recommend/document further necessary actions.

- Support, as needed, to respond to any service provider appeals of adverse decisions on mobile challenges, including, but not limited to:
  - Additional supporting analysis or documentation development.
  - Supporting engagement and communications with service providers to gather or verify additional information related to the appeal.

Deliverables

Sample outputs and deliverables required under this task may include, but are not limited to:

- Documentation supporting successful or unsuccessful challenge rebuttal.
- Documentation supporting technical review of methodology for entities using their own software and hardware to collect speed test data for the Mobile Challenge Process to ensure the required metrics are met.
- Higher tier technical support, including, for example, providing guidance and support on escalated BDC technical parameter questions from mobile providers.

4.2.2.c Audit Process Support

The FCC may initiate an audit of a service provider's coverage map. In the case of mobile wireless broadband availability data, FCC staff will initiate an OTG speed test of the audit area and report results back to the BDC system. In the case of fixed wireless broadband availability data, the FCC may initiate an audit of a fixed wireless provider's propagation maps and model details, or list of broadband locations, using such audit tools as, for example, field surveys, investigations, statistical analyses, and random annual audits—all based on the provider's fixed wireless infrastructure information. The Contractor shall provide a range of analytical and advisory services, including, but not limited to:

- Review audit area and support generation of speed test routes to be given to staff who will conduct the actual collection of OTG data.
    - Use previously submitted infrastructure data to support drive route generation, if applicable.
- Review collected OTG data and confirm that the speed test followed routes specified and/or document exceptions.
- Support, as needed, to respond to any service provider appeals of audit results, including, but not limited to:
    - Additional supporting analysis or documentation development.
    - Supporting engagement and communications with service providers to gather or verify additional information related to the appeal.

Deliverables

Sample outputs and deliverables required under this task may include, but are not limited to:

- Documentation of speed test routes.
- Documentation of test results.
- Higher tier technical support, including, for example, providing guidance and support on escalated BDC technical parameter questions from mobile providers.

4.2.2.d Crowdsource Process Support

Mobile crowdsource data will be evaluated through a combination of automated processing and further review by FCC staff. The automated process will identify areas for further review by first excluding or "culling" any anomalous or otherwise unusable speed test information and then using data clustering to identify groupings of potential targeted areas where a provider's coverage map is inaccurate that would trigger further review. Staff will then review the identified potential targeted areas and any other relevant data to confirm whether this cluster presents a credible basis to warrant verification. Areas identified from crowdsourced data using this methodology would be subject to a verification inquiry consistent with the mobile verification process.

In supporting the crowdsource process, the Contractor shall provide a range of analytical and advisory services, including, but not limited to:

- Assessment of areas identified for further review by automatic process.
- Review available evidence, such as speed test data, infrastructure data, crowdsource and other third-party data, and the staff's review of submitted coverage data, including coverage maps, link budget parameters, and other credible information to determine whether a credible basis for conducting a verification inquiry has been established and whether a verification request is appropriate.

Deliverables

Sample outputs and deliverables required under this task may include, but are not limited to:

- Documentation supporting determination of credible basis for initiating verification inquiry.
- Higher tier technical support, including, for example, providing guidance and support on escalated BDC technical parameter questions from mobile providers.

4.2.3 Process Improvement Support

The Contractor shall provide analytical, consulting, and advisory services to support overall quality control and continuous improvement assessments of BDC systems, tools, processes, and analytical methods. Specifically, the Contractor shall:

- Support BDC Core Coverage Generation and Quality Control.
  - Review the automatically generated results from the Forsk propagation modeling product suite for accuracy and completeness.
  - Identify potential ways to improve the configuration of the Forsk tools used in automation to enhance the accuracy of the automatically generated results.

