GEN2129421P1 - Next Generation 911 (NG911)

BPRO Electronic Procurement System Back to list

Project Details

Project: Next Generation 911 (NG911)

Ref. #: GEN2129421P1

Department: FASD - Purchasing

Type: RFP

Status: CLOSED

Open Date: Jul 11th 2025, 5:30 PM EDT

Questions Due Date: Jul 30th 2025, 5:00 PM EDT

Contact Information: Latoya Clark Forbes, Dazarene Lescott, lclarkforbes@broward.org, dlescott@broward.org

Close Date: Aug 22nd 2025, 2:00 PM EDT

Days Left: Submissions are now closed

Contract Duration:
Open-End; Five-Year Initial

Contract Renewal:
Five One-Year Renewals

Bid Validity:
Not Applicable

Bonding Required:
Yes

Total Amount of Pass-Thru Allowance (Initial Term or Fixed):
0

OESBD Designation Goal Participation Type (Non-Multi):
No Goal

OESBD Designation Goal Participation Type (Multi):
No Goal

Goal Assigned Percentage (0 if No Goal):
0

Public Works/Construction:
No

Project Description:
Scope of Work: The Broward County Office of Regional Communications and Technology is seeking a qualified vendor to provide a Next Generation 911 (NG911) Solution. Scope includes the requirements to procure a market-ready National Emergency Number Association (NENA) i3-compliant Next Generation 911 (NG911) System, which consists of an Emergency Services Internet Protocol (IP) Network (ESInet) and Next Generation Core Services (NGCS), to support the Regional and Non-Regional PSAPs within Broward County.

Solicitation Provisions/Requirements: (Vendor is cautioned that this is a summary only and the full solicitation must be reviewed).

August 2025 prev next

Sun	Mon	Tue	Wed	Thu	Fri	Sat

- Broward County Standard Service Level Agreement
- Broward County Standard Technology Agreement
- Enterprise Technology Services Security Requirements
- Enterprise Technology Services Vendor Security Questionnaire
- Bonding Requirements

Office of Economic and Small Business Development Requirements: Not applicable to this solicitation.

Questions and Answers: The County provides a specified time for Vendors to ask questions and seek clarification regarding the solicitation requirements. All questions or clarification inquiries must be submitted through BPRO by the Questions due date. The County will respond to questions in BPRO (Messages section).

Submittals: Vendor MUST submit its solicitation response electronically through BPRO and receive a Submission Receipt. It is solely the Vendor's responsibility to ensure its response is submitted and received through BPRO by the closing date and time. The County will not consider solicitation responses received by other means. Vendors are encouraged to submit in advance of the closing date and time. Refer to the Purchasing Division website or contact support@gobonfire.com for submittal instructions. In the event that the Vendor is having difficulty submitting a document, immediately notify the Purchasing Agent and then contact support@gobonfire.com for technical assistance.

Conflict of Interest: Any person or vendor that participated in the development of the specifications for this project may be barred, in part or in full, from submitting, or assist in submitting, a response to this solicitation. The County reserves the right to review all potential conflicts and to make determinations in its sole discretion.

Important Events:

Search

Status	Event Name	Location	Description	Dates	
PASSED	Open Date	Online Portal	Posting date for the Opportunity	Jul 11th 2025, 5:30 PM EDT	N/A
PASSED	OPTIONAL PRE-PROPOSAL CONFERENCE	Central Regional Public Safety Answering Point: 10440 W Oakland Park Blvd, Sunrise, FL 33351 or Teams	Attendance at the Pre-Proposal Conference is OPTIONAL. This information session presents an opportunity for the vendors to ask questions regarding proposal requirements. A mandatory site visit of the Central Regional Public Safety Answering Point will start promptly after the Optional Pre-Proposal Conference. Copy and paste LINK into your browser: https://teams.microsoft.com/l/meetup-join/19%3ameeting_NGY1Nzc5MzltYTgwNC00ZDk2LWEwNTktMDE2ODQ0ODA5N2Q1%40thread.v2/0?context=%7b%22Tid%22%3a%229483ae6c-808a-4f02-98a1-8154c0b35bfd%22%2c%22Oid%22%3a%22c8f431ec-15ed-48a9-a952-a133889caae7%22%7d or dial by PHONE: (754) 900-8519; Conference ID 183 119 360#	Jul 24th 2025, 9:30 AM EDT - Jul 24th 2025, 10:30 AM EDT	No
PASSED	MANDATORY SITE VISITS - DAY 1	Central, North, and Coral Springs, Public Safety Answering Points	To attend the mandatory site visits at the Central, North, and Coral Springs Public Safety Answering Point (PSAP) locations, participants are required to bring a government issued photo identification and employee badge of company being represented. The mandatory site visits will start promptly after the Optional Pre-Proposal Conference held at the Central PSAP. Please make arrangements to be represented or failure to attend the mandatory site visit will deem the Vendor non-responsive. This information session presents an opportunity for the vendors to ask questions regarding proposal requirements. If you require any auxiliary aids for communication, please call (954) 357-	Jul 24th 2025, 10:30 AM EDT - Jul 24th 2025, 4:00 PM EDT	Yes

			6066 so that arrangements can be made in advance. The addresses for the Public Safety Answering Point locations are as follows: - Central: 10440 W Oakland Park Blvd, Sunrise, FL 33351 - North: 4900 W Copans Road, Coconut Creek, FL 33063 - Coral Springs: 2801 Coral Springs Drive, Coral Springs, FL 33065		
PASSED	MANDATORY SITE VISITS - DAY 2	South, Plantation, and EOC Public Safety Answering Point Locations	To attend the mandatory site visits at the South, Plantation, EOC Public Safety Answering Point locations, participants are required to present a government issued photo identification and employee badge of company being represented. Please make arrangements to be represented or failure to attend the mandatory site visit will deem the Vendor non-responsive. The addresses for the Public Safety Answering Point locations are as follows: - South: 6057 SW 198th Terrace, Pembroke Pines, FL 33332 - Plantation: 451 NW 70th Terrace, Plantation, FL 33317 - Emergency Operations Center (EOC): 201 NW 84th Ave, Plantation, FL 33324	Jul 25th 2025, 9:30 AM EDT - Jul 25th 2025, 4:00 PM EDT	Yes
PASSED	Questions Due Date	Online Portal	Deadline to submit Questions	Jul 30th 2025, 5:00 PM EDT	N/A
PASSED	Close Date	Online Portal	Deadline for Submissions	Aug 22nd 2025, 2:00 PM EDT	N/A

Commodity Codes:

NIGP 20464 **Network Components: Adapter Cards, Bridges, Connectors, Expansion Modules/Ports, Firewall Devices, Hubs, Line Drivers, MSAUs, Routers, Switches, Transceivers, etc.**

NIGP 20830 **Computer Aided Design (CAD) and Vectorization Software, Microcomputer**

NIGP 20836 **Data Processing Software, Microcomputer**

NIGP 20837 **Database Software, Microcomputer**

NIGP 20841 **Engineering Software, Microcomputer**

NIGP 20842 **EDI (Electronic Data Interchange) Translator Software, Microcomputer**

NIGP 20854 **Internet, Web Site and Mobile Application Development Software, Microcomputer**

NIGP 20954 **Internet, Web Site and Mobile Application Software, Mainframes and Servers**

NIGP 83845 **Emergency Radio/Telephone Systems, 411, 911 etc., Dispatch**

NIGP 83883 **Telecommunication, Internet Protocol, Network Monitoring, Surveillance, Intrusion Detection Systems and Networking Products**

NIGP 93972 **Radio, Telecommunications, Telephone Equipment, Including 911 Systems and Facsimile Transceivers, Maintenance and Repair**

NIGP 2042065 **REPEATERS, NETWORK, COMPUTER**

NIGP 2046445 **CONTROLLERS, NETWORK INTERFACE**

NIGP 2046453 **NETWORK EXTENDER UNITS**

NIGP 2062045 **MODULES, INTERFACE, MAINFRAME, NETWORK**

NIGP 2065530 **INTEGRATED HARDWARE AND SOFTWARE SOLUTION**

NIGP 2089078 **SOFTWARE, INFORMATION SECURITY, MICROCOMPUTER**

NIGP 8398427 **TELEPHONES, IP (INTERNET PROTOCOL), (BRAND LISTED OR EQUAL)**

NIGP 9152628 **FILE TRANSFER PROTOCOL (FTP)**

NIGP 9182810 **CONSULTANT SERVICES, COMPUTER SYSTEMS/NETWORKING**

NIGP 9587025 **INFORMATION TECHNOLOGY SERVICES**

Supporting Documentation:

Search

File		Type	Description
Addendum No. 1, Evaluation Criteria, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 1, Functionality Checklist, GEN2129421P1, Next Generation 911 (NG911).docx	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 1, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 1, Non-Regional PSAP Diagram, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT

Addendum No. 1, Project Questionnaire, GEN2129421P1, Next Generation 911 (NG911).docx	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 1, Regional PSAP Diagram, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 1, Scope of Work, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 1	Aug 8th 2025, 2:54 PM EDT
Addendum No. 2, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 2	Aug 13th 2025, 8:43 AM EDT
Addendum No. 3, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 3	Aug 18th 2025, 5:19 PM EDT
Addendum No. 3, General Compliance, GEN2129421P1, Next Generation 911 (NG911).docx	Other	Document - Addendum No. 3	Aug 18th 2025, 5:19 PM EDT
Addendum No. 4, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Addendum No. 4	Aug 19th 2025, 2:25 PM EDT
Agreement Exceptions - RFP-RFQ-RLI.docx	Documentation		May 9th 2025, 7:00 AM EDT
Anti-Human Trafficking Affidavit	Documentation		Sep 6th 2024, 1:09 PM EDT
Bid Bonds, Performance and Payment Bonds, and Surety Qualification Requirements.pdf	Documentation		Jul 10th 2025, 8:23 AM EDT
Criminal History Screening Practices Certification	Documentation		Sep 6th 2024, 1:09 PM EDT
Demonstration Script, GEN2129421P1, Next Generation 911 (NG911).pdf	Documentation		Jul 8th 2025, 2:11 PM EDT
Domestic Partnership Act Certification - RFP-RFQ-RLI.docx	Documentation	Complete and sign this form.	May 9th 2025, 8:00 AM EDT
Enterprise Technology Services Security Requirements Exhibit - High Risk, GEN2129421P1, Next Generation 911 (NG911) System.pdf	Documentation		Nov 18th 2024, 3:03 PM EST
ETS Vendor Security Questionnaire, GEN2129421P1, Next Generation 911 (NG911).xlsx	Documentation		May 5th 2025, 11:39 AM EDT
Instructions to Vendors, GEN2129421P1, Next Generation 911 (NG911).pdf	Documentation		Jul 10th 2025, 9:01 AM EDT
Insurance Requirements Form, GEN2129421P1, Next Generation 911 (NG911).pdf	Documentation		Nov 22nd 2024, 2:47 PM EST
Litigation History	Documentation		Sep 10th 2024, 12:25 PM EDT
Lobbyist Registration Requirement Certification	Documentation		Sep 6th 2024, 1:09 PM EDT
Location Certification - RFP-RFQ-RLI.docx	Documentation	Complete and sign this form.	May 9th 2025, 8:00 AM EDT
OESBD Affiliated Entities of the Principals Certification	Documentation		Sep 6th 2024, 1:09 PM EDT
OESBD Ownership Disclosure	Documentation		Sep 6th 2024, 1:09 PM EDT
Security Requirements	Documentation		Sep 7th 2024, 12:18 PM EDT
Sign-in Sheets for Optional Pre-Proposal Conference and Mandatory Site Visits.pdf	Other	Document - Sign-in Sheets for Read more...	Jul 31st 2025, 11:32 AM EDT

Subcontractors-Subconsultants-Suppliers Requirement	Documentation		Sep 6th 2024, 1:09 PM EDT
Submissions, GEN2129421P1, Next Generation 911 (NG911).pdf	Other	Document - Submissions	Aug 25th 2025, 10:22 AM EDT
Summary of Vendor Rights for Broward County Competitive Solicitations	Documentation		Sep 6th 2024, 1:09 PM EDT
Vendor Questionnaire and Standard Certifications - RFP-RFQ-RLI.docx	Documentation	Complete and sign this form.	Jul 7th 2025, 12:29 PM EDT
Vendor Reference Verification, GEN2129421P1, Next Generation 911 (NG911).docx	Documentation		May 5th 2025, 12:07 PM EDT
Volume of Previous Payments Attestation - RFP-RFQ-RLI.docx	Documentation		May 9th 2025, 8:00 AM EDT

Requested Information:

Listed below are the documents and information needed to complete your submission:

Required with Submittal

Name		Type		# Files	Requirement	Instructions
Next Generation (NG911) Proposed Solution (BT-04TX)	BidTable: Excel (.xlsx)	1	REQUIRED		You will need to fill out the provided Response Template for this BidTable.	
Optional Renewal Terms (BT-26BS)	BidTable: Excel (.xlsx)	1	REQUIRED		You will need to fill out the provided Response Template for this BidTable.	
Vendor Proposal	File Type: Any (.*)	Multiple	REQUIRED			
Functionality Checklist	File Type: Any (.*)	Multiple	REQUIRED			
Location Certification - RFP RFQ RLI	File Type: Any (.*)	Multiple	REQUIRED			
Proposal Bond or Alternate Bid Security	File Type: Any (.*)	Multiple	REQUIRED			
Vendor Questionnaire and Standard Certifications - RFP RFQ RLI	File Type: Any (.*)	Multiple	REQUIRED			

Submit with response or with three business days of County's request

Name			Type	# Files
Anti-Human Trafficking Affidavit	File Type: Any (.*)	Multiple	OPTIONAL	
Broward County Local Business Tax Receipt	File Type: Any (.*)	Multiple	OPTIONAL	
Certificate of Insurance/Letter from Insurance Carrier or Requirements	File Type: Any (.*)	Multiple	OPTIONAL	
Criminal History Screening Practices Certification	File Type: Any (.*)	Multiple	OPTIONAL	
Domestic Partnership Act Certification - RFP RFQ RLI	File Type: Any (.*)	Multiple	OPTIONAL	
General Compliance	File Type: Any (.*)	Multiple	OPTIONAL	
Litigation History	File Type: Any (.*)	Multiple	OPTIONAL	
Lobbyist Registration Requirement Certification	File Type: Any (.*)	Multiple	OPTIONAL	
OESBD Affiliated Entities of the Principals Certification	File Type: Any (.*)	Multiple	OPTIONAL	
Subcontractors Subconsultants Suppliers Requirement	File Type: Any (.*)	Multiple	OPTIONAL	
Project Questionnaire	File Type: Any (.*)	Multiple	OPTIONAL	
Vendor Security Questionnaire	File Type: Any (.*)	Multiple	OPTIONAL	
Vendor Reference Verfication - RFP RFQ RLI	File Type: Any (.*)	Multiple	OPTIONAL	

Volume of Previous Payments Attestation - RFP RFQ RLI	File Type: Any (.*)	Multiple	OPTIONAL	

Submit with response; County will not request after submittal

Name	Type		# Files	Requirement
Agreement Exception - RFP RFQ RLI	File Type: Any (.*)	Multiple	OPTIONAL	

Document Takers

Search

Vendors	# Files	Actions
22nd Century Technologies, Inc.	22	
A.A.B.S.	1	
AT&T	10	
AT&T	3	
AT&T	23	
AT&T	3	
BBR Printers	35	
Bowes Enterprise L.L.C	25	
Broward County Commission	11	
BuildCentral Inc	13	
CDW Government LLC	23	
Construction Bid Source	2	
Deltek	29	
DISYS SOLUTIONS, INC.	21	
Elegant Enterprise-Wide Solutions, Inc.	21	
Enterprise Pals, Inc.	21	
GovGuide	1	
INdigital	90	
Lanzo Construction Co., Florida	1	
LinkSystems, LLC	70	
Lockton	3	
Lumen Technologies	22	
Mission Critical Partners, LLC	74	
Motorola Solutions Connectivity, Inc.	43	
Motorola Solutions, Inc.	25	
Motorola Solutions, Inc.	33	
Nerds Inc	32	
NGA 911 LLC	25	
PWXPress	55	
RADgov, Inc	45	
re	10	
SevenOutsource	21	
Software Information Resource Corp	1	
vCloud Tech Inc.	2	

Interested Contractors

Prime/General Contractors | Subcontractors

Search

Vendors	Contact	Email	Phone	Subcontract Services
INdigital	Larry Stidham	lstidham@indigital.net	877-469-2010	All aspects of the Broward opportunity.

Vendors	Contact	Email	Phone	Subcontract Services
Motorola Solutions Connectivity, Inc.	Jarrod Shupe	trk473@motorolasolutions.com	386-227-7675	Next Generation 911 (NG911)

Messages

Public Notices (6) | Vendor Discussions (0) | Public Q&A (18)

Search

Search...

Latoya Clark-Forbes
Submissions
Vendor Submissions for RFP No.

Latoya Clark-Forbes
Addendum No. 4
Refer to Addendum No. 4 for deta

Latoya Clark-Forbes
Addendum No. 3
Refer to attached Addendum No.

Latoya Clark-Forbes
Addendum No. 2
Evaluation Criteria, Section 2, Pro

Latoya Clark-Forbes
Addendum No. 1
Refer to attached Addendum No.

Latoya Clark-Forbes
Sign-in Sheets for Optional Pre
Attached are the sign-in sheets fo

Click New Public

Submissions and Prime/Subcontractor Interest

This project is not open for proposal submissions at this time.

Public Q&A

#1 - Population

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:02 PM EDT, Public - Pending
Could you please clarify which population count vendors shall use for Broward County? We have identified several potential sources, including the UF BEBR, Broward.org, the Census 2020 Actual FL EDR, and the Census 2024 Estimate, but the latest actual reported by BEBR, Broward.org, and the 2020 Census was 1,981,888.
Latoya Clark-Forbes, Aug 08, 2025 3:06 PM EDT, Public - Answered
According to the US Census Bureau, the total population of Broward County is 2,037,472.