- Consulting services to assist FCC staff with evaluating the effectiveness of the Mobile Challenge Process, Mobile Verification Process, and other aspects of the BDC processes from a technical engineering perspective, to ensure that the quality of reported data furthers the goals of the overall BDC program. Upon FCC request, support would include:
  - Performing an evaluation of the types and quality of the challenge data, provider response data, and coverage data.
  - Identifying areas where the various BDC processes are not necessary, are not providing an adequate technical picture, or are producing anomalous results of the on-the-ground reality related to coverage and developing recommended process improvements.

- Making recommendations or technical/engineering improvements to ensure/improve data quality and system integrity in the overall BDC data collection process.
- Identifying additional process improvements, automation opportunities, and other potential efficiencies to improve the overall effectiveness of the challenge and verification processes.

4.2.4 Analytical Support

In providing support across the task areas in this PWS, the Contractor shall apply knowledge and expertise in relevant modeling and statistical analysis tools and techniques, including, but not limited to, the following:

- **Propagation Modeling Tool (PMT):** As noted in Section 1, in support of the wireless engineering task areas in this PWS, the FCC has licensed Forsk's Atoll/Naos propagation modeling tool (PMT). The Contractor shall possess demonstrated proficiency in general propagation modeling tools and analytical techniques. Experience working with the Forsk Atoll/Naos platform is desired. If there is no experience working with Forsk Atoll/Naos, give examples of other PMT modeling tools in which there is proficiency.

- **Statistical Analysis:** The Contractor shall be proficient in, and have practical experience using, various tools to perform statistical analysis and shall apply these tools to derive metrics from data submitted by service providers and/or produced in the BDC system. Provide examples of the tools where experience is possessed and describe that experience. Sample tools and analysis types include, but are not limited to the following:
  - Example tools: SAS, SPSS, R, etc.
  - Examples of required statistical analyses:
    - Derivation of statistical metrics of service providers' wireless coverage as well as metrics related to the challenge and verification cases.
    - Follow-on Spatial Interpolation Analysis Using GIS tools, such as ArcGIS, QGIS, PostGIS etc. to perform spatial interpolation techniques such as Kriging using available OTG data to (1) predict coverage for areas of interest, and (2) evaluate and verify accuracy of coverage maps.

- **Data Analytics and Visualization:** The Contractor shall be proficient in, and have practical experience using, data analytics and visualization tools to create informative and impactful data visualizations and summary reports. The Contractor shall apply such tools to effectively review, manage, and analyze the data submitted by service providers or produced in the BDC system to create data visualizations to support recommendations and final decision making by FCC management. Provide examples of the tools where experience is possessed and describe that experience.

- Example tools: Tableau, Alteryx, Microsoft Excel, Power BI, and RDBMS tools such as PostGreSQL
- Examples of required analytics and visualizations:
  - Display of USA maps with wireless coverage from data submitted by service providers
  - Visualization of statistical metrics of service providers' wireless coverage as well as metrics related to the daily operations of challenge and verification processes

4.3 TASK 3 (OPTIONAL): SPECIAL PROJECTS

At the FCC's discretion during any performance period, but only upon the Contracting Officer's written authorization to proceed, the Contractor shall provide services to support Special Projects to provide additional analytical, consulting, and advisory support related to the task areas above. This optional work may be directed on a labor-hour basis, within the ceiling established under the contract, or may be performed on a Firm Fixed Price basis agreed upon in a bilateral modification.

As technology and FCC needs change, or when special situations arise, this optional task provides the flexibility for the FCC to obtain from the Contractor additional support for other tasks relating to Tasks 1 & 2, and other related requirements, as may be necessary.

Optional Task Exercise Procedure

Work under Optional Task 3 may be exercised by the Government, in its sole discretion, as often as it requires and as funding allows. When an optional task is exercised, the FCC shall send the Contractor a work plan, which shall detail requirements, deliverables, and timelines and provide a labor-hour estimate or firm fixed price and proposed ceiling amount to accomplish the work in the plan. The Contractor may be asked to provide feedback on the work plan, and a final work plan will be determined by the Contracting Officer, setting forth final requirements and a ceiling amount for the work. If, in the estimation of either party, the work plan provides the Contractor with information that is sufficient to accurately estimate the extent and duration of work and to anticipate costs with confidence, either party may propose to use Firm Fixed Price for the work. A fixed price for the work shall require mutual agreement of the parties represented in a bilateral modification to this task order. The optional tasks do not represent a commitment by the FCC to exercise the line item, nor, when exercised, does it represent a commitment of the FCC to direct work up to the ceiling amount established under a specific work plan, nor direct labor-hour work or negotiate Firm Fixed Price amounts up to the activity ceiling amount, or up to the amount used for estimates in pricing the activity in the Contractor's proposal, or up to the activity ceiling amount for the option period in which the work occurs, or up to the ceiling amount for the activity aggregated for all optional periods.

5 DELIVERABLES

The Contractor shall provide the deliverables outlined in the schedule below.

Deliverables Schedule

Deliverable	Description	Schedule
Project Planning Documents	The Contractor shall produce an overall Program Management Plan containing: a) Project Management Plan b) Staffing Plan c) Quality Assurance Plan d) Communication Plan e) Training & Documentation Plan	Draft submitted with Proposal Updated and validated with government COR within 30 days after the award Periodic updates upon request
Incident Response Plan & Breach Response Plan	The Contractor shall provide evidence of its cybersecurity training, an Incident Response Plan, a Breach Response Plan, and evidence of compliance with Privacy Federal Acquisition Regulation (FAR) clauses as outlined in Section 10 of the PWS.	Within 30 days after the award
Onboarding Documentation	The Contractor shall provide prompt and accurate documentation as part of this contract's security requirements. Vendor shall be aware that it takes approximately 10 days for U.S. Citizens to get fully onboarded and cleared through FCC Security Office. Non-U.S. Citizens will need to undergo a full background security investigation which takes approximately 90 to 120 days to get fully onboarded and cleared through FCC Security Office. The vendor shall describe an onboarding approach ensuring their employees will be onboarded and fully cleared by FCC Security Office to start work within 20 days of contract award date. The Contractor shall provide resumes for all personnel to be staffed on the project, as well as all requested information to support required background investigations in a timely manner.	Submit personnel onboarding documentation and resumes within 2 business days after the award unless otherwise agreed.
Kick-off Meeting	The Contractor shall coordinate a kick-off meeting to review the Project Plan. The meeting shall include stakeholders, subject matter experts (SMEs), and the FCC Project Manager in order to ensure common understanding of requirements and to set expectations.	Scheduled within 5 business days after the award

Deliverable	Description	Schedule
Weekly Meeting & Status Report	The Contractor shall provide a weekly status report outlining progress over the past week and planned activities for the following week. The report shall document any issues encountered or anticipated along with proposed mitigations. The FCC will work with the Contractor to develop a standard template for the weekly status report. The Contractor shall provide a draft format within one week after the kickoff meeting for FCC review and approval. The Contractor shall support a weekly status meeting with the FCC Project Manager to review status, staffing/workload scheduling, risks, recommendations/changes to priorities, and review of interim and final deliverables.	Template Draft within 1 week of kickoff Final approved template within 3 days of receiving FCC feedback Status reports and meetings Weekly throughout Tasks 1 & 2 Period of Performance (PoP) As Requested for optional tasks under Task 3
Executive Briefings	Upon request, the Contractor shall develop an executive briefing outlining key accomplishments along with any risks/issues encountered or anticipated along with proposed mitigations.	Upon Request
Wireless Engineering Deliverables (Task 2)	The types of deliverables anticipated to be required are outlined in Task 2 of the PWS. Specific wireless engineering and analytical deliverables will be defined on an ongoing basis based on the timing and frequency of external BDC inquiries. The Project Management Plan shall be a living document continuously updating and prioritizing required wireless engineering deliverables.	To be determined – as required based on timing of inquiries
Additional Deliverables (OPTIONAL Task 3)	For special projects (if any) initiated under OPTIONAL Task 3, deliverables will be specified within each order.	To be determined at time of order

6 GOVERNMENT-FURNISHED PROPERTY, EQUIPMENT, OR INFORMATION

The Contractor will be granted access to FCC's commercial wireless propagation modeling and planning tool software licenses, as needed, to support the task areas and requirements outlined in this PWS. Requirements for government furnished property, equipment, or information, if any, will be determined by FCC post-award.