#2 - Scope of Work - # of Positions and 911 Call Volume at each PSAP

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:05 PM EDT, Public - Pending
The Scope of Work section of the RFP includes the Total number of Call Taking Positions for the Regional and Non-Regional systems. Could you provide the number of call-taking positions at each Public Safety Answering Point (PSAP), along with the annual 9-1-1 call volume for each?
Latoya Clark-Forbes, Aug 08, 2025 3:07 PM EDT, Public - Answered
The number of call-taking positions at each PSAP are as follows: Regional PSAPs: Central - 32, North - 27, South - 31, and Emergency Operations Center (EOC) - 6 (Satellite positions) Non-Regional PSAPs: Coral Springs - 21, Plantation - 12, and EOC - 20 Please note that in Q4-2026, the North PSAP will be moving to a new facility and the number of positions will increase from 27 to 49. Provided below is the call volume for Regional and Non-Regional PSAPs: - The total 911 Calls incoming for Regional PSAPs which includes TTYs , TTY Challenges, and Abandoned Calls from 10/1/2023 – 9/30/2024 was: 1,187,528.

- The total 911 Calls incoming for Coral Springs PSAP which includes TTYs , TTY Challenges, and Abandoned Calls from 10/1/2023 – 9/30/2024 was: 81,486.

- The total 911 Calls incoming for Plantation PSAP which includes TTYs , TTY Challenges, and Abandoned Calls from 10/1/2023 – 9/30/2024 was: 52,631.

#3 - SR-NR Network Redundancy and Resiliency - SR-NR001

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:06 PM EDT, Public - Pending

According to requirement SR-NR001 - "The NG911 Service Provider shall provision two redundant circuits into each location to terminate at the VIPER load balancers." Can the County provide a diagram indicating the PSAP(s) where the load balancers are located and the associated connectivity points (i.e. firewalls, routers, load balancers) required to interface with the NGCS ESInet Edge Devices?

Latoya Clark-Forbes, Aug 08, 2025 3:08 PM EDT, Public - Answered

As a result of the VIPER 7 implementation that completed on June 25, 2025, each Regional and Non-Regional PSAP has VIPER 7 servers and load balancers (Primary and Secondary).

Refer to Addendum No. 1, a diagram for the Regional and Non-Regional PSAPs have been uploaded.

#4 - SR-NR Network Redundancy and Resiliency - SR-NR002

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:06 PM EDT, Public - Pending

According to requirement SR-NR002 - "The NG911 Service Provider shall provision two circuits into two locations in each environment (Regional and Non-Regional) to terminate at the VIPER servers" Can the County provide a diagram indicating the PSAP(s) where the VIPER servers are located and the associated connectivity points (i.e. firewalls, routers) required for the CHE to interface with the NGCS ESInet Edge Devices? The diagram on page 12 of the Scope of Work doesn't portray where the servers exists today. Based on the site walks the remote sites now have VIPER servers and would act as a Host.

Latoya Clark-Forbes, Aug 08, 2025 3:09 PM EDT, Public - Answered
Refer to the response to Question 3. The diagram on page 12 of the Scope of Work, was the existing design. In addition, the CHE was also upgraded during the VIPER 7 implementation.

#5 - Scope of Work - General Overview of Desired System

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:20 PM EDT, Public - Pending
Regarding the requirement for "c) 911 Call Egress/Call Delivery", it currently states that circuits must terminate directly into the Load balancers and VIPER Servers. Typically, an NGCS provider does not terminate circuits directly on the CHE; instead, they provide an ESInet demarcation point for the CHE provider's equipment. Shall this requirement be updated to specify that the NGCS provider will coordinate with the CHE provider to establish connections to the NGCS network edge devices?
Latoya Clark-Forbes, Aug 08, 2025 3:09 PM EDT, Public - Answered
No, refer to the Project Questionnaire SR-NR001 and SR-NR002: SR-NR001 states that "The NG911 Service Provider shall provision two redundant circuits into each location to terminate at the VIPER load balancers." SR-NR002 states that "The NG911 Service Provider shall provision two circuits into two locations in each environment (Regional and Non-Regional) to terminate at the VIPER servers." There is no requirement for the NG911 Service Provider to connect directly to the CHE. However, as stated in Project Questionaire, SR-DL003, the NG911 Service Provider must work with and coordinate the installation and testing of all circuits from the NG911 Service Provider's network to PSAP data rooms.

#6 - Scope of Work - General Overview of Desired System #2

Motorola Solutions Connectivity, Inc., Jul 29, 2025 2:41 PM EDT, Public - Pending
For all sites, could the County provide the distance from the minimum point of building circuit entry to the equipment room's rack where the ESinet network edge devices would be installed in the PSAP facilities?
Latoya Clark-Forbes, Aug 08, 2025 3:11 PM EDT, Public - Answered
Vendor can expect a minimum distance of between 150-200 feet, however, the County highly encourages the vendors to contact the County Local Exchange Carrier (LEC) for an approximate distance.

#7 - Next Generation (NG911) Proposed Solution - Connectivity to other networks (within Neighboring Counties)

AT&T, Jul 30, 2025 2:25 PM EDT, Public - Pending
Thank you for the information regarding the connectivity to other networks through Network to Network Interfaces for NG911 systems and Legacy Systems. To better understand the requirements for the legacy systems, could you please provide the following details: What is the expected volume of data that will be handled by the legacy systems? What is the Maximum Transmission Unit (MTU) size for the legacy systems? Which protocols are currently being used or expected to be used by the legacy systems?
Latoya Clark-Forbes, Aug 08, 2025 3:17 PM EDT, Public - Answered
At this point, all of the surrounding Counties have contracted for NG911 services. Legacy connectivity will only be required should one or more of the Counties not be migrated to their chosen NG911 services prior to Go-Live of Broward County services. The Legacy System will be traditional enhanced 911 Systems to include selective routers and ALI.

What is the expected volume of data that will be handled by the legacy systems?

Response to this question pending from County.

What is the Maximum Transmission Unit (MTU) size for the legacy systems?

The MTU size is dependent on the capabilities between both sides of Network to Network Interface (NNI) NG911 Service Providers. The County would like that the NG911 Service Provider to ensure that the MTU is sufficient to process all Legacy calls via the NNI to meet all SLA requirements.

Which protocols are currently being used or expected to be used by the legacy systems? The protocols are dependent on the capabilities between both sides of Network to Network Interface (NNI) NG911 Service Providers. The County would like that the NG911 Service Provider to ensure that the protocols are compatible to process all Legacy calls via the NNI to meet all SLA requirements.

#8 - Next Generation (NG911) Proposed Solution - OSP in county POI Connectivity

AT&T, Jul 30, 2025 2:26 PM EDT, Public - Pending

Are POIs inside Broward County a requirement?

EG ATTMO?

Latoya Clark-Forbes, Aug 08, 2025 3:18 PM EDT, Public - Answered

SR-IN003 Requirement has been modified and split into two parts.

SR-IN003.a (Project Questionnaire) The NG911 Service Provider shall provide multiple POIs for OSPs both locally and nationally with a minimum of four POI.

SR-IN003.b (Functionality Checklist) The NG911 Service Provider should provide at least two within 100 miles of the Broward County border. Having local and national POIs will provide OSPs with interconnection choices.

#9 - Next Generation (NG911) Proposed Solution - Design Sessions to include up to 6 onsite 3 hour sessions

AT&T, Jul 30, 2025 2:26 PM EDT, Public - Pending
Please define the portions of the solutions that are expected to be in scope for Desing Sessions.
Latoya Clark-Forbes, Aug 08, 2025 3:18 PM EDT, Public - Answered
The design sessions will entail discussions specific to the project activities that are required to meet the scope of this project. All requirements documented in the Scope of Work, Project Questionnaire, General Compliance, and Functionality Checklist will be discussed in more detail during the requested design sessions.

#10 - Functionality Checklist NG911 - SR-CR009

AT&T, Jul 30, 2025 3:33 PM EDT, Public - Pending
Please define in detail the term “Non Regional PSAP Routing”
Latoya Clark-Forbes, Aug 08, 2025 3:38 PM EDT, Public - Answered
SR-CR009 (Functionality Checklist) Non-Regional PSAP Routing: Non-Regional PSAP routing should include: • Ability for all calls to be load-balanced across the three hosts similar to how it is balanced today • Ability for the VIPER load balancers to distribute calls to the VIPER servers regardless of the proper PSAP • Ability for the VIPER CHE to distribute calls to the proper PSAP
Latoya Clark-Forbes, Aug 08, 2025 4:01 PM EDT, Public - Answered
Note: The description can be found in Functionality Checklist document.

#11 - Functionality Checklist NG911 - RPT004

AT&T, Jul 30, 2025 3:39 PM EDT, Public - Pending
Log Retrieval - The NG911 system would not process non-911 calls – so requirements for non-911 calls would not be expected – please confirm & clarify the ask.
Latoya Clark-Forbes, Aug 08, 2025 3:20 PM EDT, Public - Answered
As stated in the Functionality Checklist, RPT004, the 911 and Non-Emergency calls are within the scope of the NG911 System. Non-Emergency calls in this instance will include outgoing calls via the NG911 System as stated in Project Questionnaire SR-DL011 requirement.

#12 - Functionality Checklist NG911 - RPT002.b

AT&T, Jul 30, 2025 3:41 PM EDT, Public - Pending
The NG911 system does not have access or visibility to agent availability – so requirements around CPE specific capabilities would not be expected – please confirm
Latoya Clark-Forbes, Aug 08, 2025 3:36 PM EDT, Public - Answered
The list in RPT002.b (Functionality Checklist) are examples of reports. The NG911 Service Provider should provide a list of all available reports and provide at least three report examples.

#13 - Project Questionnaire NG911 - PS002

AT&T, Jul 30, 2025 3:44 PM EDT, Public - Pending
For question PS002, it requires a project plan and schedule to be provided. Is the requirement that this will be provided once awarded as part of the deliverables, or does Broward want those provided as part of the RFP response?
Latoya Clark-Forbes, Aug 08, 2025 3:25 PM EDT, Public - Answered
As stated in the Project Questionnaire, PS002.a, a draft project plan and timeline shall be provided to Broward County that shows the entire project calculated from the date of contract signature to go-live. The draft project plan and timeline are to be provided after contract award.

PS002.b (General Compliance) states that "the NG911 Service Provider should provide an example of project plan and the expected project schedule." as part of the RFP response.

#14 - General Overview a)

Motorola Solutions Connectivity, Inc., Jul 30, 2025 4:19 PM EDT, Public - Pending

The current County requirement SR-IN003 stipulates that "The NG911 Service Provider shall provide multiple POIs for OSPs both locally and nationally with a minimum of four POIs—at least two within Broward County. Having local and national POIs will provide OSPs with interconnection choices." Given the goal of having local and national POIs to provide OSPs with interconnection choices, would the County consider removing the geographical restraint of locating two within the county boundaries, as long as the POIs used are geographically diverse and provide 99.999% service availability?

Latoya Clark-Forbes, Aug 08, 2025 3:26 PM EDT, Public - Answered

Refer to the response to Question 8.

#15 - Scope of Work - General Overview of Desired System

Motorola Solutions Connectivity, Inc., Jul 30, 2025 4:19 PM EDT, Public - Pending

Regarding the requirement for "c) 911 Call Egress/Call Delivery", it currently states that circuits must terminate directly into the Load balancers and VIPER Servers. Typically, an NGCS provider does not terminate circuits directly on the CHE; instead, they provide an ESInet demarcation point for the CHE provider's equipment.

Shall this requirement be updated to specify that the NGCS provider will coordinate with the CHE provider to establish connections to the NGCS network edge devices?

Latoya Clark-Forbes, Aug 08, 2025 3:27 PM EDT, Public - Answered

Refer to the response to Question 5.

#16 - VN007

Motorola Solutions Connectivity, Inc., Jul 30, 2025 4:20 PM EDT, Public - Pending
This requirement states "The NG911 Service Provider should provide the NG911 Solution (OSP interface, NGCS and ESInet) MTBF metric for the last 24 months for its customer base in Florida, Georgia, and Alabama." Given that NGCS providers typically offer services nationwide, would it be possible to broaden this requirement to include 24 months of metrics from their NGCS customers across the entire nation?
Latoya Clark-Forbes, Aug 08, 2025 3:27 PM EDT, Public - Answered
Per the General Compliance questionnaire, VN007, the County only wants to see MTBF metrics for customers in Florida, Georgia, and Alabama.

#17 - VN008

Motorola Solutions Connectivity, Inc., Jul 30, 2025 4:20 PM EDT, Public - Pending
This requirement states "The NG911 Service Provider should provide Call delivery (NGCS to PSAP) network metrics for latency and Mean Opinion Score (MOS) for the last 24 months for its customer base in Florida, Georgia, and Alabama." Given that NGCS providers typically offer services nationwide, would it be possible to broaden this requirement to include 24 months of metrics from their NGCS customers across the entire nation?
Latoya Clark-Forbes, Aug 08, 2025 3:27 PM EDT, Public - Answered
Per the General Compliance questionnaire, VN008, the County only wants to see the Call delivery (NGCS to PSAP) network metrics for latency and Mean Opinion Score (MOS) metric for customers in Florida, Georgia, and Alabama.

#18 - Question Submitted to County

Latoya Clark-Forbes, Aug 11, 2025 4:38 PM EDT, Public - Answered

Regarding Project Questionnaire, PS010, Staff CJIS Certification Requirements:

1) All NG911 Service Provider's staff and subcontractors with access to the components of the NG911 System shall have a background check and Criminal Justice Information Services (CJIS) Level 1 basic security awareness certification. All staff that will be onsite at a County PSAP shall also have CJIS Level 4 advanced security awareness certification which requires Levels 1, 2, and 3 certifications.

2) What is the cost for each CJIS level 1 certification? What is the turnaround time?

3) What is the cost for each CJIS level 4 certification? What is the turnaround time?

4) What additional criteria will be required for the "sponsorship" by Broward County?

Latoya Clark-Forbes, Aug 11, 2025 4:38 PM EDT, Public - Answered

1) For clarification, all staff seeking unescorted access to the Broward County Public Safety Answering Points, access to any PSAP Systems for call taking or dispatching, or Public Safety Networks, requires a CJIS certification for a Security and Privacy: Privileged Role. Any dedicated resources onsite should have CJIS certification. Otherwise, the resources onsite will need to be escorted by E911 or other designated staff for access at any and all times.

2) Broward is unaware of any costs to obtain the CJIS level 1 certification. In recent experiences, turnaround time can range from one to three months.

3) Broward is unaware of any costs to obtain the CJIS level 4 certification. For clarification, the CJIS certification will be for a Security and Privacy: Privileged Role. In recent experiences, turnaround time can range from one to three months.

4) There is no sponsorship required as a part of this project. The CJIS certification will require fingerprints taken and placed on file for each dedicated onsite resource or unescorted resource, a background check is required, sign off of a Security Addendum, and completion of a CJIS Security Awareness Course.

Submissions

Supplier	Date Submitted	Name	Email	Confirmation Code
AT&T	Aug 22, 2025 9:34 AM EDT	Mario Ruiz	maruiz@att.com	NjgwMTc1
INdigital	Aug 22, 2025 1:36 PM EDT	Larry Stidham	lstidham@indigital.net	NjgwNTg1
Motorola Solutions Connectivity, Inc.	Aug 22, 2025 11:04 AM EDT	Jarrod Shupe	jarrod.shupe@motorolasolutions.com	NjgwMjc4

Responses

Success: All data is valid!

							Numeric	
Status	Bid/No Bid Decision	#	Item	Item Description	Quantity Required	Unit of Measure	Unit Price	Total Cost
Network - Pricing provided shall include all non-recurring costs to deliver all of the requirements in the Scope of Work for the complete solution propose								
Not Bidding	No Bid	#1-1	Primary Connectivity to PSAPs	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide primary connectivity to the Regional and Non Regional Public Safety Answering Points (PSAPs) through Load Balancers.	1	Lumpsum		-
Not Bidding	No Bid	#1-2	Secondary Connectivity to each environment	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide secondary connectivity to the Regional and Non Regional PSAP Environment through the	1	Lumpsum		-
Not Bidding	No Bid	#1-3	Tertiary Connectivity to PSAPs	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide tertiary connectivity to the Regional and Non-Regional PSAPs through various options available (e.g. Non Terrestrial - Satellite, FirstNet, etc.).	1	Lumpsum		-
Not Bidding	No Bid	#1-4	Connectivity to other networks (within Neighboring Counties)	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide connectivity to other networks through Network to Network Interfaces for NG911 systems and Legacy Systems.	1	Lumpsum		-
Not Bidding	No Bid	#1-5	OSP in county POI Connectivity	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide OSP connectivity to POIs within Broward County.	1	Lumpsum		-
Basket Total								$ 0.00

NG911 Services - Pricing provided shall include all non-recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#2-1	**Next Generation Core Services Configuration**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Next Generation Core Services as a part of the collection and configuration of all NGCS NENA i3 Core Functions including normal, business continuity, failover, and alternate call routing.	1	Lumpsum		-
Not Bidding	**No Bid**	#2-2	**NGCS Build Out - Call Ingress**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide NGCS Call Ingress Build Out Components used to receive calls from the OSPs such as BCF, POI, LNG, LSRG, etc.	1	Lumpsum		-
Not Bidding	**No Bid**	#2-3	**NGCS Build Out - Call Processing**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide NGCS Call Processing Build Out Components used to process calls in the NGCS such as ESRP, ECRF, PRF, etc.	1	Lumpsum		-
Not Bidding	**No Bid**	#2-4	**NGCS Build Out - Call Egress**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide NGCS Call Egress Build Out Components use to deliver calls to the PSAPs such as BCF, LPG, etc.	1	Lumpsum		-
Not Bidding	**No Bid**	#2-5	**NGCS Build Out - Data Systems**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide NGCS Data Systems Build Out Components used to collect, process, store and use NG911 data such as SI, LVF,GIS validation tools, GIS repository integration etc.	1	Lumpsum		-

Not Bidding	No Bid	#2-6	**Real Time Text and SMS Text to 911 Delivery**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Transitional costs for Real Time Text and SMS Text to 911 delivery that is expected to be eliminated with OSP Phase 2 migration.	1	Lumpsum		-
Basket Total								**$ 0.00**