7 PLACE OF PERFORMANCE

The services specified in this performance work statement shall be performed primarily at the contractor facility (or facilities). However, work may be required periodically at FCC Headquarters, 45 L Street, NE, Washington, DC 20554 or other FCC facilities at the direction of the Contracting Officer Representative (COR). In the event that work is required onsite at government facilities and would require the Contractor to incur travel costs, the FCC will work with the Contractor regarding the process for reimbursing approved travel expenses. No travel costs shall be reimbursed without prior approval in writing by the COR.

8 PERIOD OF PERFORMANCE

The base period of performance for this contract shall be twelve (12) months starting at the date of award, with two twelve (12) month option periods, to be exercised at the discretion of the FCC.

9 STAFFING PLAN AND PERSONNEL REQUIREMENTS

As noted in Section 4.1 Program Management, given the uncertainty regarding the volume and timing of work requirements, the Offeror's approach to ensuring the availability of qualified support staff is a critical aspect of the Offeror's overall Technical Approach. The following sections provide additional information regarding personnel requirements and estimated support requirements.

9.1 Standardized Labor Categories

Attachment 1 to the PWS outlines a set of standardized Labor Categories relevant to these requirements. The Offeror shall use these Labor Categories and associated qualifications when building its cost proposal. The Offeror shall provide a crosswalk between its defined personnel labor categories and the standardized Labor Categories to ensure that all personnel proposed for a given labor category meet or exceed the minimum qualifications specified in Attachment 1.

9.2 Estimated Support Requirements

The BDC verification, challenge, audit, and other processes described in this PWS are being implemented for the first time, and therefore historical data are not available regarding these support requirements. Because much of the workload will be driven by external inquiries, the FCC is unable to forecast with certainty the quantity, frequency, and timing of the various types of analysis that will be required.

Given this uncertainty, the FCC is structuring the support requirements in two pieces:

- **Core Team** – An initial core support team staffed on a full-time basis beginning at contract award. The number of resources and the mix of Labor Categories for this Core Team have been specified by the FCC and will be the same for all Offerors.

- **Additional / Surge Support** – At FCC discretion, additional resources may be added if and when the total workload exceeds the capacity of the combined FCC and Contractor Core Team resources.

Requirements, if any, for additional surge support will be defined post award based on the actual changes in workload experienced throughout the period of performance.

Please refer to the pricing instructions and accompanying Excel Pricing Template for additional information regarding the composition of the Core Team and the contract CLIN structure.

9.3 Key Personnel

Certain experienced professional and/or technical personnel are critical for successful accomplishment of the work to be performed under this PWS and are defined as "Key Personnel." Key Contractor personnel shall be maintained through completion of the order. ***Post award, the Contractor agrees that such personnel shall not be removed from the contract work or replaced without compliance with the following***:

- Vendor shall be aware that it takes approximately 10 days for U.S. Citizens to get fully onboarded and cleared through FCC Security Office. Non-U.S. Citizens will need to undergo a full background security investigation which takes approximately 90 to 120 days to get fully onboarded and cleared through FCC Security Office. The vendor shall describe an onboarding approach ensuring their employees will be onboarded and fully cleared by FCC Security Office to start work within 20 days of contract award date. The Contractor shall provide resumes for all personnel to be staffed on the project, as well as all requested information to support required background investigations in a timely manner.
- If one or more of the key personnel are unavailable for work for a continuous period exceeding 30 workdays, with the approval of the Contracting Officer's Representative (COR) or Contracting Officer (CO), the Contractor shall promptly replace personnel with personnel of equal ability and qualifications.
- All requests for approval of substitutions must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. The request must contain a resume for the proposed substitute, a corresponding transition plan, and any other information requested by the COR and CO). At the discretion of the COR, an interview with the proposed key individual may be required to verify that the proposed substitute has qualifications equal to, or greater than, the person to be replaced. The COR shall promptly notify the contractor of approval or disapproval in writing.
- The Contractor shall provide 30 days' notice and allow for two-week overlap/transition of duties when positions are replaced due to departure of standing key personnel. The FCC's CO, in consultation with the COR, has the right to request removal of, or approval