Professional Services - Pricing provided shall include all non-recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	No Bid	#3-1	**Training**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Training as indicated in sections TRN001-TRN012.	1	Lumpsum		-
Not Bidding	No Bid	#3-2	**Onsite technical support for installation test, go live and post go live**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Onsite technical support for installation test, go live and post go live.	1	Lumpsum		-
Not Bidding	No Bid	#3-3	**Project Management and Senior Technical Support**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide all Project Management and Technical Support onsite resources for the project kickoff, design sessions, all phases of testing, project implementation, and up to 20 business days per environment for post go live	1	Lumpsum		-
Not Bidding	No Bid	#3-4	**Integration / Coordination Services with OSPs, CHE, other service providers**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Integration/Coordination Services with OSPs, CHE, other service providers.	1	Lumpsum		-

Not Bidding	**No Bid**	#3-5	**Design Sessions to include up to 6 onsite 3 hour sessions**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Price to provide Design Sessions to include up to 6 onsite 3 hour sessions.	1	Lumpsum		-
Basket Total								**$ 0.00**

Year 1 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#4-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide Ongoing Hosting during Post Implementation. Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance for all environments and Broward County has notified the NG911 Service	12	Month		-
Not Bidding	**No Bid**	#4-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide Primary Connectivity to the PSAPs. Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance of all environments and Broward County has notified the NG911 Service	12	Month		-
Not Bidding	**No Bid**	#4-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide Secondary Connectivity to each environment. Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance of all environments and Broward County has notified the NG911 Service	12	Month		-

Not Bidding	No Bid	#4-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide Tertiary Connectivity to the Regional and Non-Regional PSAPs through various options available (e.g. Non Terrestrial - Satellite, FirstNet, etc.). Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance of all environments and Broward	12	Month		-
Not Bidding	No Bid	#4-5	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide OSP connectivity to POIs within Broward County. Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance of all environments and Broward County has notified the NG911 Service	12	Month		-
Not Bidding	No Bid	#4-6	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price to provide OSP connectivity to POIs within Broward County. Please note: Year 1 billing will begin after successfully completing 60 days of final acceptance of all environments and Broward County has notified the NG911 Service	12	Month		-
Basket Total								**$ 0.00**

Year 2 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	No Bid	#5-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide Ongoing Hosting during Post Implementation.	12	Month		-

Not Bidding	No Bid	#5-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide Primary Connectivity to	12	Month		-
Not Bidding	No Bid	#5-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide Secondary Connectivity to each environment.	12	Month		-
Not Bidding	No Bid	#5-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide Tertiary	12	Month		-
Not Bidding	No Bid	#5-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide Connectivity to other networks (within neighboring counties).	12	Month		-
Not Bidding	No Bid	#5-6	**OSP in county POI Connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 2 to provide OSP connectivity to POIs within Broward County.	12	Month		-
Basket Total								**$ 0.00**

Year 3 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	No Bid	#6-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide Ongoing Hosting during Post Implementation.	12	Month		-
Not Bidding	No Bid	#6-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide Primary Connectivity to	12	Month		-

Not Bidding	No Bid	#6-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide Secondary Connectivity to each environment.	12	Month		-
Not Bidding	No Bid	#6-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide Tertiary Connectivity to	12	Month		-
Not Bidding	No Bid	#6-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide Connectivity to other networks (within neighboring counties).	12	Month		-
Not Bidding	No Bid	#6-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 3 to provide OSP connectivity to POIs within Broward County.	12	Month		-
Basket Total								**$ 0.00**

Year 4 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	No Bid	#7-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide Ongoing Hosting during Post Implementation.	12	Month		-
Not Bidding	No Bid	#7-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide Primary Connectivity to	12	Month		-

Not Bidding	No Bid	#7-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide Secondary Connectivity to each environment.	12	Month		-
Not Bidding	No Bid	#7-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide Tertiary Connectivity to	12	Month		-
Not Bidding	No Bid	#7-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide Connectivity to other networks (within neighboring counties).	12	Month		-
Not Bidding	No Bid	#7-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 4 to provide OSP connectivity to POIs within	12	Month		-
Basket Total								**$ 0.00**

Year 5 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	No Bid	#8-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide Ongoing Hosting during Post Implementation.	12	Month		-
Not Bidding	No Bid	#8-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide Primary Connectivity to	12	Month		-

Not Bidding	**No Bid**	#8-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide Secondary Connectivity to each environment.	12	Month		-
Not Bidding	**No Bid**	#8-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide Tertiary Connectivity to	12	Month		-
Not Bidding	**No Bid**	#8-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide Connectivity to other networks (within neighboring counties).	12	Month		-
Not Bidding	**No Bid**	#8-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 5 to provide OSP connectivity to POIs within	12	Month		-
Basket Total								**$ 0.00**
Grand Total								**$ 0.00**

Primary Responses

Success: All data is valid!

Status	Bid/No Bid Decision	#	Item	Item Description	Quantity Required	Unit of Measure	Numeric Unit Price	Total Cost
OPTIONAL Year 6 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.								
Not Bidding	**No Bid**	#1-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide Ongoing Hosting during Post Implementation. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#1-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide Primary Connectivity to the PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-
Not Bidding	**No Bid**	#1-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide Secondary Connectivity to each environment. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#1-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide Tertiary Connectivity to PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-

Not Bidding	**No Bid**	#1-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide Connectivity to other networks (within neighboring counties). Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#1-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 6 to provide OSP connectivity to POIs within Broward County. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Basket Total								**$ 0.00**

OPTIONAL Year 7 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#2-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide Ongoing Hosting during Post Implementation. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#2-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide Primary Connectivity to the PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-

Not Bidding	**No Bid**	#2-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide Secondary Connectivity to each environment. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#2-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide Tertiary Connectivity to PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-
Not Bidding	**No Bid**	#2-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide Connectivity to other networks (within neighboring counties). Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#2-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 7 to provide OSP connectivity to POIs within Broward County. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Basket Total								**$ 0.00**

OPTIONAL Year 8 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#3-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide Ongoing Hosting during Post Implementation. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#3-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide Primary Connectivity to the PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-
Not Bidding	**No Bid**	#3-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide Secondary Connectivity to each environment. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#3-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide Tertiary Connectivity to PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-

Not Bidding	**No Bid**	#3-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide Connectivity to other networks (within neighboring counties). Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#3-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 8 to provide OSP connectivity to POIs within Broward County. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Basket Total								**$ 0.00**

OPTIONAL Year 9 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#4-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide Ongoing Hosting during Post Implementation. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#4-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide Primary Connectivity to the PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-

Not Bidding	**No Bid**	#4-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide Secondary Connectivity to each environment. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#4-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide Tertiary Connectivity to PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-
Not Bidding	**No Bid**	#4-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide Connectivity to other networks (within neighboring counties). Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#4-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 9 to provide OSP connectivity to POIs within Broward County. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Basket Total								**$ 0.00**

OPTIONAL Year 10 - Pricing provided shall include all recurring costs to deliver all of the requirements in the Scope of Work for the complete solution proposed.

Not Bidding	**No Bid**	#5-1	**Ongoing Hosting Post Implementation**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide Ongoing Hosting during Post Implementation. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#5-2	**Primary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide Primary Connectivity to the PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#5-3	**Secondary Connectivity to each environment**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide Secondary Connectivity to each environment. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#5-4	**Tertiary Connectivity to PSAPs**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide Tertiary Connectivity to PSAPs. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points	12	Month		-

Not Bidding	**No Bid**	#5-5	**Connectivity to other networks (within Neighboring Counties)**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide Connectivity to other networks (within neighboring counties). Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Not Bidding	**No Bid**	#5-6	**OSP in county POI connectivity**	Vendors are hereby informed that the Unit Price for this line item will be the Vendor's proposed (all-inclusive) not-to-exceed Monthly Price for Year 10 to provide OSP connectivity to POIs within Broward County. Note: The Vendor's proposed Unit Price will not be used in the calculation of Vendor's points for price.	12	Month		-
Basket Total								**$ 0.00**
Grand Total								**$ 0.00**

Additional Responses

Success: All data is valid!

						Numeric	
Status	**#**	**Item**	**Item Description**	**Quantity Required**	**Unit of Measure**	**Unit Price**	**Total Cost**
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-

-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-

-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-

-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-

-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-
-							-

-							-
-							-
-							-
-							-
-							-
-							-
-							-

SUMMARY OF VENDOR RIGHTS FOR BROWARD COUNTY COMPETITIVE SOLICITATIONS

The purpose of this document is to provide vendors with a summary of their rights to object to or protest a proposed award or recommended ranking of vendors in connection with Broward County competitive solicitations. These rights are fully set forth in the Broward County Procurement Code.

1. **Right to Object**
   For Requests for Proposals (RFP), Requests for Qualifications (RFQ), or Requests for Letters of Interest (RLI), vendors may object in writing to a proposed recommendation of ranking made by an Evaluation Committee. Objections must be filed within three business days after the proposed recommendation of ranking (if applicable) is posted on the Purchasing Division's website. The written objection must comply with the requirements stated in Section 21.42(h) of the Broward County Procurement Code. Failure to timely and fully meet any requirement will result in the loss of a right to object.

2. **Right to Protest**
   For Invitations to Bid (ITBs), RFPs, RFQs, and RLIs, vendors may protest the specifications or requirements of a solicitation (or of any addenda). Protests must be received in writing by the Director of Purchasing within five business days after the applicable solicitation (or addenda) is posted on the Purchasing Division's website.

   For ITBs, vendors may protest a recommendation for award made by the Broward County Purchasing Division. For RFPs, RFQs, and RLIs, vendors may protest a final recommendation of ranking made by an Evaluation Committee. In all cases, protests must be filed in writing within five business days after a recommended ranking or recommendation for award is posted on the Purchasing Division's website.

   Any protest must comply with requirements stated in Part X of the Broward County Procurement Code, including a filing fee (if applicable). Failure to timely and fully meet any requirement will result in a loss of protest rights.

   Vendors may appeal the denial of a protest. Section 21.81 of the Broward County Procurement Code identifies all other matters that may be appealed. Appeals may require payment of an appeal bond. Appeals must comply with requirements stated in Part XII of the Broward County Procurement Code. Failure to timely and fully meet any requirement will result in a loss of appeal rights.

Cone of Silence:
The County's Cone of Silence Ordinance prohibits all communications, oral or written, relating to a competitive solicitation among vendors/vendor representatives, County Staff, and Commissioner Offices while the cone is in effect. Communications with Purchasing Division employees, the solicitation's designated Project Manager(s) or designee(s), the Office of Economic and Small Business (OESBD) Small Business Development Specialist Supervisor (954-357-6400), and others as specifically identified in the Cone of Silence Ordinance are permitted. Additionally, communication is permitted at pre-bid conferences and negotiation meetings, as applicable.

The Cone of Silence begins upon the advertisement of an ITB, RFP, RFQ, or RLI. The Cone of Silence terminates when the solicitation is awarded, all responses are rejected, or the Broward County Board of County Commissioners takes other action which ends the solicitation, as stated in more detail in the Cone of Silence Ordinance.

Any violations of the Code of Silence Ordinance by any vendor or vendor representative may be reported to the County's Professional Standards/Human Rights Section. If the County's Professional Standards/Human Rights Section determines that a violation has occurred, a fine shall be imposed as provided in the Broward County Code of Ordinances. At the sole discretion of the Broward County Board of County Commissioners, a violation may void an award of the applicable competitive solicitation.

Review the Cone of Silence Ordinance, Section 1-266 of the Broward County Code of Ordinances, for more detailed information.

Form Date 9/9/24

LOBBYIST REGISTRATION REQUIREMENT CERTIFICATION

The completed form should be submitted with the solicitation response but must be submitted within three business days after County's request. The Vendor may be deemed nonresponsive for failure to fully comply within stated timeframes.

The Vendor certifies that it understands if it has retained a lobbyist(s) to lobby in connection with a competitive solicitation, it shall be deemed nonresponsive unless the firm, in responding to the competitive solicitation, certifies that each lobbyist retained has timely filed the registration or amended registration required under the Broward County Lobbyist Registration Act, Sections 1-260 through 1-262, Broward County Code of Ordinances; and it understands that if, after awarding a contract in connection with the solicitation, the County learns that the certification was erroneous, and upon investigation determines that the error was willful or intentional on the part of the Vendor, the County may, on that basis, exercise any contractual right to terminate the contract for convenience.

The Vendor hereby certifies that: (select one)

☐ It has not retained a lobbyist(s) to lobby in connection with this competitive solicitation; however, if retained after the solicitation, the County will be promptly notified.

☐ It has retained a lobbyist(s) to lobby in connection with this competitive solicitation and certifies that each lobbyist retained has timely filed the registration or amended registration required under Broward County Lobbyist Registration Act, Sections 1-260 through 1-262, Broward County Code of Ordinances.

It is a requirement of this solicitation that the names of any and all lobbyists retained to lobby in connection with this solicitation be listed below:

Name of Lobbyist: Click or tap here to enter text.	Name of Lobbyist: Click or tap here to enter text.
Lobbyist's Firm: Click or tap here to enter text.	Lobbyist's Firm: Click or tap here to enter text.
Phone: Click or tap here to enter text.	Phone: Click or tap here to enter text.
E-mail: Click or tap here to enter text.	E-mail: Click or tap here to enter text.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

OFFICE OF ECONOMIC AND SMALL BUSINESS DEVELOPMENT REQUIREMENTS
AFFILIATED ENTITIES OF THE PRINCIPAL(S) CERTIFICATION

The completed form should be submitted with the solicitation response. If not submitted with the solicitation response, it must be submitted within three business days after of County's request. Failure to timely submit may result in Vendor being deemed non-responsive.

a. All Vendors are required to disclose the names and addresses of Affiliated Entities (defined below) of the Vendor's principal(s) over the last five years (from the solicitation opening deadline) that have acted as a prime vendor with the County.

b. The County will review all Affiliated Entities of the Vendor's principal(s) for contract performance evaluations and the compliance history with the County's Small Business Development Program, including County Business Enterprise (CBE), Disadvantaged Business Enterprise (DBE) and Small Business Enterprise (SBE) goal attainment requirements. "Affiliated Entities" of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent, or sibling entity.

c. The County will consider the contract performance evaluations and the compliance history of the Affiliated Entities of the Vendor's principals in its review and determination of responsibility.

The Vendor hereby certifies that: (select one)

☐ No principal of the proposing Vendor has prior affiliations that meet the criteria defined as Affiliated Entities.

☐ Principal(s) listed below have prior affiliations that meet the criteria defined as Affiliated Entities.

Principal's Name: Click or tap here to enter text.
Names and addresses of Affiliated Entities: Click or tap here to enter text.

Principal's Name: Click or tap here to enter text.
Names and addresses of Affiliated Entities: Click or tap here to enter text.

Principal's Name: Click or tap here to enter text.
Names and addresses of Affiliated Entities: Click or tap here to enter text.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

OWNERSHIP DISCLOSURE

Broward County is collecting entity ownership information for Vendors. This is for informational purposes only and the data will be used for Broward County's research on possible contracting opportunity disparities. The forms will be maintained separately from all other records of this solicitation and will be accessible only by authorized personnel. The information provided will not be used in determining whether the Vendor will receive a contract award. **In accordance with Section 287.05701, Florida Statutes, the County may not request documentation or consider a vendor's social, political, or ideological interests when determining if the vendor is a responsible vendor or give preference to a vendor based on the vendor's social, political, or ideological interests.**

Submit the form only through the link provided below. Do not submit the form as part of Vendor's response in electronic bidding system.

Link for form submittal: Ownership Disclosure Form

Form Date 9/9/24

SUBCONTRACTORS/SUBCONSULTANTS/SUPPLIERS REQUIREMENT

The completed and signed form(s) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days after County's request. Vendor may be deemed nonresponsive for failure to fully comply within the stated timeframes.

A. The Vendor must submit a listing of all subcontractors, subconsultants, and major material suppliers (firms), if any, and the portion of the contract they will perform. A major material supplier is considered any firm that provides construction material for construction contracts, or commodities for service contracts, in excess of $50,000, to the Vendor.

B. If participation goals apply to the contract, only non-certified firms shall be identified on the form. A non- certified firm is a firm that is not listed as a firm for attainment of participation goals (e.g., County Business Enterprise or Disadvantaged Business Enterprise), if applicable to the solicitation.

C. This list shall be kept up-to-date for the duration of the contract. If subcontractors, subconsultants, or suppliers are stated, this does not relieve the Vendor from the prime responsibility of full and complete satisfactory performance under any awarded contract.

D. After completion of the contract/final payment, the Vendor shall certify the final list of non-certified subcontractors, subconsultants, and suppliers that performed or provided services to the County for the referenced contract.

E. The Vendor has confirmed that none of the listed subcontractors, subconsultants, or suppliers' principal(s), officer(s), affiliate(s), or any other related companies, have been debarred from doing business with Broward County or any other governmental agency.

If none, state "none" on this form. Use additional sheets as needed. Vendor should scan and upload any additional form(s) in electric bidding system.

1. Subcontracted Firm's Name: Click or tap here to enter text.

   Subcontracted Firm's Address: Click or tap here to enter text.

   Subcontracted Firm's Telephone Number: Click or tap here to enter text.

   Contact Person's Name and Position: Click or tap here to enter text.

   Contact Person's E-mail: Click or tap here to enter text.

   Type of Work/Supplies Provided: Click or tap here to enter text.

2. Subcontracted Firm's Name: Click or tap here to enter text.

   Subcontracted Firm's Address: Click or tap here to enter text.

   Subcontracted Firm's Telephone Number: Click or tap here to enter text.

   Contact Person's Name and Position: Click or tap here to enter text.

   Contact Person's E-mail: Click or tap here to enter text.

   Type of Work/Supplies Provided: Click or tap here to enter text.

SUBCONTRACTORS/SUBCONSULTANTS/SUPPLIERS REQUIREMENT

3. Subcontracted Firm's Name: Click or tap here to enter text.
   Subcontracted Firm's Address: Click or tap here to enter text.
   Subcontracted Firm's Telephone Number: Click or tap here to enter text.
   Contact Person's Name and Position: Click or tap here to enter text.
   Contact Person's E-mail: Click or tap here to enter text.
   Type of Work/Supplies Provided: Click or tap here to enter text.

4. Subcontracted Firm's Name: Click or tap here to enter text.
   Subcontracted Firm's Address: Click or tap here to enter text.
   Subcontracted Firm's Telephone Number: Click or tap here to enter text.
   Contact Person's Name and Position: Click or tap here to enter text.
   Contact Person's E-mail: Click or tap here to enter text.
   Type of Work/Supplies Provided: Click or tap here to enter text.

By signature below, I certify on behalf of the Vendor that the information stated above is true and correct to the best of my knowledge.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

ANTI-HUMAN TRAFFICKING AFFIDAVIT

This completed form should be returned with the Vendor's submittal. If not provided with the submittal, the Vendor must submit this form within three (3) business days after the County's request and upon award, renewal, or extension of a contract with Broward County. The Vendor may be deemed nonresponsive for failure to fully comply within the stated timeframe.

The Vendor indicated below does not use coercion for labor or services, as such terms are defined in Section 787.06, Florida Statutes.

Under penalties of perjury, the undersigned declares that they have read the foregoing statement and that the facts stated in it are true.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

SECURITY REQUIREMENTS

A. General Security Requirements:

1. All contractor personnel requiring unescorted access to Broward County facilities must obtain a County-issued contractor identification badge ("contractor ID badge"), unless otherwise specifically stated herein. The requirements for contractor personnel in this document are also required of subcontractor personnel, unless otherwise expressly stated herein.

2. The background screening requirements for obtaining a contractor ID badge will depend on the facility to which unescorted access is being requested. Contractors may contact Broward County Security at (954) 357-6000 or FMSecurity@broward.org for the required background screening requirements associated with access to specific facilities.

3. Contractor ID badges must be visible and worn at all times together with the contractor's company/business ID or badge. Requests for contractor ID badges are initially approved by the requesting agency director or designee and then submitted to Facilities Management Division (FMD) Security for final approval.

4. The issuance of a contractor ID badge for unescorted access to General Facilities requires a Level 1 FDLE background check, which can be conducted by the Florida Department of Law Enforcement (FDLE). This Level 1 FDLE background check is the contractor's responsibility and should be included in the bid price. FDLE background checks can be done by the contractor by phone at (850) 410-8109 or online at https://web.fdle.state.fl.us/search/app/default

5. Upon completion of the background check, the contractor must attach a copy of the results to the contractor's application for a contractor ID badge. The Project Manager or designee utilizing the service of the contractor will be the "Sponsor" and will either provide the contractor with a Contractor ID Badge Request Form or assist the contractor in completing an online application for the County issued contractor ID badge.

6. Requests for a contractor ID badge requiring an FDLE background check may require lengthy processing and review by the Broward Sheriff's Office (BSO). Contractors must therefore submit the request to Broward County Security at least two (2) weeks prior to the start of service by the contractor. When contractor ID badges are ready, Broward County Security will contact the contractor to arrange pick up. Upon pick up, the applicant must present a valid Florida identification and must be accompanied by their supervisor. Broward County Security will then supply a contractor ID badge valid for the anticipated period within which the work will be performed. The validity period must be clearly stated on the Contractor ID Badge Request Form; however, the period of validity will not exceed one (1) year. Background checks will be required for renewal of contractor ID badges. At the termination of the contract and separation of employee services, the contractor is responsible for the collection and return of all contractor ID badges to the Project Manager and/or to Broward County Security.

7. Compliance with the County's security requirements is part of the overall contract performance evaluation. Final payment will, in part, be contingent on the return of all contractor ID badges issued to contractor personnel.

8. Broward County Security is located at Governmental Center East, 115 South Andrews Avenue, Fort Lauderdale, FL 33301. Telephone (954) 357-6000.

9. All contractor personnel must wear distinctive and neat appearing uniforms with the contractor's company name. Subcontractor personnel must also have Broward County issued contractor IDs and meet the same security requirements and uniform standards as the primary contractor.

10. Contractor personnel will not be allowed unescorted on the job site without a valid contractor ID badge.

11. These General Security Requirements are in addition to any requirements of specific facilities as stated herein. Additional security requirements may also be included in the applicable solicitation or contract or communicated by the Contract Administrator during the contract period.

B. Facilities Critical to Security and Public Safety:

Many Broward County government facilities have areas designated as critical to security and public safety, pursuant to Broward County Code of Ordinances Sections 26-121 and 26-122, as may be amended. The issuance of a contractor ID badge for unescorted access to facilities critical to security and public safety may entail a comprehensive statewide and national background check. Unescorted access to certain facilities occupied by the Broward Sheriff's Office (BSO) or the State Attorney's Office will require a national fingerprint-based records check per the Criminal Justice Information System (CJIS) policy.

Any contractor personnel found to have a criminal record consisting of felony conviction(s) shall be disqualified from access to the State Attorney's Offices and certain BSO facilities. Any contractor personnel with a record of misdemeanor offense(s) may be granted access if the System Security Officer (CSO), Terminal Access Coordinator (TAC), and FDLE determines that the nature of the offense(s) do not warrant disqualification. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

C. Contractor Work Crews:

Background investigations are generally not required for each member of a contractor work crew working on County premises outside a building or structure. Examples are landscape crews and roofers. If it is necessary to enter the building or structure unescorted, these work crew members must obtain a contractor ID badge. If not, work crew members must be escorted at all times by the project manager or other designated escort, and must be under the direct supervision of a foreperson for the contractor. The foreperson must have a contractor ID badge granting access to the applicable building or structure, be aware of the crew members' whereabouts, have completed the appropriate background check for the location and type of work being undertaken, and been issued and is displaying a contractor ID badge.

All members of a night cleaning crew, and all work crew members who will not be escorted when working at a critical County facility, must complete a background investigation appropriate to the requirements of the facility.

D. Other Vendors:

Other vendors, such as delivery personnel and vending machine operators, without a contractor ID badge may obtain a visitor pass for limited, escorted access. Such persons must be escorted by County personnel when accessing and working in designated non-public and employee work areas at both general facilities and facilities critical to security and public safety.

E. Port Everglades Locations:

1. The Port Everglades Department requires persons to present, at port entry, a valid driver license, and valid reason for wishing to be granted Port access in order to obtain a temporary/visitor ID badge. For persons who will visit the Port more than 15 times in a 90-day period, a permanent identification badge must be obtained and paid for by the contractor for all employees, subcontractors, and agents visiting or working

on the Port project. A restricted access badge application process will include fingerprints and a comprehensive background check. Badges must be renewed annually and the fees paid pursuant to Broward County Administrative Code, Section 42.6. For further information, please call 954-765-4225.

2. All vehicles that are used regularly on the dock apron must have a Dockside Parking Permit. Only a limited number of permits will be issued per business entity. The fee is $100.00 per permit/vehicle. Individuals requesting a permit must possess a valid Port-issued Restricted Access Area badge with a "Dock" destination. Requests for Dockside Parking Permits must be submitted in writing, on company letterhead, to the ID Badge Office. Applicants must demonstrate a need for access to the dock apron. Requests shall be investigated, and approved, if appropriate justification is provided. Supporting documentation must be supplied, if requested. Dock permits are not transferable and must be affixed to the lower left corner of the permitted vehicle's windshield. Should the permit holder wish to transfer the permit to another vehicle during the term of issuance, the permit will be removed and exchanged at no charge for a new permit. Only one business entity representative will be permitted on the dock at a time at the vessel location.

3. The Federal Government has instituted requirements for a Transportation Worker Identification Credential (TWIC) for all personnel requiring unescorted access to designated secure areas within Port Everglades. The contractor will be responsible for complying with the applicable TWIC requirements. For further information, please call 1-855-347-8371, or go online to https://www.tsa.gov/for-industry/twic.

F. Airport Security Program and Aviation Regulations:

1. Contractors must comply with all security and other applicable requirements of the Federal Aviation Regulations applicable to contractor, including, but not limited to, all regulations of the United States Department of Transportation, the Federal Aviation Administration, and the Transportation Security Administration. Contractor shall comply with County's Airport Security Program and the Air Operations Area ("AOA") Vehicle Access Program, and any amendments thereto, and with such other rules and regulations as may be prescribed by the County, including any regulations pertaining to emergency response training, and shall take such steps as may be necessary or directed by County to ensure that contractor and subcontractor personnel, including, but not limited to, employees, invitees, and guests of contractor and subcontractor (collectively, "Contractor Personnel") observe these requirements. If required by the Aviation Department, contractors shall conduct background checks of Contractor Personnel in accordance with applicable federal regulations. If as a result of any act or omission of contractor, subcontractor, or Contractor Personnel, the County incurs any fine and/or penalty imposed by any governmental agency, including, but not limited to, the United States Department of Transportation, the Federal Aviation Administration, or the Transportation Security Administration, or any expense in enforcing any federal regulations, including, but not limited to, airport security regulations or the rules and regulations of the County, and/or any expense in enforcing the County's Airport Security Program, then contractor shall pay and/or reimburse to the County all such fines, penalties, costs, and expenses, including all costs of administrative proceedings, court costs, and attorneys' fees and all costs incurred by the County in enforcing this provision. Contractors shall rectify any security deficiency or other deficiency as may be determined as such by the County or the United States Department of Transportation, Federal Aviation Administration, the Transportation Security Administration, or any other federal agency with jurisdiction. If a contractor fails to remedy any such deficiency, the County may do so at the sole cost and expense of contractor. The County reserves the right to take whatever action is necessary to rectify any security deficiency or other deficiency.

2. Access to Security Identification Display Areas and Identification Media. Contractors shall be responsible for requesting the Aviation Department to issue Airport Issued Identification Media to all Contractor Personnel including those who are authorized access to Security Identification Display Areas ("SIDA") on

the Airport, as designated in the Airport Security Program. In addition, contractors shall be responsible for the immediate reporting of all lost or stolen Airport Issued Identification Media, the immediate return of the media of Contractor Personnel transferred from the Airport or terminated from the employ of contractor or subcontractor, and the immediate return of all Airport Issued Identification Media issued to all Contractor Personnel upon expiration or termination of contractor's agreement with County. Before an Airport Issued Identification Media is issued to Contractor Personnel, contractors must comply with the requirements of applicable federal regulations with regard to fingerprinting for criminal history record checks and security threat assessments, and must require that each Contractor Personnel complete security training programs conducted by the Aviation Department. Contractors shall pay or cause to be paid to the Aviation Department such charges as may be established from time to time for lost or stolen Airport Issued Identification Media and those not returned to the Aviation Department in accordance with these provisions. The Aviation Department has the right to require contractors to conduct background investigations and to furnish certain data on such Contractor Personnel before the issuance of Airport Issued Identification Media, which data may include the fingerprinting of applicants for such media.

3. Operation of Vehicles on the AOA. Unless escorted by an Aviation Department approved escort, before a contractor permits any Contractor Personnel to operate a motor vehicle of any kind or type on the AOA, the contractor shall ensure that all such vehicle operators possess current, valid, and appropriate Florida driver's licenses. In addition, any motor vehicles and equipment of the contractor or of any subcontractor operating on the AOA must have an appropriate vehicle identification permit issued by the Aviation Department, which identification must be displayed as required by the Aviation Department.

4. Consent to Search/Inspection. Contractor vehicles, cargo, goods, and other personal property are subject to being inspected and searched when attempting to enter or leave and while on the AOA. Contractors and subcontractors shall not allow any Contractor Personnel to enter the AOA unless and until such Contractor Personnel has executed a written consent-to-search/inspection form acceptable to the Aviation Department. The foregoing requirements are for the protection of users of the Airport and are intended to reduce incidents of cargo tampering, aircraft sabotage, thefts and other unlawful activities at the Airport. For this reason, Contractor Personnel who do not execute such consent-to-search/inspection form shall not be employed or retained by contractors or by any subcontractor at the Airport in any position requiring access to the AOA or allowed entry to the AOA by any contractor or subcontractor.

5. Nondisclosure Agreement. If any Contractor Personnel are required by a contract with the County to access or otherwise be in contact with Sensitive Security Information ("SSI"), as defined and construed under federal law, such Contractor Personnel will be required to execute a SSI Nondisclosure Agreement provided by the Aviation Department.

G. Water and Wastewater Services (WWS) Security Requirements:

1. Contractors may receive a WWS ID Badge and/or Access Card and/or Keys while working at WWS facility work sites. These items provide modified access to certain areas and systems otherwise restricted to non-WWS employees and can only be obtained from the WWS Security Manager. These items may be rescinded at the discretion of the WWS Security Officer. The WWS ID Badge, Access Card and/or Keys remain the property of Broward County and must be returned to your WWS contact person at the end of the contract/project.

2. To obtain a WWS ID Badge and/or Access Card and/or Keys, contractor personnel must complete and sign the WWS Contractor/Consultant Security Memorandum and provide a copy of their Driver's License to be recorded on Schlage Card Access System Profile.

3. A lost or stolen WWS ID Badge and/or Access Card and/or Keys must be reported to the WWS Security Manager immediately.

4. WWS may terminate access to any contractor personnel who acts inappropriately while on County property. WWS may also contact law enforcement if necessary, to have the contractor personnel removed and/or file charges against them.

H. Parks and Recreation Security Requirements:

1. The awarded contractor ("Contractor") must provide ongoing disclosure throughout the term of its contract with Broward County relative to the criminal background screening required by this Section H.

2. Contractor shall perform criminal background screening as identified in Section H(3) below on contractor personnel who will perform work under its contract in any County park ("collectively referred to as "County Park Property"). Notwithstanding the above, the requirements of this Section H do not apply to independent contractors or subcontractors whose only activities on County Park Property are to make deliveries of goods for the goods or services described in this Contract.

3. Contractor shall not permit any contractor personnel work on County Park Property who: (i) is listed as a sexual predator or sexual offender on the Florida Department of Law Enforcement, Sexual Offenders and Predators Website or the United States Department of Justice, National Sex Offender Public Website; or (ii) who has been convicted of or is pending adjudication of any of the following charges: sexual misconduct; adult abuse, neglect, or exploitation of aged persons or disabled adults or failure to report such abuse; criminal offenses that constitute domestic violence, whether committed in Florida or another jurisdiction; murder; manslaughter, aggravated manslaughter of an elderly person or disabled adult, or aggravated manslaughter of a child; vehicular homicide; killing an unborn child by injury to the mother; assault, battery, and culpable negligence, if the offense was a felony; assault of a minor; battery of a minor; kidnapping; false imprisonment; luring or enticing a child; taking, enticing, or removing a child beyond state limits with criminal intent pending a custody proceeding; carrying a child beyond the state lines with criminal intent to avoid producing a child at a custody hearing or delivering the child to a designated person; exhibiting firearms or weapons within 1,000 feet of a school; possessing an electric weapon or device, destructive device, or other weapon on school property; sexual battery; prohibited acts of persons in familial or custodial authority; unlawful sexual activity with a minor; prostitution; lewd and lascivious behavior; lewdness or indecent exposure; arson; burglary; felony voyeurism; felony theft or robbery; felony fraudulent sale of controlled substances; abuse, aggravated abuse, or neglect of an elderly person or disabled adult; lewd or lascivious offenses committed upon or in the presence of an elderly person or disabled adult; felony exploitation of disabled adults or elderly persons; incest; child abuse, aggravated child abuse, or neglect of a child; contributing to the delinquency or dependency of a child; negligent treatment of children; sexual performance by a child; resisting arrest with violence; depriving a law enforcement, correctional, or correctional probation officer's means of protection or communication; aiding in an escape; aiding in the escape of juvenile inmates in a correctional institution; any offense related to obscene literature; encouraging or recruiting another to join a criminal gang; felony sale, manufacturing, delivery, or possession with intent to sell, manufacture, or deliver, of a controlled substance to a minor; inflicting cruel or inhuman treatment on an inmate resulting in great bodily harm; harboring, concealing, or aiding an escaped prisoner; introduction of contraband into a correctional facility; sexual misconduct in juvenile justice programs; contraband introduced into detention facilities; a crime under Section 944.35, Florida Statutes; or any attempt, solicitation, or conspiracy to commit any of the crimes included in this section. Each of the foregoing crimes are referred to as a "disqualifying offense."

4. Contractor shall maintain copies of the results of all criminal background screening required by this Section H for the term of its contract with Broward County and shall promptly forward copies of same to the County upon request.

5. Contractor shall be required to furnish to County's Parks and Recreation Project Manager ("Project Manager"), on a monthly basis, a Declaration of Criminal Background Screening in the form provided by the Project Manager, listing the information required therein and affirming the persons listed therein have been background screened as required in Item H(3), above, and have been deemed eligible by Contractor to work on County Park Property. Contractor's first monthly declaration must be provided to the Project Manager before Contractor or any of its subcontractors begin working on County Park Property, and shall include all individuals working on County Park Property and the screening results. After the first monthly declaration, Contractor must submit the monthly declaration on or before the fifth (5^{th}) day of each calendar month for the remainder of the Contract's term. Except for the annual rescreening referenced below, the monthly declaration need only identify persons newly working on County Park Property or no longer working on County Park Property since the previous monthly declaration. The Project Manager may, in their discretion, permit Contractor to furnish the monthly declaration in an electronic format. Contractor personnel subject to the criminal background screening under this attachment shall be rescreened annually based on the date of each person's initial screening and the results of same included in the applicable monthly declaration.

6. If Contractor obtains, or is provided, supplemental criminal background information, including police reports and arrest information, showing that a contractor personnel previously deemed eligible by Contractor to work on County Park Property has been arrested on or convicted of a disqualifying offense, Contractor shall take immediate action to review the matter; however, during such review time and until a determination of eligibility is made by Contractor based on the requirements of this Section I, Contractor shall immediately cease allowing such personnel to work on County Park Property. Additionally, Contractor shall require any person background screened pursuant to this Section H to notify Contractor within twenty-four (24) hours of any arrest related to a disqualifying offense that has occurred after the person was deemed eligible to work on County Park Property.

7. Contractor shall, by written contract, require its subcontractors who work on County Park Property to be subject to the requirements and obligations of this Section H.