of, any contractor or subcontractor personnel assigned to accomplish this task order. Any personnel replacement shall be performed within 30 calendar days from date of the vacancy.

All personnel specified in the initial Core Team below are considered Key Personnel:

- Project Manager
- Principal Engineer
- Senior Engineer

Please refer to the position descriptions and experience, qualifications, and certification requirements referenced in Attachment 1 for each position. Please note the extent to which Key Personnel hold any preferred qualifications, as well as the required qualifications, for each position. Resumes for these personnel shall be submitted by the Offeror with its proposal and will be incorporated into the overall technical evaluation.

9.4 Staffing Plan

The BDC processes outlined in this PWS are being initiated for the first time and the volume, frequency, and timing of work requirements will be driven largely by external factors that cannot be predicted with precision in advance. Therefore, a robust and flexible Contractor staffing approach enabling deployment of additional qualified resources on short notice is a critical success factor.

Upon award of the contract, the Contractor shall work with FCC to finalize the Staffing Plan submitted during the RFP process and begin to execute against the plan upon FCC approval. The Staffing Plan shall document the Contractor's approach to providing the required personnel to support the PWS requirements including, but not limited to:

- Approach to ensuring access to qualified personnel for all positions, including ability to ***staff additional personnel within 30 days of FCC request*** in order to respond to any unexpected surges in workload
- Approach to ramping up new personnel quickly and efficiently
- Approach to ensuring access to additional technical capabilities and expertise in the future as new market technologies are developed and adopted over time
- Approach to ensuring personnel maintain up-to-date skills, knowledge and expertise in leading edge technologies and best practices, including any specific training or certifications
- Approach to providing managerial oversight and support to ensure that all staff are qualified, functioning at an acceptable level of performance, and receiving adequate training

- Approach to, and past demonstrated success in, attracting and retaining quality personnel to maintain a "strong bench" of qualified, tenured resources, particularly for key personnel categories aligned with PWS technical requirements
    - Of particular interest are innovative or unique aspects of the Offeror's Talent Management Strategy rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract
- If applicable, a clear subcontracting plan outlining the roles to be performed and tasks to be supported by the Prime Contractor and all subcontractors / teaming partners
    - Where known, please provide the approximate percentage allocations of workshare among teaming partners
- Approach to meeting the security clearance, background check, and other personnel security requirements outlined in Section 10 of the PWS and Clause LOCAL-27 Security Requirements Suitability and Security Processing

Throughout the life of the contract, the Contractor shall ensure continuity of activities in the event of personnel absence, whether scheduled time-off, military leave, or sick leave, to ensure continued support throughout the life of the contract.

For all new personnel, throughout the life of the contract, the Contractor must provide the vetted candidate resume to the Contracting Officer Representative (COR) for review and approval prior to personnel selection. The Government reserves the right to meet with contractor personnel prior to onboarding. Before removing or replacing any of the specified individuals, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the Contracting Officer approves the change.