8. The County Administrator may terminate this contract immediately for cause, and without an opportunity to cure, by written notice provided to Contractor, for any violation related to Contractor's failure to comply with this Section H. Contractor will not be subject to immediate termination if the County Administrator determines, in their sole discretion, that a violation of this Section H was outside the reasonable control of Contractor, and Contractor has demonstrated to the County Administrator subsequent compliance with the requirements of this Section H.

Last updated: 9/9/24

CRIMINAL HISTORY SCREENING PRACTICES CERTIFICATION

The completed form should be returned with the Vendor's submittal. If not provided with the submittal, Vendor must submit the form within three business days after County's request. Vendor may be deemed nonresponsive for failure to fully comply within the stated timeframe.

Section 26-125(d) of the Broward County Code of Ordinances ("Criminal History Screening Practices") requires that a Vendor seeking a contract in the amount of $100,000 or more with Broward County shall certify:

A. Vendor has implemented, or will implement upon award of the contract, policies, practices, and procedures regarding inquiry into the criminal history of an applicant for employment, including a criminal history background check of any such person, that preclude inquiry into an applicant's criminal history until the applicant is selected as a finalist and interviewed for the position.

B. This requirement shall apply only to positions located within the United States that will foreseeably perform work under a contract with Broward County.

C. The failure of Vendor to comply with Section 26-125(d) at any time during the contract term shall constitute a material breach of the contract, entitling Broward County to pursue any remedy permitted under the contract and any other remedy provided under applicable law.

D. If Vendor fails to comply with Section 26-125(d) at any time during the contract term, Broward County may, in addition to all other available remedies, terminate the contract and Vendor may be subject to debarment or suspension proceedings consistent with the procedures in Chapter 21 of the Broward County Administrative Code.

By signing below, Vendor certifies that it is aware of the requirements of Section 26-125(d) of the Broward County Code of Ordinances and certifies the following: (check only one box below).

☐ Vendor certifies that, for positions located within the United States that will foreseeably perform work under a contract with Broward County, it has implemented, or will implement upon award of the contract, policies, practices, and procedures regarding inquiry into the criminal history of an applicant for employment, including a criminal history background check of any such person, that preclude inquiry into an applicant's criminal history until the applicant is selected as a finalist and interviewed for the position.

☐ Vendor is exempt from the requirements of Section 26-125(d) of the Broward County Code of Ordinances because Vendor is required by applicable federal, state, or local law to conduct a criminal history background check in connection with potential employment at a time or in a manner that would otherwise be prohibited by this section, or because Vendor is a governmental agency.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

LITIGATION HISTORY

A. Vendor is required to disclose to the County all "material" cases during the last three (3) years prior to the solicitation response end date, whether such cases were brought by or against the Vendor, any parent or subsidiary of the Vendor, or any predecessor organization.

B. Additionally, the Vendor is required to disclose to the County all "material" cases against any principal of Vendor, regardless of whether the principal was associated with Vendor at the time of the "material" cases against the principal, during the last three (3) years prior to the solicitation response.

C. A "case" means any filed, pending, or resolved litigation, arbitration, or administrative proceeding.

D. A case is considered "material" if it relates, in whole or in part, to any of the following:

1. A similar type of work that the Vendor is seeking to perform for the County under the current solicitation;
2. An allegation of fraud, negligence, error or omissions, or malpractice against the Vendor or any of its principals or agents who would be performing work under the current solicitation;
3. A vendor's default, termination, suspension, failure to perform, or improper performance in connection with any contract;
4. The financial condition of the Vendor, including any bankruptcy petition (voluntary and involuntary) or receivership; or
5. A criminal proceeding or hearing concerning business-related offenses in which the Vendor or its principals (including officers) were/are defendants.

E. For each material case, the Vendor is required to provide all information identified in the **Litigation History Form**. Additionally, the Vendor shall provide a copy of any judgment or settlement of any material case during the last three (3) years prior to the solicitation response. Redactions of any confidential portions of the settlement agreement are only permitted upon a certification by the Vendor that all redactions are required under the express terms of a pre-existing confidentiality agreement or provision.

F. The County will consider the Vendor's litigation history information in its review and determination of responsibility.

G. If the Vendor is a joint venture, the information provided must encompass the joint venture and each of the entities forming the joint venture.

H. Vendor is required to disclose to the County any and all cases(s) that exist between the County and any of the Vendor's subcontractors/subconsultants proposed to work on this project during the last five (5) years prior to the solicitation response.

I. Failure to disclose any material case, including all requested information in connection with each such case, as well as failure to disclose the Vendor's subcontractors/subconsultants litigation history against the County, may result in the Vendor being deemed nonresponsive.

LITIGATION HISTORY FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

☐ There are no material cases for this Vendor; or

☐ Material Case(s) are disclosed below:

Is this for a: (check type)
- ☐ Parent Company
- ☐ Subsidiary
- ☐ Predecessor Firm
- ☐ None of the above

If Yes: Name of Parent Subsidiary/Predecessor: Click or tap here to enter text.

Vendor is Plaintiff ☐ Vendor is Defendant ☐

Case Number: Click or tap here to enter text.

Case Name: Click or tap here to enter text.

Date Filed: Click or tap here to enter text.

Name of Court or other Tribunal: Click or tap here to enter text.

Type of Case: Bankruptcy ☐ Civil ☐ Criminal ☐ Administrative/Regulatory ☐

Claim or Cause of Action and Brief description of each Count: Click or tap here to enter text.

Brief Description of the Subject Matter and Project Involved: Click or tap here to enter text.

Disposition of Case: Pending ☐ Settled ☐ Dismissed ☐

Judgment: Vendor's Favor ☐ Against Vendor ☐

If Judgment is against, is Judgment Satisfied? Yes: ☐ No: ☐

Attach copy of any applicable Judgment, Settlement Agreement, and Satisfaction of Judgement.

Opposing Counsel Name: Click or tap here to enter text.

Opposing Counsel email: Click or tap here to enter text.

Opposing Counsel Phone: Click or tap here to enter text.

Vendor Name: Click or tap here to enter text.

Enterprise Technology Services Security Requirements Exhibit – High Risk

1. Definitions

1.1. County Confidential Information means any County Data that includes employee information, financial information, protected health information, or personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, an individual's biometrics and geolocation, birth dates, banking and financial information, and other information deemed exempt or confidential under state or federal law or applicable regulatory body, including without limitation Section 501.171, Florida Statutes).

1.2. County Data means the data and information (including text, pictures, sound, graphics, video and other data) relating to County or its employees or subcontractors and any third parties , or made available or provided by County or its subcontractors and any third parties to Contractor, for or in the performance of this Agreement, including all derivative data and results derived therefrom, whether or not derived through the use of the Contractor's services, whether or not electronically retained, and regardless of the retention media.

1.3. Equipment means the hardware being provided by Contractor under the Agreement.

1.4. Software means software provided or licensed by Contractor pursuant to the Agreement.

All other capitalized terms not expressly defined within this exhibit shall retain the meaning ascribed to such terms in the Agreement (and if not so defined, then the plain language meaning appropriate to the context in which it is used).

2. County Network Access

2.1. <u>County Network Access.</u> If Contractor will have access to any aspect of County's network via an Active Directory account, onsite access, remote access, or otherwise, Contractor must:

2.1.1. comply at all times with all applicable County access and security standards, regulatory requirements, policies, and procedures related to County's network, as well as any other or additional restrictions or standards for which County provides written notice to Contractor;

2.1.2. provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Contractor's compliance with County security standards;

2.1.3. provide privacy and cybersecurity training to its employees with access to County's network upon hire and at least once annually; and

2.1.4. notify County of any terminations or separations of Contractor's employees who had access to County's network.

In addition, for any remote access to County's network, Contractor must:

2.1.5. utilize secure, strictly-controlled industry standards for encryption (e.g., Virtual Private Networks, Multi-Factor Authentication (MFA), passphrases), and safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure;

2.1.6. utilize only connections that are under Contractor's complete control or under the complete control of a person or entity authorized in advance by County in writing; unencrypted third-party public WiFi networks are not permitted to be used to connect to County's network; ·

2.1.7. utilize only equipment that contains antivirus protection software with current signatures, a currently supported and fully patched operating system, firmware, and third-party applications that are configured for least privileged access;

2.1.8. utilize, at a minimum, industry standard security measures, as determined in County's sole discretion, to safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure; and

2.1.9. activate remote access from Contractor and its approved Subcontractors into the County network only to the extent necessary to perform Services under this Agreement, deactivating such access immediately after use.

If at any point in time County, in the sole discretion of its Chief Information Officer (CIO), determines that Contractor's access to any aspect of County's network presents an unacceptable security risk, or if Contractor exceeds the scope of access required to perform the required Services under the Agreement, County may immediately suspend or terminate Contractor's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's CIO, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to County network to Contractor).

3. Data and Privacy

Data and Privacy. To the extent applicable to the Services being provided by Contractor under the Agreement, Contractor shall comply with all applicable data and privacy laws and regulations, including without limitation Florida Statutes Section 501.171 and Chapter 119, and shall ensure that County Data processed, transmitted, or stored by Contractor or in Contractor's system is not accessed, transmitted or stored outside the United States. Contractor shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification or cybersecurity incident information (as defined by Florida Statutes Sections 501.171, 817.568,

or 817.5685, or Chapter 119, as amended) that Contractor may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If applicable and requested by County, Contractor shall ensure that all hard drives or other storage devices and media that contained County Data have been wiped in accordance with the then-current best industry practices, including without limitation DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

4. Cybersecurity Incidents

Cybersecurity Incidents. Contractor shall report any cybersecurity incident or random incident (as those terms are defined in Section 282.0041, Florida Statutes) impacting or relating to County Data (including but not limited to servers or fail-over servers) to County, including the details required by Section 282.3185(5)(a), in sufficient time to reasonably permit County to timely comply with any required reporting under Section 282.3185(b) and no later than twenty-four (24) hours after becoming aware of such breach (or such shorter time period as may be required under applicable law), unless an extension is granted by County's CIO. Contractor shall provide County with a detailed incident report within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Contractor shall fully cooperate with County on incident response, forensics, and investigations into Contractor's infrastructure as it relates to any County Data or County applications.

5. Managed or Professional Services

5.1. Managed or Professional Services. To the extent applicable to the Services being provided by Contractor under the Agreement:

5.1.1. Contractor shall ensure adequate background checks have been performed on any personnel having access to County Confidential Information. Contractor shall not knowingly allow convicted felons or other persons deemed by Contractor to be a security risk to access County Confidential Data. Contractor shall immediately notify County of any terminations or separations of Contractor's employees who performed Services under the Agreement and who had access to County Confidential Information or the County network.

5.1.2. Contractor shall not release County Data or copies of County Data without the advance written consent of County. If Contractor will be transmitting County Data, Contractor agrees that it will only transmit or exchange County Data via a secure method, including HTTPS, SFTP, or another method approved by County's CIO.

5.1.3. Contractor shall ensure the use of any open source or third-party software or hardware does not undermine the security posture of the Contractor or County.

6. System and Organization Controls (SOC) Report

System and Organization Controls (SOC) Report. If requested by County, Contractor must provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II Report for Contractor and for any third party that provides the applicable services comprising the system, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a sworn declaration certifying Contractor has obtained the referenced SOC 2 Type II Report and listing all complementary user entity controls (CEUCs) identified therein, prior to commencement of the Agreement and on an annual basis during the Agreement, unless this requirement is waived or substitute documentation is accepted in writing by the County's CIO or designee.

7. Software Installed in County's Network

7.1. Software Installed in County's Network. To the extent Contractor provides any Software to be installed in County's network, Contractor must:

7.1.1. advise County of all versions of any third-party software (e.g., Java, Adobe Reader) to be installed and support updates for critical and high-risk vulnerabilities discovered in applicable third-party or open source software;

7.1.2. ensure that the Software is developed based on industry standards and best practices, including following secure programming techniques and incorporating security throughout the Software-development life cycle;

7.1.3. develop and maintain the Software to operate on County-supported and approved operating systems and firmware versions;

7.1.4. mitigate critical and high-risk vulnerabilities (as defined by Common Vulnerability and Exposures (CVE) scoring system) to the Software or Contractor platform within 30 days after patch release, and medium-risk vulnerabilities within 60 days after patch release, notifying County of proposed mitigation steps to be taken and timeline for resolution if Contractor is unable to apply a patch to remedy the vulnerability;

7.1.5. ensure the Software provides for role-based access controls and runs with least privilege access, enables auditing by default for any privileged access or changes, and supports electronic delivery of digitally signed upgrades from Contractor's or the third-party licensor's website;

7.1.6. ensure software connectivity to database systems can be configured to integrate with Active Directory (AD);

7.1.7. ensure the Software is not within three (3) years from its end-of-life date and provide County with end-of-life-schedules for all applicable Software;

7.1.8. support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards, whichever is higher, for County Confidential Data at rest and use transport layer security (TLS) 1.2 or current industry standards, whichever is higher, for data in motion; and

7.1.9. upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

8. Equipment Leased or Purchased from Contractor

8.1. Equipment Leased or Purchased from Contractor. To the extent Contractor is the Original Equipment Manufacturer (OEM) or an authorized reseller for the OEM for any Equipment provided under this Agreement, Contractor must:

8.1.1. ensure that physical security features to prevent tampering are included in any Equipment provided to County and ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment;

8.1.2. ensure any Equipment provided does not contain any embedded remote-control features unless approved in writing by County's Contract Administrator, and disclose any default accounts or backdoors that exist for access to County's network;

8.1.3. shall supply a patch, firmware update, or workaround approved in writing by County's Contract Administrator within thirty (30) days after identification of a new critical or high risk vulnerability, and within sixty (60) days after identification of a medium risk vulnerability and notify County of proposed mitigation steps taken;

8.1.4. develop and maintain Equipment to interface with County-supported and approved operating systems and firmware versions;

8.1.5. upon request by County, make available any required certifications as may be applicable per compliance and regulatory requirements (e.g., Common Criteria, Federal Information Processing Standard 140);

8.1.6. ensure the Equipment is not within three (3) years from its end-of-life date at the time of delivery and provide County with end-of-life-schedules for all applicable Equipment;

8.1.7. (for OEMs only) support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Contractor's or the OEM's website; and

8.1.8. (for OEMs only) upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

9. Payment Card Industry (PCI) Compliance

9.1. Payment Card Industry (PCI) Compliance. If and to the extent at any point during the Agreement the Software accepts, transmits, or stores any cardholder data or is reasonably determined by County to potentially impact the security of County's cardholder data environment ("CDE"), Contractor must:

9.1.1. comply with the most recent version of VISA Cardholder Information Security Program ("CISP") Payment Application Best Practices and Audit Procedures including Security Standards Council's Payment Card Industry ("PCI") Data Security Standard ("DSS"), including the functions relating to storing, processing, and transmitting of the cardholder data;

9.1.2. maintain PCI DSS compliance for the duration of the Agreement;

9.1.3. prior to commencement of the Agreement (or at such time the Software will process cardholder data), prior to Final Acceptance (if applicable), after any significant change to the CDE, and annually, provide to County: (i) a copy of Contractor's Annual PCI DSS Attestation of Compliance ("AOC"); and (ii) a written acknowledgement of responsibility for the security of cardholder data Contractor possesses or otherwise stores, processes, or transmits and for any service Contractor provides that could impact the security of County's CDE (if Contractor subcontracts or in any way outsources the credit card processing, or provides an API that redirects or transmits cardholder to a payment gateway, Contractor is responsible for maintaining PCI compliance for the API and providing the AOC for the subcontractor or payment gateway to County);

9.1.4. maintain and provide to County a PCI DSS responsibility matrix that outlines the exact PCI DSS controls that are the responsibility of either party and the PCI DSS controls that are the shared responsibility of Contractor and County;

9.1.5. follow Open Web Application Security Project (OWASP) for secure coding and transmission of cardholder data only to the extent Contractor provides a payment application;

9.1.6. immediately notify County if Contractor learns or suspects that Contractor, its Software, or its platform is no longer PCI DSS compliant and provide County the steps being taken to remediate the noncompliant status no later than seven (7) calendar days after Contractor learns or suspects it is no longer PCI DSS compliant;

9.1.7. activate remote access from Contractor and its approved Subcontractors into County's network only to the extent necessary to perform Services under this Agreement, deactivating such access immediately after use; and

9.1.8. maintain all inbound and outbound connections to County's CDE using Transport Layer Security (TLS) 1.2 or current industry standard, whichever is higher.

10. HIPAA Compliance

HIPAA Compliance. County has access to protected health information ("PHI") that is subject to the requirements of 45 C.F.R. Parts 160, 162, and 164 and related regulations. If Contractor is considered by County to be a covered entity or business associate or is required to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Contractor shall fully protect individually identifiable health information as required by HIPAA or HITECH and, if requested by County, shall execute a Business Associate Agreement in the form set forth at **www.broward.org/Purchasing/Pages/StandardTerms.aspx.** The County Administrator is authorized to execute a Business Associate Agreement on behalf of County. Where required, Contractor shall handle and secure such PHI in compliance with HIPAA, HITECH, and related regulations and, if required by HIPAA, HITECH, or other Applicable Law, include in its "Notice of Privacy Practices" notice of Contractor's and County's uses of client's PHI. The requirement to comply with this provision, HIPAA, and HITECH shall survive the expiration or earlier termination of this Agreement. Contractor shall ensure that the requirements of this section are included in all agreements with Subcontractors.

11. Application Development Services

Application Development Services. To the extent applicable to the Services being provided by Contractor under the Agreement, Contractor shall develop, implement, and comply with industry-standard secure coding best practices as outlined by the County's Service Provider Application Secure Coding Standard. In addition, if application development services are performed by Contractor augmented staff on behalf of County, staff must strictly follow and adhere to the County's established application development policies, process, procedures, practices and standards. Upon request by County, Contractor shall provide an attestation letter to certify that security testing as specified above was performed along with security scan test results and tests performed. Any exceptions must be documented with the delivery of the attestation letter for acceptance by the County.