10 SECURITY & PRIVACY

The Contractor's solution, including all products and services provided, shall comply with all FCC Information Technology (IT) policy requirements, NIST standards, OMB guidelines, and other applicable Government-wide laws and regulations. Such requirements include, but are not limited to:

- Federal Information Security Modernization Act of 2014 (FISMA), as amended
- Privacy Act of 1974, (5 U.S.C. § 552a)
- E-Government Act of 2002, Section 208

- Title V – Confidential Information Protection and Statistical Efficiency Act of 2002 of the E-Government Act of 2002 (CIPSEA)
- Executive Order 14028, "Improving the Nation's Cybersecurity"
- Executive Order 13556, "Controlled Unclassified Information (CUI)"
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996"
- Office of Management and Budget (OMB) Circular A-130, "Managing Strategic Information as a Resource"
- OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"
- OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident"
- OMB M-21-07, "Completing the Transition to Internet Protocol Version 9 (Ipv6)"
- OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"
- NIST Special Publication (SP) 800-18 (as amended), "Guide for Developing Security Plans for Federal Information Systems"
- NIST SP 800-30 (as amended), "Guide for Conducting Risk Assessments"
- NIST SP 800-34 (as amended), "Contingency Planning Guide for Federal Information Systems"
- NIST SP 800-37 (as amended), "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems"
- NIST SP 800-53 (as amended), "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-53A (as amended), "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessments Plans"
- NIST SP 800-60 vol 1 (as amended), "Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-60 vol 2 (as amended), "Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices"
- NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide"
- NIST SP 800-63-3, "Digital Identity Guidelines"
- NIST SP 800-171 (as amended), "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"
- NIST SP 800-177 (as amended), "Trustworthy Email"
- FIPS PUB 140-3, "Security Requirements for Cryptographic Modules"

- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems"
- FCC Cybersecurity and Privacy Policy
- Any other relevant Federal laws, regulations, policies, and guidance that FCC must adhere to

10.1 Personnel Security

Prior to gaining access to FCC's information, information systems,[4] network, or physical space, or doing work on behalf of FCC, the selected Contractor's personnel must meet FCC Personnel Security background investigation requirements as set forth in additional detail in Local 27. Depending on position risk, as determined by FCC, these requirements may include the following:

- A background investigation (initiated by FCC);
- A commercial background investigation (initiated by FCC or the individual's company if to the FCC's standards);
- Criminal history record information via a fingerprint check; and
- Drug testing.

These requirements may change at the discretion of FCC, and individual access may be denied at any point. The Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting FCC.
The Contractor shall bear the cost of obtaining and sustaining the background investigations. It is the responsibility of the Contractor to provide the individuals with the required background investigation needed to complete the work. The fact that the FCC performs security investigations for contractor employees shall not in any manner relieve the Contractor of its responsibility to ensure that all personnel furnished are reliable and of reputable background and sound character.

10.2 Cybersecurity Training

The Contractor shall provide evidence that all personnel assigned to work on this contract have completed cybersecurity training and have received and signed Rules of Behavior governing their use of Federal information and/or information systems. The cybersecurity training and Rules of Behavior may be company-provided, subject to review by the FCC, or provided by FCC. FCC policy requires cybersecurity training to occur on an annual basis.

[4] Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST SP 800-53). FCC defines information resources as any information (e.g., files, data, etc.), system, application, or service that a FCC employee or contractor can access.

10.3 Access to FCC Network and Information

If the FCC determines that, to complete the defined work, the Contractor must have direct access to the FCC network using FCC network accounts, the following Federal Acquisition Regulation clauses will apply to Contractor:

- 52.204-9 Personal Identity Verification of Contractor Personnel
- 52.245-1 Government Property

As set forth in additional detail in Local 27, all personnel assigned to work on this contract will be issued a Personal Identity Verification (PIV) card in order to access the FCC network upon successful completion of the personnel security background investigation. The Contractor will receive their FCC network accounts once their personnel have completed the required training and signed the required Rules of Behavior.

If the FCC determines that it is necessary or appropriate to share Federal information with Contractor personnel outside of the FCC network, and such information is or could potentially reveal PII (or is otherwise determined by FCC to be confidential), such information shall be exchanged by a secure file transfer that the FCC determines is appropriate to safeguard the information.

10.4 Usage of FCC Information[5]

The Contractor must not publish or disclose[6] in any manner, without prior written consent, the data/information which the Contractor will receive or to which the Contractor will have access because of this contract. Contractors may be held responsible for any violations of confidentiality. Contractor shall:

- Use FCC information only for the purposes described in the contract and not otherwise use or monetize the information;
- Not reproduce the FCC information and hold it in confidence and protect the information from dissemination to, and use by, any third party;
- Not create any derivative work from FCC information disclosed, except as required in performance obligations under the contract;
- Restrict access to the FCC information its personnel, agents, or consultants, if any, who have a need to have access and who have been advised of and have agreed in writing or are otherwise bound to treat such information in accordance with the terms of the contract;

[5] FCC Information refers to single or multiple instances of facts, data, ideas, knowledge, instructions, etc. that Contractor receives, obtains, or accesses under the Contract in any medium or form that can be stored, transferred, communicated, or processed.

[6] Disclose: To share, give access to, or disseminate in any manner.

- Not commingle FCC information with Contractor specific records or the records of other parties;
- As part of the contract closeout, return or destroy all FCC information in its possession, including any backup datasets or internal tracking or metadata that may contain or reveal FCC information, upon termination or expiration of the contract or as otherwise requested by the FCC. Contractor shall submit evidence of compliance with the close-out requirements in this provision, in a manner described by the FCC, at its discretion; and
- Ensure records created and maintained using electronic media, social media, websites, wikis, emails, or any other type of electronic communication in fulfillment of this contract follow FCC's Records Control Schedule and/or the General Records Schedules and managed in accordance with approved dispositions.

In addition, the NARA Records Management Language for Contracts clause applies to this solicitation and is available at https://www.archives.gov/records-mgmt/policy/records-mgmt-language.

10.5 Incident[7] Response

The Contractor shall provide an Incident Response Plan to ensure that it is able to respond to any incident that may impact its ability to successfully complete the obligations of the contract. The Contractor shall provide full access and cooperation for all activities determined by FCC to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of the incident. FCC, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid or investigate incident response activities.

10.6 Breach Response

Consistent with Local-26, the Contractor shall provide a Breach Response Plan to demonstrate that it can respond to any PII breach—*i.e.*, 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 PII; or (2) an authorized user accesses or potentially accesses PII for other than the authorized purpose.[8]

Upon award, Contractor shall work with FCC IT and FCC Privacy to ensure that the Breach Response Plan, at a minimum, documents that, in the event of a breach, Contractor shall:

[7] Incident: An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

[8] A breach may take any form, including paper, oral, and electronic.

- Notify within one hour of a suspected or confirmed breach, FCC Chief Information Security Officer (CISO), FCC Privacy Team at PII@fcc.gov, COR, and Contracting Officer (CO).
- Provide the following information as part of the notification to FCC:
    - Date and time the breach was discovered;
    - The type of information potentially compromised by the suspected or confirmed breach;
    - Number of individuals affected by the suspected or confirmed breach;
    - Identification of the breakdown in safeguards that led to the suspected or confirmed breach;
    - Incident response activities in progress or completed; and
    - Any additional information relevant to the breach.

In the event of a breach, the FCC will coordinate with the Contractor to notify individuals affected by the suspected or confirmed breach. The Contractor shall provide in writing to the COR, CO, and Senior Agency Official for Privacy all actions taken that relate to FCC information or individuals, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring). The notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by FCC. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- A brief description of the incident;
- A description of the types of PII impacted by the breach;
- A statement as to whether the PII was encrypted or protected by other means;
- Steps individuals may take to protect themselves;
- What the Contractor is doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- Information on how to obtain additional information.

Reporting a privacy breach shall not, by itself, be interpreted as evidence that the Contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

10.7 Processing of PII

The Contractor will restrict the processing and storage of FCC Information containing PII to facilities within the legal jurisdictional boundary of the United States.