MINIMUM INSURANCE REQUIREMENTS

Project: Next Generation 911 (NG911) Project
Agency: Communications and Technology Division

TYPE OF INSURANCE	ADDL INSD	SUBR WVD	MINIMUM LIABILITY LIMITS		
				Each Occurrence	Aggregate
GENERAL LIABILITY - Broad form ☑ Commercial General Liability ☑ Premises–Operations ☐ XCU Explosion/Collapse/Underground ☑ Products/Completed Operations Hazard ☑ Contractual Insurance ☑ Broad Form Property Damage ☑ Independent Contractors ☑ Personal Injury **Per Occurrence or Claims-Made:** ☑ Per Occurrence ☐ Claims-Made **Gen'l Aggregate Limit Applies per:** ☐ Project ☐ Policy ☐ Loc. ☐ Other _____	☑	☑	Bodily Injury		
			Property Damage		
			Combined Bodily Injury and Property Damage	**$1,000,000**	**$2,000,000**
			Personal Injury		
			Products & Completed Operations		
AUTO LIABILITY ☑ Comprehensive Form ☑ Owned ☑ Hired ☑ Non-owned ☑ Any Auto, If applicable ***Note: May be waived if no driving will be done in performance of services/project.***			Bodily Injury (each person)		
			Bodily Injury (each accident)		
			Property Damage		
			Combined Bodily Injury and Property Damage	**$500,000**	
☐ **EXCESS LIABILITY / UMBRELLA** **Per Occurrence or Claims-Made:** ☑ Per Occurrence ☐ Claims-Made *Note: May be used to supplement minimum liability coverage requirements.*					
☑ **WORKER'S COMPENSATION** *Required only of the vendor comes on site to perform services.*	N/A	☑	Each Accident	**STATUTORY LIMITS**	
☑ **EMPLOYER'S LIABILITY**			Each Accident	**$500,000**	
☑ **CYBER LIABILITY**	N/A		Each Claim:	**$3,000,000**	**$5,000,000**
			*Maximum Deductible:	$100,000	
☑ **PROFESSIONAL LIABILITY (ERRORS & OMISSIONS) / TECHNOLOGY ERRORS & OMISSOONS**	N/A		Each Claim:	**$2,000,000**	**$4,000,000**
			*Maximum Deductible:	$100,000	

Description of Operations: Broward County is additional insured for liability. Insured's insurance shall provide primary coverage and shall not require contribution from the County, self-insurance or otherwise. Waiver of subrogation applies in favor of Broward County. For Claims-Made policies insurance must be maintained and evidence of insurance must be provided for at least three (3) years after completion of the contract or work.

CERTIFICATE HOLDER:

Broward County
115 South Andrews Avenue
Fort Lauderdale, Florida 33301

_____
Risk Management Division

Enterprise Technology Services

Vendor Security Questionnaire (VSQ)

ETS Vendor Security Questionnaire (VSQ): Vendor is required to submit a completed ETS Vendor Security Questionnaire (VSQ) (for applicable solution – services, hardware, and/or software). If a response requires additional information, attach additional pages with the required additional information with the additional pages and information labeled to match the applicable question number. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

The Vendor Security Questionnaire (VSQ) assesses the Vendor's security policies and/or system protocol and to identify any potential security vulnerabilities. The County will review the Vendor's VSQ response; any identified security concerns will be disclosed to the Evaluation Committee. Unresolved security concerns shall be considered by the Evaluation Committee as part of its final evaluation and may affect the Vendor's evaluation.

As the Vendor's authorized representative, I attest that any and all statements, oral, written or otherwise, made in support of the Vendor's response, are accurate, true and correct. I also acknowledge that inaccurate, untruthful, or incorrect statements made in support of the Vendor's response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to PART XI of the Broward County Procurement Code.

Vendor Name:	
Vendor Type (Manufacturer, Reseller, Other? If Other, specify.):	
Vendor Contact Person's Name / Title / Email Address:	
Product Name / Description:	
Solicitation Number and Title (If applicable):	

For each applicable section, complete the matrix by using the dropdown option to select YES or NO. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. **Select "N/A" if a question within a given section is not applicable.**

SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES /

No.	Area	Question	Vendor Response	
			YES/NO	Comments
1		**REQUIRED RESPONSE:** Will your organization provide **SOFTWARE-AS-A-SERVICE (SaaS)**? (e.g. Software-as-a-service/SaaS, application, website)		
2		**REQUIRED RESPONSE:** Will your organization provide **HOSTING SERVICES**?		
3		**REQUIRED RESPONSE:** Will your organization provide **APPLICATION DEVELOPMENT SERVICES**? (e.g. on-premise, mobile, web, or other custom code)		
4		**REQUIRED RESPONSE:** Will your organization provide **MANAGED OR PROFESSIONAL SERVICES (UNSUPERVISED BY COUNTY PERSONNEL)**? *(**Note:** "Managed or Professional Services" used herein refers to unsupervised (by County personnel) installation, configuration, consulting, maintenance or monitoring of County systems, applications or infrastructure related to your organization's proposed solution.)*		
		STOP: If you selected NO for Questions 1 through 4 above, **PROCEED TO SECTION 2.**		
5	**Supporting Documentation *(Upon County's request)***	Provide the following: a) Workflow diagram of stored or transmitted information (for SaaS and Hosting Services only)		
6		b) Security / Network Architecture diagram (for SaaS and Hosting Services only)		
7		c) Secure Coding standard (for Application Development Services only)		
8		d) Application Security Program standard (for Application Development Services only)		
9	**Audit Reporting Requirements**	Does your organization have a current System and Organization Controls (SOC) 2, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy)? *(**Note:** For any SaaS or hosted application, the SOC report should be for the organization or application specifically, not the datacenter only.)*		
10	**Payment Card Industry (PCI) environments - Applicable only if Organization or its proposed subcontractor processes or collects credit card information.**	Does your organization have a current Payment Card Industry (PCI) certification (e.g., Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ))?		
11		Will the product or solution process or collect credit card information?		
12		Does your organization maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to confidential County data?		
13	**Electronic Protected Health Information (ePHI) - Applicable only if Organization has access to or will be hosting or storing County ePHI.**	Has your organization had a Risk Assessment performed in the past five years by an external auditor in conjunction with the HIPAA Security rule?		
14		Does your organization maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?		
15		Does your organization have a designated HIPAA Security and Privacy Officer(s)?		
16		Does your organization provide HIPAA Security training to your employees at time of hire and at least annually thereafter?		
17	**Roles & Responsibilities**	Has your organization appointed a central point of contact for security coordination?		
18		Does your organization have an expected timeframe to respond to initial contact for security related issues? Provide timeframe.		
19		Does your organization define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Describe.		

20		Does your organization have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Describe.		
21	**Federated Identity Management and Web Services Integration**	Does your organization's product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory)? Describe.		
22		Does your organization use web services and/or data import/export functions (e.g., API, FTP)? Describe.		
23	**External Parties**	Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization?		
24		Does your organization have a Disaster Recovery and Continuity of Operations plan that includes third-party dependencies to ensure critical business functions can continue even during a major disruption?		
25		Does your organization outsource any aspect of the service to a third party?		
26		Does your organization utilize any off-shore resources for development? Provide location(s).		
27		Does your organization build the application in-house?		
28		Does your organization share customer data with or enable direct access by any third-party?		
29		Will any proposed subcontractors process, access, transmit or store any County data?		
30		Do all proposed subcontractors contractually comply with your organization's security standards for data processing?		
31		Does your organization regularly audit your critical vendors? Describe.		
32	**Information Security Policy & Procedures**	Does your organization have documented standard policies and procedures for security and compliance?		
33	**Risk Assessment**	Does your organization have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?		
34	**Regulatory Compliance**	Is the product or solution currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.		
35		Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?		
36		Has your organization experienced a data breach within the past five years that legally required reporting under applicable law?		
37		Does your organization have procedures for preservation of electronic records and audit logs in case of litigation hold?		
38	**During Employment – Training, Education & Awareness**	Have employees and proposed subcontractors received formal information security awareness training? Provide frequency.		
39		Have your organization's security policies and procedures been communicated to your employees?		
40		Are periodic security reminders provided to your organization's employees?		
41	**Background Checks**	Does your organization perform background checks (e.g., credential verification, criminal history, credit history) to examine and assess an employee's or proposed subcontractor's work and criminal history?		
42		Are individuals who would have access to the County's data subjected to periodic follow-up background checks?		
43	**Prior to Employment - Terms and Conditions of Employment**	Are employees and proposed subcontractors required to sign a non-disclosure agreement and/or confidentiality form upon initial employment?		
44		If so, are employees and proposed subcontractors required to sign the non-disclosure agreement annually?		
45	**Termination or Change in Employment**	Does your organization require that all equipment of any terminated employee or subcontractor is returned and that their user ID is disabled in all systems and badges and/or keys are returned?		
46		Upon transfer, is existing access reviewed for relevance for employees and subcontractors?		
47	**Secure Areas**	Does your organization have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?		
48		Is a locked screensaver displayed on unattended workstations?		
49		Do personnel abide by a clean desk policy to remove and secure sensitive/confidential information from their workspace at the end of the work day?		
50		Does your organization have a contingency plan in place to handle emergency access to facilities?		
51		Are physical access controls authorized? Describe who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data.		
52		Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?		

53		Are employees or subcontractors permitted access to customer environments from your physical locations only?		
54	**Application and Information Access Control - Confidential System Isolation**	Are systems and networks that host, process, and/or transfer confidential information "protected" (i.e., isolated, logically or physically separated) from other systems and/or networks?		
55		Are internal and external networks separated by firewalls with access policies and rules?		
56	**Data Security**	Are development and test environments separate from production environments to protect production applications from inadvertent changes or disruption?		
57		Does your organization apply database and application logical segregation of customer data?		
58		Is this a multi-tenant solution?		
59		Will County's data be co-mingled with data of any other customer?		
60		Does your organization provide a means to encrypt data at rest (e.g., AES)?		
61		Will County's data be processed, accessed, transmitted or stored through an off shore environment (e.g., outside continental U.S, Alaska, Hawaii)?		
62		Does your organization provide a means to encrypt County confidential information in transit? Describe controls that are in place to protect confidential information when transferred (e.g., encryption).		
63		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g., firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?		
64		Does your organization use email encryption to protect sensitive/confidential information when communicating with third parties (e.g., IT vendors)?		
65		Are employees permitted to work remotely from a facility not owned or leased by the organization?		
66		Are encrypted communications required for all remote connections?		
67		Does your organization use a secure VPN connection with third parties (e.g., IT vendors)?		
68		Does your organization have protections in place for ensuring secure remote access (e.g., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling)?		
69		Is there a formal (documented, approved, published, communicated, and implemented) remote access policy?		
70		Can your organization restrict access to the solution to and from the County's network in a "deny all, permit by exception" configuration (i.e., whitelist County IP addresses only)?		
71	**Audit Logging**	Does the software or solution perform audit logging? Describe.		
72		Does the software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?		
73		Does the software track events for user activity (e.g., failed/successful logins, privileged access)? Describe.		
74	**Vulnerability Assessment and Remediation**	Does your organization perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? Provide frequency.		
75		Are internal or proposed subcontractors vulnerability assessments automated?		
76		Does your organization have a security patch management cycle in place to address identified vulnerabilities?		
77		Does your organization provide disclosure of vulnerabilities found in your environment and remediation timelines?		
78		Does your organization notify customer of applicable patches?		
79	**Security Monitoring**	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (e.g., with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports)?		
80		Does your organization monitor your systems and networks for security events? Describe monitoring (e.g., server and networking equipment logs such as servers, routers, switches, wireless APs, monitored regularly).		
81		Does your organization periodically review system activity? Provide frequency.		
82	**Identity & Access Management**	Does your organization have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (e.g., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form)?		
83		Are systems and applications configured to restrict access only to authorized individuals (e.g., use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, expiration)?		
84		Is there a list maintained of authorized users with general access and administrative access (e.g., active directory user lists within a confidential application, a spreadsheet of users, a human resources file)?		

85		Does your organization maintain a list of "accepted mobile devices" (e.g., smart phones, cell phones) and are these devices tracked and managed (e.g., Mobile Device Management)?		
86		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of confidential information?		
87		Is software installation for desktops, laptops, and servers restricted to administrative users only?		
88		Does software or system have automatic logoff for session inactivity?		
89		Does your organization control and monitor access to application source code in a secure manner?		
90		Does your organization deny developers access to production environments, as well as to any environments containing customer data?		
91		Are user IDs for your system uniquely identifiable?		
92		Does your organization have any shared accounts? Describe.		
93		Will your organization allow remote access from proposed subcontractors to the County network, with immediate deactivation after use?		
94		Can service accounts be configured to run as non-privileged user (i.e., non-Domain Admin)?		
95		Is Multi-Factor Authentication (MFA) required for employees/contractors for remote access to production systems?		
96		Is Multi-Factor Authentication (MFA) included as a feature in the proposed system?		
97	**Entitlement Reviews**	Does your organization have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?		
98	**Antivirus**	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?		
99		Is this antivirus product centrally managed (e.g., monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Explain your policies and procedures for management of antivirus software.		
100		Does your organization have a process for detecting and reporting malicious software?		
101	**Network Defense and Host Intrusion Prevention Systems**	Does your organization have any Intrusion Protection System (IPS) in place for your environment?		
102		Are employees prevented from using personally owned smart phones or mobile devices to connect to the organization's network?		
103	**Media Handling**	Does your organization have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?		
104		Is confidential data encrypted when stored on laptop, desktop, server hard drive, flash drive, backup tape (i.e., data at rest)?		
105		Are backup archives stored externally / offsite from your facility?		
106	**Secure Disposal**	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices that contain or process confidential information?		
107	**Separation of Duties**	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?		
108	**Change Management**	Do formal testing and change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability during patching activities, changes to the system, changes to the workstations and servers with appropriate testing, notification, and approval, etc.?		
109	**Incident Management**	In the event of a major security incident or data breach, do you provide the County a third-party digital forensics/incident report?		
110		Does your organization identify, respond to, and mitigate suspected or known security incidents (e.g., incident form completed as a response to each incident)?		
111		Does your organization have a formal incident response and data breach notification plan and team?		
112		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties)?		
113		Are incidents identified, investigated, and reported according to applicable legal requirements?		
114		Are incidents escalated and communicated? Describe.		
115		Do you have a contingency plan in place to handle emergency access to the proposed solution?		
116	**Disaster Recovery Plan & Backups**	Does your organization have a mechanism to back up critical IT systems and County data? Describe.		
117		Does your organization periodically test your backup/restoration plan by restoring from backup media?		
118		Does your organization have a disaster recovery plan?		
119		Are disaster recovery plans updated and tested at least annually?		
120		Do any single points of failure exist that would disrupt functionality of the proposed product or service?		

121	**Product Security Development Lifecycle**	Does your organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing)?		
122		Does your organization maintain an end-of-life-schedule for the proposed software product or solution?		
123		Is the product engineered as a multi-tier architecture design?		
124		Is any proposed product or service within three years of end of life?		
125	**Crypto Materials and Key Management**	Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure?		
126	**Secure Software Design/Testing**	Is the software currently certified by any security standards? (e.g., OWASP, NIST). List standards.		
127		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
128		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
129		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
130		Does your organization remediate all vulnerabilities identified prior to production deployment?		
131		Is your organization outsourcing any aspect of the service to a third party?		
132		Is the product engineered as a multi-tier architecture design?		
133		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?		
134	**Application Development Services - This section is applicable only if Organization is providing Application Development Services (e.g. on-premise, mobile, web, or other custom code)**	Does your organization's development and testing teams receive training specific to application security? Describe.		
135		Does your organization's development team use a development framework? List development languages and framework.		
136		Does your organization follow secure coding development standards?		
137		Does your organization have a security methodology for continuous maintenance of the application and applicable components?		
138		Does your organization review security at each phase of the software development life cycle?		
139		Does your organization use an industry standard methodology for conducting security testing? Describe.		
140		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
141		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
142		Does your organization use an independent third party for periodic security penetration testing?		
143		Does your organization perform peer code reviews on source code prior to production deployment?		
144		Does your organization remediate all vulnerabilities identified prior to production deployment?		
145		Is your organization outsourcing any aspect of the development to a third party?		
146		Will the County receive a copy of the source code?		
147	**Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data.**	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
148		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
149		Does the proposed product or solution use a GenAI model that was developed in house?		
150		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
151		Does this solution interface with a third-party GenAI product?		
152		Does this solution interface with any free or open source GenAI components?		
153		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
154		Is data labeling used to identify content generated by the GenAI product or solution?		
155		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model verified to ensure content provided is accurate?		
156		Will County data be used to train or fine tune the GenAI model used in this solution?		
157		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
158		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
159		Is PII information handled or stored by this GenAI solution?		
160		Will any County data be stored or accessed by the GenAI component?		

161		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
162		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
163		Will the system continue to function if the GenAI service is not available?		
164		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		
165		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
166		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
167		Has a third party vendor risk assessment been performed on this GenAI solution?		
SECTION 2: SOFTWARE INSTALLED IN COUNTY'S NETWORK				
No.	**Area**	**Question**	**Vendor Response**	
			YES/NO	**Comments**
1	**REQUIRED RESPONSE:** Will your organization provide **SOFTWARE INSTALLED LOCALLY IN COUNTY NETWORK**?			
		STOP: If you selected NO for Question 1, **PROCEED TO SECTION 3.**		
2	**Supporting Documentation** ***(Upon County's request)***	Provide the following: a) Hardware and Software requirements (i.e. Operating System, CPUs, RAM)		
3		b) Network connectivity requirements		
4	**Reseller**	Will your organization act as a reseller to provide software to the County? If so, provide manufacturer documentation regarding the security controls of the software and a secure configuration document.		
5	**Software Installation Requirements**	Can the application and service accounts used to run the application be configured to run as non-privileged users (e.g., non-Local Administrator rights)?		
6		Does software require admin rights to be installed? Describe the level of administrative access the software will need on the County domain.		
7		Is remote access required for installation and support? Describe.		
8		Can the software be installed on and operated in a virtualized environment?		
9	**Third Party Software Requirements**	Is third party software (e.g., Java, Adobe, Log4j) required to be installed or embedded within your software for it to work? Provide software and minimum version.		
10		Are you using any open source software components (e.g., no paid license) without paid product support? If so, list software components.		
11		Will the software remain compatible with all updates and new releases of required third party software?		
12	**Secure Software Design/Testing**	Is the software currently certified by any security standards? (e.g., PCI-DSS). Provide standards.		
13		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
14		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
15		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
16		Does your organization remediate all vulnerabilities identified prior to production deployment?		
17		Is your organization outsourcing any aspect of the service to a third party?		
18		Is the product engineered as a multi-tier architecture design?		
19		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?		
20	**Audit Logging**	Does software or solution perform audit logging? Describe.		
21		Does software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?		
22		Does software have audit reporting capabilities (e.g., user activity, privileged access)? Describe.		
23	**Security Updates/Patching**	Does software have a security patch process? Describe your software security patch process, frequency of security patches and upgrade cycle releases.		
24		Does your organization support electronic delivery of digitally signed software and upgrades?		
25	**Secure Configuration / Installation (i.e. PA-DSS configuration)**	Does software allow for secure configuration and installation (e.g., OS hardening, disabling unnecessary services, antivirus compatibility)?		
26		Will software or solution process or collect credit card information?		
27	**Confidential Data**	Does product or solution process, store or transmit confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?		
28		Does software restrict confidential data (e.g., Social Security Number or Date of Birth) from being used as a primary identifier?		
29		Does software have documentation showing where all confidential data is stored in the application?		
30	**Encryption**	Does software support encryption of data in motion (e.g., SSL)?		