11 SECTION 508

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms, and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines.

11.1 Installation, Configuration & Integration Services

When the Contractor provides installation, configuration, or integration services for equipment and software pursuant to this contract, the Contractor shall not install, configure, or integrate the equipment and software in a way that reduces the level of conformance with the applicable Revised 508 Standards.

11.2 Maintenance Upgrades & Replacements

The Contractor shall ensure that maintenance upgrades, substitutions, and replacements to equipment and software, if any, pursuant to this contract do not reduce the original level of conformance with the applicable Revised 508 Standards at the time of contract award.

11.3 Service Personnel

The Contractor shall ensure that the personnel providing the labor hours possess the knowledge, skills, and ability necessary to address the applicable Revised 508 Standards defined in this contract and shall provide supporting documentation upon request.

11.4 Hosting Services

When providing hosting services for electronic content provided by the Agency, the Contractor shall not implement the hosting services in a manner that reduces the existing level of conformance of the electronic content with applicable Revised 508 Standards. Throughout the life of the contract, the Agency reserves the right to perform testing on a Vendor or Contractor's hosted solution to verify conformance with this requirement.

11.5 Validation for ICT Items

The Contractor shall test and validate the ICT solution for conformance to the Revised 508 Standards, in accordance with the required testing methods.

- For web and software, WCAG Level A and AA Conformance Test Results must be based on the Harmonized Testing Process for Section 508 Compliance: Baseline Tests for Software and Web Accessibility available at https://www.dhs.gov/508-testing.
- For Microsoft Office and PDF documents, WCAG Level A and AA Conformance test results must be based on the Harmonized Testing Guidance from the AED ACOP.
- For ICT Items that are not electronic content, the Contractor shall validate conformance to the applicable Revised 508 Standards using a defined testing process. The Contractor must describe test process and provide the testing results to the Agency.

11.6 Documentation

The Contractor shall maintain and retain full documentation of the measures taken to ensure compliance with the applicable requirements, including records of any testing or demonstrations conducted. For reference see Section 508 testing available at https://www.dhs.gov/compliance-test-processes.

12 ORGANIZATIONAL CONFLICTS OF INTEREST (OCI)

It is recognized that some prospective Offerors may conduct business with wireless/broadband providers, including supporting providers with compiling required data and information for submittal to the FCC in compliance with the BDA.

As part of its Technical Approach, the Offeror shall document its approach to avoiding/mitigating any real or perceived conflicts of interest in providing independent and objective analysis and advice related to the tasks outlined in this PWS.

Please refer to clause LOCAL-7 “Organizational Conflicts of Interest” in the solicitation for additional information and requirements.

13 ADDITIONAL REFERENCES

Please refer to the additional resources at the following links for additional information regarding these requirements.

- The Broadband Data Collection Help Center - https://help.bdc.fcc.gov/hc/en-us
- Broadband Data Collection (BDC) Mobile Technical Requirements Order, DA 22-241, Mar. 9, 2022 - https://www.fcc.gov/document/fcc-releases-bdc-mobile-technical-requirements-order
- Data Specifications for Biannual Submission of Subscription, Availability, and Supporting Data, August 2022 - https://us-fcc.app.box.com/v/bdc-availability-spec

- Data Specifications for Provider Infrastructure Data in the Mobile Challenge and Mobile Verification Processes, March 2022 - https://us-fcc.app.box.com/v/bdc-infrastructure-spec
- Data Specifications for Mobile Speed Test Data, September 2022 - https://us-fcc.app.box.com/v/bdc-mobile-speedtest-spec
- Mobile Broadband Supporting Data - https://help.bdc.fcc.gov/hc/en-us/articles/5342522028059-Mobile-Broadband-Supporting-Data
- Fixed Wireless Broadband Supporting Data - https://help.bdc.fcc.gov/hc/en-us/articles/5291309996699-Fixed-Wireless-Broadband-Supporting-Data