31		Does software support encryption of data at rest (e.g., column-level encryption, files)? List controls.		
32	**Authentication**	Does product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.)? Describe.		
33	**Roles and Responsibilities**	Does software provide role-based access control?		
34		Is a service account required for this software to run?		
35		If so, does the service account require admin rights?		
36	**Product Security Development Lifecycle**	Does organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?		
37		Does your organization maintain end-of-life-schedule for the software product?		
38		Is product or service within three years of end of life?		
39	**Regulatory Compliance**	Is the software or solution currently certified by any security standards (e.g., PCI-DSS, HIPAA)? Provide proof of compliance documentation.		
40	**Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data**	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
41		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
42		Does the proposed product or solution use a GenAI model that was developed in house?		
43		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
44		Does this solution interface with a third-party GenAI product?		
45		Does this solution interface with any free or open source GenAI components?		
46		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
47		Is data labeling used to identify content generated by the GenAI product or solution?		
48		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model verified to ensure content provided is accurate?		
49		Will County data be used to train or fine tune the GenAI model used in this solution?		
50		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
51		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
52		Is PII information handled or stored by this GenAI solution?		
53		Will any County data be stored or accessed by the GenAI component?		
54		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
55		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
56		Will the system continue to function if the GenAI service is not available?		
57		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		
58		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
59		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
60		Has a third party vendor risk assessment been performed on this GenAI solution?		

SECTION 3: HARDWARE

No.	Area	Description	Vendor Response	
			YES/NO	Comments
1	**REQUIRED RESPONSE:** Will your organization provide **HARDWARE**?			
	STOP: If you selected NO to Question 1, **SKIP THIS SECTION.**			
2	**Reseller**	Will your organization act as a reseller to provide hardware products to the County? If so, provide manufacturer documentation regarding the supply chain security controls around the hardware and a secure configuration document.		
3	**Secure Hardware Design/Testing**	Is the hardware currently certified by any security standards (e.g., NIST FIPS)?		
4		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
5		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
6		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
7		Does your organization remediate all vulnerabilities identified prior to production deployment?		

8		Is your hardware scanned to detect any vulnerabilities or backdoors within the firmware (i.e, operating system, application code)?		
9		Is your firmware upgraded to remediate vulnerabilities? Provide frequency.		
10		If a new vulnerability is identified, is there a documented timeframe for updates/releases? Provide frequency.		
11		Do you implement security measures during the manufacturing of the hardware? Describe.		
12		Is your organization outsourcing any aspect of the service to a third party?		
13		Are there physical security features used to prevent tampering of the hardware? Identify features.		
14	**Security Updates/Patching**	Does the hardware have a security patch process? Describe your hardware security patch process, frequency of security patches and upgrade cycle releases.		
15		Are there contingencies where key third-party dependencies are concerned?		
16		Will your organization provide a Software Bill of Materials (SBOM) listing all the open-source and third-party components included in the hardware you will be supplying?		
17	**Identity & Access Management**	Are remote control features embedded for the manufacturer's support or ability to remotely access? Describe.		
18		Do backdoors exist that can lead to unauthorized access? Describe.		
19		Do default accounts exist? List all default accounts.		
20		Can default accounts and passwords be changed by Broward County?		
21		Can service accounts be configured to run as non-privileged user (i.e., non-Domain Admin)?		
22	**Confidential Data**	Does the product or solution collect confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?		
23	**Roles and Responsibilities**	Is a service account required for this hardware?		
24		If so, does the service account require admin rights?		
25	**Product Security Development**	Is an end-of-life schedule maintained for the hardware?		
26	**Lifecycle**	Is any proposed product or service within three years of end of life?		
27	**Media Handling**	Does your organization have a secure data wipe and data destruction program for proper drive disposal (e.g., Certificate of destruction, electronic media purging)? Describe.		
28	**Regulatory Compliance**	Is the hardware currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.		
29		Will the product or solution process or collect credit card information?		
30		Does your organization have a process to identify new laws and regulations with IT security implications?		
31	**Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data.**	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
32		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
33		Does the proposed product or solution use a GenAI model that was developed in house?		
34		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
35		Does this solution interface with a third-party GenAI product?		
36		Does this solution interface with any free or open source GenAI components?		
37		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
38		Is data labeling used to identify content generated by the GenAI product or solution?		
39		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model identified to ensure content provided is verifiable?		
40		Will County data be used to train or fine tune the GenAI model used in this solution?		
41		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
42		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
43		Is PII information handled or stored by this GenAI solution?		
44		Will any County data be stored or accessed by the GenAI component?		
45		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
46		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
47		Will the system continue to function if the GenAI service is not available?		
48		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		

49		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
50		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
51		Has a third party vendor risk assessment been performed on this GenAI solution?		

VENDOR REFERENCE VERIFICATION

REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

Vendor should provide a minimum of three (3) non-Broward County Board of County Commissioners' references or as per **Evaluation Criteria** instructions. Vendor should provide the **Vendor Reference Verification Form** to its reference organization/firm to complete and return to the Vendor's attention.

Completed **Vendor Reference Verification Forms** should be submitted with submittal. If not provided with submittal, or if reference is not able to be verified, the Vendor must submit form(s) (or a new Vendor Reference Verification Form) within three business days after the County's written request.

VENDOR REFERENCE VERIFICATION FORM (RFP/RLI/RFQ)

Solicitation No. & Title: GEN2129421P1, Next Generation 911 (NG 911)				
Reference For (hereinafter, "Vendor"):				
Reference Date:				
Organization/Firm Providing Reference:				
Contact Name:				
Contact Title:				
Contact Email:				
Contact Phone:				
Name of Referenced Project:				
Contract Number:				
Date Range of Services Provided:	Start Date:		End Date:	
Project Amount:				
Vendor's Role in Project:	☐ Prime	☐ Subconsultant/Subcontractor		
Would you use this Vendor again?	☐ Yes	☐ No		
If you answered no to the question above, please specify below: (attach additional sheet if needed)				
Description of services provided by Vendor, please specify below: (attach additional sheet if needed)				

Please rate your experience with the referenced Vendor via checkbox:	Needs Improvement	Satisfactory	Excellent	Not Applicable
Vendor's Quality of Service:				
Responsive:	☐	☐	☐	☐
Accuracy:	☐	☐	☐	☐
Deliverables:	☐	☐	☐	☐
Vendor's Organization:				
Staff Expertise:	☐	☐	☐	☐
Professionalism:	☐	☐	☐	☐
Turnover:	☐	☐	☐	☐
Timeliness of:				
Project:	☐	☐	☐	☐
Deliverables:	☐	☐	☐	☐
Project completed within budget:	☐	☐	☐	☐
Cooperation with:				
Your Firm:	☐	☐	☐	☐
Subcontractor(s)/Subconsultant(s):	☐	☐	☐	☐
Regulatory Agency(ies):	☐	☐	☐	☐

All information provided to Broward County is subject to verification. Vendor acknowledges that inaccurate, untruthful, or incorrect statements made in support of this response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to the Broward County Procurement Code.

*****THE SECTION BELOW IS FOR COUNTY USE ONLY*****

Verified via: ☐ Email ☐ Verbal	Verified by:		Division:	
			Date:	

AGREEMENT EXCEPTIONS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, REQUEST FOR LETTER OF INTEREST

The completed form should be submitted with the solicitation response. If not submitted with solicitation response, it shall be deemed an affirmation by the Vendor that it accepts contract terms and conditions stated in the solicitation.

The Vendor must provide on the form below any and all exceptions it takes to the contract terms and conditions stated in the solicitation, including all proposed modifications to the contract terms and conditions or proposed additional terms and conditions. Additionally, a brief justification specifically addressing each provision to which an exception is taken should be provided.

☐ The Vendor takes no exceptions to the contract terms and conditions stated in the solicitation.

☐ The Vendor takes the following exceptions to the contract terms and conditions stated in the solicitation: (use additional forms as needed; separately identify each article/section number)

Term or Condition Article / Section	**Insert proposed modifications to the contract terms and conditions or proposed additional terms and conditions**	**Provide brief justification for proposed modifications**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Vendor Name: Click or tap here to enter text.

Form Date 9/9/24

DOMESTIC PARTNERSHIP ACT CERTIFICATION

REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

Refer to applicable section below. Failure to submit this form by stated timeframes may deem the Vendor nonresponsive to the solicitation *or* ineligible for the Domestic Partnership tiebreaker, as applicable.

Domestic Partnership Responsiveness Requirement (Refer to Instructions to Vendors, if applicable)
This completed and signed form should be returned with the Vendor's submittal. If not provided with the submittal, the Vendor must submit this form within three business days after County's request. A Vendor shall be deemed non-responsive for failure to fully comply within stated timeframes.

Domestic Partnership Tiebreaker (Refer to Instructions to Vendors, if applicable)
To be eligible for the Domestic Partnership tiebreaker, **the Vendor must currently offer the Domestic Partnership benefit and the completed form must be returned at the time of solicitation submittal**. Vendors who fail to comply with this submittal deadline will not be eligible for the Domestic Partnership tiebreaker.

The Domestic Partnership Act, Sections 16½- 150 through 16½-165, Broward County Code of Ordinances (the "Act") requires any Vendor contracting to provide goods or services to the County in an amount over $100,000 to provide benefits to registered domestic partners of its employees on the same basis as the Vendor provides benefits to its employees' spouses, with certain exceptions as provided by the Act.

For all submittals over $100,000, the Vendor, by virtue of the signature below, certifies that it is aware of the requirements of Broward County's Domestic Partnership Act, Section 16½-157, Broward County Code of Ordinances, and certifies the following: (check only one below)

- ☐ The Vendor currently complies with the requirements of the County's Domestic Partnership Act and provides benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses.
- ☐ The Vendor will comply with the requirements of the County's Domestic Partnership Act at time of contract award and provide benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses.
- ☐ The Vendor will not comply with the requirements of the County's Domestic Partnership Act at time of award.
- ☐ The Vendor does not need to comply with the requirements of the County's Domestic Partnership Act at time of award because the following exception(s) applies: (check only one below).
  - ☐ The Vendor employs less than five (5) employees.
  - ☐ The Vendor does not provide benefits to employees' spouses.
  - ☐ The Vendor is a governmental entity, not-for-profit corporation, or charitable organization.
  - ☐ The Vendor is a religious organization, association, society, or non-profit charitable or educational institution.

DOMESTIC PARTNERSHIP ACT CERTIFICATION

REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

☐ The Vendor provides an employee the cash equivalent of benefits. (Attach a notarized affidavitin compliance with the Act stating the efforts taken to provide such benefits and the amount of the cash equivalent).

☐ The Vendor cannot comply with the provisions of the Domestic Partnership Act because it would violate the laws, rules or regulations of federal or state law or would violate or be inconsistent with the terms or conditions of a grant or contract with the United States or the State of Florida. (State the law, statute or regulation and attach explanation of its applicability).

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

LOCATION CERTIFICATION
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

To Be Eligible for Local Preference: (refer to Instructions to Vendors if applicable to the solicitation)
The Vendor should submit this fully completed form and all Required Supporting Documentation (as indicated below) by solicitation end date. If not provided with submittal, the Vendor must submit within three business days after County's written request. Failure to submit required forms or information by stated timeframes may deem the Vendor ineligible for local preference or points for location.

To be eligible for the 'Location' tiebreaker: (refer to Instructions to Vendors if applicable to the solicitation)
The Vendor must submit this fully completed form *and* a copy of its Broward County local business tax receipt by solicitation end date. Vendors who fail to comply with this submittal deadline *will not* be eligible for the location tiebreaker.

Broward County Code of Ordinances, Section 1-74, et seq., provides certain preferences to Local Businesses, Locally Based Businesses, and Locally Based Subsidiaries, and the Broward County Procurement Code provides location as the first tiebreaker criteria. The undersigned Vendor hereby certifies that (check the box for only one option below):

☐ **Option 1:** The Vendor is a **Local Business**, but does not qualify as a Locally Based Business or a Locally Based Subsidiary, as each term is defined by Section 1-74, Broward County Code of Ordinances. The Vendor further certifies that:

A. It has continuously maintained, for at least the one (1) year period immediately preceding the bid posting date (i.e., the date on which the solicitation was advertised),
   i. a physical business address located within the limits of Broward County, listed on the Vendor's valid business tax receipt issued by Broward County (unless exemptfrom business tax receipt requirements),
   ii. in an area zoned for the conduct of such business,
   iii. that the Vendor owns or has the legal right to use, and
   iv. from which the Vendor operates and performs on a day-to-day basis business that is a substantial component of the goods or services being offered to Broward County in connection with the applicable competitive solicitation (as so defined, the "Local Business Location").

   If Option 1 selected, indicate **Local Business Location**:
   Street Address: Click or tap here to enter text.
   City, State, Zip: Click or tap here to enter text.

☐ **Option 2:** The Vendor is both a **Local Business** and a **Locally Based Business** as each term is defined by Section 1-74, Broward County Code of Ordinances. The Vendor further certifies that:

A. The Vendor has continuously maintained, for at least the one (1) year period immediately preceding the bid posting date (i.e., the date on which the solicitationwas advertised),
   i. a physical business address located within the limits of Broward County, listed on the Vendor's valid business tax receipt issued by Broward County(unless exempt from business tax receipt requirements),
   ii. in an area zoned for the conduct of such business,
   iii. that the Vendor owns or has the legal right to use, and
   iv. from which the Vendor operates and performs on a day-to-day basisbusiness that is a substantial component of the goods or services being offered to Broward County in connection with the applicable competitive solicitation as so defined, the "Local Business Location").

B. The Local Business Location is the primary business address of the majority of the Vendor's employees as of the bid posting date, and/or the majority of the work under the solicitation, if

awarded to the Vendor, will be performed by employees of the Vendor whose primary business address is the Local Business Location;

C. The Vendor's management directs, controls, and coordinates all or substantially all of the day-to-day activities of the entity (such as marketing, finance, accounting, human resources, payroll, and operations) from the Local Business Location;

D. The Vendor has not claimed any other location as its principal place of business within the one (1) year period immediately preceding the bid posting date; and

E. Less than fifty percent (50%) of the total equity interests in the business are owned, directly or indirectly, by one or more entities with a principal place of business located outside of Broward County. The Vendor certifies that the total equity interests in the owned, directly or indirectly, by one or more entities with a principal place of business Vendor located outside of Broward County is __ %.

If Option 2 selected, indicate **Local Business Location**:
Street Address: Click or tap here to enter text.
City, State, Zip: Click or tap here to enter text.

☐ **Option 3:** The Vendor is both a **Local Business** and a **Locally Based Subsidiary** as each term is defined by Section 1-74, Broward County Code of Ordinances. The Vendor further certifies that:

A. The Vendor has continuously maintained:
   i. for at least the one (1) year period immediately preceding the bid posting date(i.e., the date on which the solicitation was advertised),
   ii. a physical business address located within the limits of Broward County, listedon the Vendor's valid business tax receipt issued by Broward County (unless exempt from business tax receipt requirements),
   iii. in an area zoned for the conduct of such business,
   iv. that the Vendor owns or has the legal right to use, and
   v. from which the Vendor operates and performs on a day-to-day basis businessthat is a substantial component of the goods or services being offered to Broward County in connection with the applicable competitive solicitation (as so defined, the "Local Business Location").

B. The Local Business Location is the primary business address of the majority of the Vendor's employees as of the bid posting date, and/or the majority of the work under the solicitation, if awarded to the Vendor, will be performed by employees of the Vendor whose primary business address is the Local Business Location;

C. The Vendor's management directs, controls, and coordinates all or substantially all of the day-to-day activities of the entity (such as marketing, finance, accounting, human resources, payroll, and operations) from the Local Business Location;

D. The Vendor has not claimed any other location as its principal place of business within the one (1) year period immediately preceding the bid posting date; and

E. At least fifty percent (50%) of the total equity interests in the business are owned, directly or indirectly, by one or more entities with a principal place of business located outside of Broward County. The Vendor certifies that the total equity interests in the Vendor owned, directly or indirectly, by one or more entities with a principal place of business located outside of Broward County is ____%.

If Option 3 selected, indicate **Local Business Location**:
Street Address: Click or tap here to enter text.
City, State, Zip: Click or tap here to enter text.

LOCATION CERTIFICATION
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

☐ **Option 4:** The Vendor is a **joint venture** composed of one or more Local Businesses,Locally Based Businesses, or Locally Based Subsidiaries, as each term is defined by Section 1-74, Broward County Code of Ordinances. Fill in blanks with percentage equity interest or list "N/A" if section does not apply. The Vendor further certifies that:

A. The proportion of equity interests in the joint venture owned by **Local Business(es)** (each Local Business must comply with all of the requirements stated in Option 1) is _____% of the total equity interests in the joint venture; and/or

B. The proportion of equity interests in the joint venture owned by **Locally Based Business(es)** (each Locally Based Business must comply with all of the requirements stated in Option 2) is _____% of the total equity interests in thejoint venture; and/or

C. The proportion of equity interests in the joint venture owned by **Locally Based Subsidiary(ies)** (each Locally Based Subsidiary must comply with all of the requirements stated in Option 3) is _____% of the total equity interests in the joint venture.

If Option 4 selected, indicate the Local Business Location(s) on separate sheet.

☐ **Option 5:** Vendor is not a Local Business, a Locally Based Business, or a Locally Based Subsidiary, as each term is defined by Section 1-74, Broward County Code of Ordinances.

Required Supporting Documentation (in addition to this form):

Option 1 or 2 (Local Business or Locally Based Business)

1. Broward County local business tax receipt.

Option 3 (**Locally Based Subsidiary**)

1. Broward County local business tax receipt.
2. Documentation identifying the Vendor's vertical corporate organization and names of parent entities.

Option 4 (**joint venture** composed of one or more Local Business(es), Locally Based Business(es), or Locally Based Subsidiary(ies):

1. Broward County local business tax receipt(s) for each Local Business(es), Locally Based Business(es), and/or Locally Based Subsidiary(ies).
2. Executed joint venture agreement if the Vendor is a joint venture.
3. If joint venture is comprised of one or more Locally Based Subsidiary(ies), submit documentation identifying the vertical corporate organization and parent entities name(s) of each Locally Based Subsidiary.

If requested by County (any option):

1. Written proof of the Vendor's ownership or right to use the real property at the Local Business Location.
2. Additional documentation relating to the parent entities of the Vendor.
3. Additional documentation demonstrating the applicable percentage of equity interests in the joint venture, if not shown in the joint venture agreement.
4. Any other documentation requested by County regarding the location from which theactivities of the Vendor are directed, controlled, and coordinated.

By submitting this form, the Vendor certifies that if awarded a contract, it is the intent of the Vendor to remain at the Local Business Locations listed above, if any (or another qualifying Local Business Location within Broward County), for the duration of the contract term, including any renewals or extensions.

LOCATION CERTIFICATION
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

True and Correct Attestations:
Any misleading, inaccurate, or false information or documentation submitted by any party affiliated with this procurement may lead to suspension and/or debarment from doingbusiness with Broward County as authorized by the Broward County Procurement Code. The Vendor understands that, if after contract award, the County learns that any of the information provided by the Vendor on this form was false, and the County determines, upon investigation, that the Vendor's provision of such false information was willful or intentional, the County may exercise any contractual right to terminate the contract. The provision of false or fraudulent information or documentation by a Vendor may subject the Vendor to civil and criminal penalties.

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

Form Date 9/9/24

VOLUME OF PREVIOUS PAYMENTS ATTESTATION

REQUEST FOR PROPOSALS, REQUEST FOR QUALIFICATIONS, OR REQUEST FOR LETTERS OF INTEREST

The completed form(s) should be returned with the Vendor's submittal. If not provided with the submittal, Vendor must submit the form(s) within three business days after County's request. Failure to timely submit this form and supporting documentation may affect the Vendor's evaluation.

Points assigned for Volume of Previous Payments will be based on the amount paid-to-date by the Broward County Board of County Commissioners (County) to a prime Vendor **MINUS** the Vendor's confirmed payments paid-to-date to approved certified County Business Enterprise (CBE) firms performing services as Vendor's subcontractor/subconsultant to obtain the CBE goal commitment as confirmed by County's Office of Economic and Small Business Development. Reporting must be within five (5) years of the current solicitation's closing date.

Vendor must list all received payments paid-to-date by contract as a prime vendor from Broward County Board of County Commissioners. Reporting must be within five (5) years of the current solicitation's closing date.

Vendor must also list all total confirmed payments paid-to-date by contract, to approved certified CBE firms utilized to obtain the contract's CBE goal commitment. Reporting must be within five (5) years of the current solicitation's closing date.

In accordance with Section 21.41(h)(4) and 21.42(d)(3) of the Broward County Procurement Code, the Vendor with the lowest dollar volume of payments previously paid by the County over a five-year period from the current solicitation's closing date will receive the Tie Breaker.

The Vendor attests to the following:

Project Title	Contract No.	Department/Division	Date Awarded	Prime: Paid to Date	CBE: Paid to Date
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Has the Vendor been a member/partner of a Joint Venture firm that was awarded a contract by the County?

☐ Yes (if Yes, Vendor must submit a **Joint Venture Volume of Previous Payments Attestation.)**

☐ No

Vendor Name: Click or tap here to enter text.

Form Date 9/9/24

VOLUME OF PREVIOUS PAYMENTS ATTESTATION

REQUEST FOR PROPOSALS, REQUEST FOR QUALIFICATIONS, OR REQUEST FOR LETTERS OF INTEREST

VOLUME OF PREVIOUS PAYMENTS ATTESTATION FORM FOR JOINT VENTURE

The completed form(s) should be returned with the Vendor's submittal. If not provided with the submittal, Vendor must submit the form(s) within three business days after County's request. Failure to timely submit this form and supporting documentation may affect the Vendor's evaluation.

If a Joint Venture, the payments paid-to-date by contract provided must encompass the Joint Venture and each of the entities forming the Joint Venture. Points assigned for Volume of Previous Payments will be based on the amount paid-to-date by contract to the Joint Venture firm **MINUS** all confirmed payments paid-to-date to approved certified CBE firms utilized to obtain the CBE goal commitment. Reporting must be within five (5) years of the current solicitation's closing date. Amount will then be multiplied by the member firm's equity percentage.

In accordance with Section 21.41(h)(4) and 21.42(d)(3) of the Broward County Procurement Code, the Vendor with the lowest dollar volume of payments previously paid by the County over a five-year period from current solicitation's closing date will receive the Tie Breaker.

The Vendor attests to the following:

Project Title	Contract No.	Department/ Division	Date Awarded	JV Equity Percent	Prime: Paid to Date	CBE: Paid to Date
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Vendor is required to submit an executed Joint Venture agreement(s) and any amendments for each project listed above. Each agreement must be executed prior to the opening date of this solicitation.

Vendor Name: Click or tap here to enter text.

Form Date 9/9/24

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

The completed form, including standard certifications, should be submitted with the solicitation response. If a response requires additional information, the Vendor should upload a written detailed response with submittal; each response should be labeled to match the question number.

If not submitted with solicitation response, it must be submitted within three business days after County's written request. Failure to timely submit may affect Vendor's evaluation.

1. Legal business name: Click or tap here to enter text.
2. Doing Business As/Fictitious Name (if applicable): Click or tap here to enter text.
3. Federal Employer I.D. No. (FEIN): Click or tap here to enter text.
4. Dun and Bradstreet No.: Click or tap here to enter text.
5. Website address (if applicable): Click or tap here to enter text.
6. Principal place of business address: Click or tap here to enter text.
7. Office location responsible for this project: Click or tap here to enter text.
8. Telephone No.: Click or tap here to enter text. Fax No.: Click or tap here to enter text.
9. Generic e-mail for purchase orders: Click or tap here to enter text.
   (Broward County auto distributes purchase orders; to ensure Vendor receives purchase orders, a company accessible e-mail address is suggested.)
10. Type of business (check appropriate box):
    - ☐ Corporation (specify the state of incorporation) Click or tap here to enter text.
    - ☐ Sole Proprietor
    - ☐ Limited Liability Company (LLC)
    - ☐ Limited Partnership
    - ☐ General Partnership
    - ☐ Other – Specify: Click or tap here to enter text.
11. Authorized Contact(s):

Name: Click or tap here to enter text.	Name: Click or tap here to enter text.
Title: Click or tap here to enter text.	Title: Click or tap here to enter text.
E-mail: Click or tap here to enter text.	E-mail: Click or tap here to enter text.
Telephone No.: Click or tap here to enter text.	Telephone No.: Click or tap here to enter text.

12. List name and title of each principal, owner, officer, and majority shareholder:

a) Click or tap here to enter text.	d) Click or tap here to enter text.
b) Click or tap here to enter text.	e) Click or tap here to enter text.
c) Click or tap here to enter text.	f) Click or tap here to enter text.

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

For Questions 13 – 19, if any answer is "Yes", specify details in an attached written response with submittal; each response should be labeled to match the question number.

13. Is Vendor or any of its principals or officers currently a principal or officer of another organization?
☐ Yes ☐ No

14. Has Vendor, or any of its principals, officers, or predecessor organization(s), been debarred or suspended by any government entity within the last three years? ☐ Yes ☐ No

15. Has Vendor ever failed to complete any services and/or delivery of products during the last three years?
☐ Yes ☐ No

16. Have any voluntary or involuntary bankruptcy petitions been filed by or against Vendor, its parent or subsidiaries or predecessor organizations during the last three years? ☐ Yes ☐ No

17. Has Vendor's surety ever intervened to assist in the completion of a contract or have Performance and/or Payment Bond claims been made to Vendor's or its predecessor's sureties during the last three years?
☐ Yes ☐ No

18. Has Vendor ever failed to complete any services and/or delivery of products during the last three years?
☐ Yes ☐ No

19. Has Vendor been terminated from a contract within the last three years? ☐ Yes ☐ No

20. Participation in Solicitation Development: By submission of this solicitation response, the Vendor certifies as follows (select one):

    ☐ I have not participated in the preparation or drafting of any language, scope, or specification that would provide my firm or any affiliate an unfair advantage of securing this solicitation.

    ☐ I have provided information regarding the specifications and/or products listed in this solicitation. If this box is checked, provide the following:

        Name of Person the information was provided to: Click or tap here to enter text.
        Title: Click or tap here to enter text.
        Date information provided: Click or tap here to enter text.
        For what purpose was the information provided? Click or tap here to enter text.

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

Standard Certifications:

Drug-Free Workplace Certification
In accordance with Section 287.087, Florida Statutes, whenever two or more submittals are tied, a submittal received from a Vendor that certifies it has implemented a drug-free workplace program shall be given preference in the award process.

The Vendor hereby certifies that: (only if Vendor is certifying it currently complies, check box)

☐ The Vendor hereby certifies that it has established a drug-free workplace program in accordance with the requirements of Section 287.087, Florida Statutes, ("Preference to businesses with drug-free workplace programs.")

Non-Collusion Certification
Vendor shall disclose, to their best knowledge, any Broward County officer or employee, or any relative of any such officer or employee as defined in Section 112.3135 (1) (c), Florida Statutes, who is an officer or director of, or has a material interest in, the Vendor's business, who is in a position to influence this procurement. Any Broward County officer or employee who has any input into the writing of specifications or requirements, solicitation of offers, decision to award, evaluation of offers, or any other activity pertinent to this procurement is presumed, for purposes hereof, to be in a position to influence this procurement. Failure of a Vendor to disclose any relationship described herein shall be reason for debarment in accordance with the provisions of the Broward County Procurement Code.

The Vendor hereby certifies that: (select one)

☐ The Vendor certifies that this offer is made independently and free from collusion; or

☐ The Vendor is disclosing names of officers or employees who have a material interest in this procurement and is in a position to influence this procurement. Vendor must include a list of name(s), and relationship(s) with its submittal.

Public Entities Crimes Certification
In accordance with Public Entity Crimes, Section 287.133, Florida Statutes, a person or affiliate placed on the convicted vendor list following a conviction for a public entity crime may not submit on a contract: to provide any goods or services; for construction or repair of a public building or public work; for leases of real property to a public entity; and may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for Category Two for a period of 36 months following the date of being placed on the convicted vendor list.

The Vendor hereby certifies that: (check box)

☐ The Vendor certifies that no person or affiliates of the Vendor are currently on the convicted vendor list and/or has not been found to commit a public entity crime, as described in the statutes.

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

Scrutinized Companies List Certification
Pursuant to Section 287.135, Florida Statutes, any company or other entity on the **Scrutinized Companies with Activities in Sudan List**, the **Scrutinized Companies with Activities in Iran Terrorism Sectors List**, or the **Scrutinized Companies or Other Entities that Boycott Israel List**, are prohibited from bidding on, submitting a proposal for, or entering into or renewing a contract with an agency or local governmental entity for goods or services of (a) $100,000 or more if, at the time of bidding on, submitting a proposal for, or entering into or renewing such contract, the company or other entity is on the Scrutinized Companies or Other Entities that Boycott Israel List, created pursuant to Section 215.4725, Florida Statutes, or is engaged in a boycott of Israel; or (b) $1,000,000 or more if, at the time of bidding on, submitting a proposal for, or entering into or renewing such contract, the company or other entity is on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in Iran Terrorism Sectors List, created pursuant to Section 215.473, Florida Statutes; or is engaged in business operations in Cuba or Syria.

The Vendor hereby certifies that: (check each box)

- ☐ The company or other entity is aware of the above cited requirements of Sections 287.135215.473, and 215.4725, Florida Statutes, regarding the above cited lists; and
- ☐ The company or other entity is eligible to participate in this solicitation and are not listed on the cited lists above; and
- ☐ If awarded the Contract, the company or other entity will immediately notify the County in writing if it is placed on the above cited lists.

I hereby certify the information provided in this Vendor Questionnaire and Standard Certifications is true and correct*:

Vendor Name: Click or tap here to enter text.

Signature: _____

Printed Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

* I certify that I am authorized to sign this solicitation response on behalf of the Vendor as indicated in Certificate as to Corporate Principal, designation letter by Director/Corporate Officer, or other business authorization to bind on behalf of the Vendor. As the Vendor's authorized representative, I attest that any and all statements, oral, written or otherwise, made in support of the Vendor's response, are accurate, true and correct. I also acknowledge that inaccurate, untruthful, or incorrect statements made in support of the Vendor's response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to PART XI of the Broward County Procurement Code. I certify that the Vendor's response is made without prior understanding, agreement, or connection with any corporation, firm or person submitting a response for the same items/services, and is in all respects fair and without collusion or fraud. I also certify that the Vendor agrees to abide by all terms and conditions of this solicitation, acknowledge and accept all of the solicitation pages as well as any special instructions sheet(s).

Form Date 7/1/25

Next Generation 911 (NG 911) Demonstration Script

Version 0.4

05/30/25

Instructions

The purpose of this document is to provide the Next Generation 911 (NG911) Service Providers a standard set of items to demonstrate its proposed solution against the requirements that are outlined in the NG911 Scope of Work and Functionality Checklist document. Broward County (County) expects detailed information of the systems and applications that will be part of the proposed solution. The guidelines may include the use of test or lab systems and can be remote sessions into the lab or other devices.

Per NG911 Scope of Work and Functionality Checklist document, the County will be using VIPER 7 call-handling equipment (CHE) on the NG911 system.

The presentation guidelines consist of the following parts:

- **Description** – This is a high-level description of the demonstration process.
- **References** – This lists the functional or technical requirements related to this demonstration. These may not be all the requirements that apply but are included for reference.
- **Components** – This lists the expected components that should be included, at a minimum, in the explanations and demonstrations.

Presentations will be scheduled with a limited number of the short-listed vendors. The presentations will be focused on the vendors being able to present overview and the system architecture diagram of the solution presented in their proposal. During the presentation, the County will ask questions regarding the presentation and the proposals. Each vendor shall have staff that are very knowledgeable with the proposal provided to Broward County and the specific components of the proposed solution.

Each vendor will have a strict 2.5 hours time limit to complete each published guidelines and questions and answers with the following breakdown:

- **First 115 minutes** – Vendor led presentation of the components of their proposed solution for Broward County following this document. Each script has an individual time limit.
- **Last 35 Minutes** – County led questions based on both the presentation and the proposals provided.

The demonstration will be held onsite at a county facility. The County will provide access to the internet, a projector, and a screen for all demonstrations. If other resources are needed, the provider shall notify the County at least 10 business days in advance of its scheduled date.

Scripts

Script 1 – System Diagram (15 Minutes)

Description:

Present a functional Call Flow and System Diagram to represent the proposed solution. The Diagram shall depict the requirements outlined in the Scope of Work, Functionality Checklist, Project Questionnaire, and General Compliance documents.

References:

SD004	Design Specifications

Components:

The NG911 Service Provider shall present the following functions of their proposed solution:

- Call Flow
- OSP
- Alternate Routing
- PSAP and CHE Connectivity
- Data Center Connectivity
- Network to Network Interfaces
- Redundancy and Resiliency
- GIS Repository

Script 2 – PSAP[1] Dashboard (10 Minutes)

Description:

Demonstrate the use of the PSAP dashboard to include the security for access and role-based access.

References:

RPT001	Single Reporting Platform
RPT002	Reporting Platform PSAP Functions
RPT005	Real-Time System Monitoring

Components:

The NG911 Service Provider shall demonstrate the following functions of their proposed solution:

[1] Public safety answering point

- Log in (may require multiple accounts and log ins to show security controls and role-based access)
- Display the ability to be able to limit access to specific PSAPs for specific users
- Display and review all available reports
- Display and review live status display (if available)
- Display and review ad hoc report creation
- Display the ability to run reports for specific dates and times
- Display the ability to run reports for specific PSAPs
- Display the following elements:
    - Date and time stamp
    - Call delivery time
    - Call answer time
    - Call disconnect time
    - Call duration
    - Average call duration
    - Average call answer time
    - Seizure time
    - Call volumes by call type
    - Alternate-routed calls
    - Text-to-911 instances
    - Abandoned calls
    - Call volume by hour
    - Call volume by day of the week
    - Individual call information
    - Summary of call volumes
    - Call transfers/bridges
    - Call conferences
    - Agent availability
    - Call volumes by originating service provider (OSP)
    - Repeat callers
    - Routing method (e.g., geospatial, Federal Information Processing Standard [FIPS]/emergency service number [ESN], default, etc.)

Script 3 – Staff Dashboard (10 Minutes)

Description:

Demonstrate the use of the County staff dashboard to include the security for access and role-based access.

References:

RPT001	Single Reporting Platform
RPT003	Reporting Platform County Staff Functions
RPT004	Access to Logs via Reporting Platform
RPT005	Real-Time System Monitoring

Components:

The NG911 Service Provider shall demonstrate the following functions of their proposed solution:

- Log in (may require multiple accounts and log ins to show security controls and role-based access)
- Display the ability to limit access for specific users
- Display and review all available reports
- Display and review live status display (if available)
- Display and review ad hoc report creation
- Display the ability to run reports for specific dates and times
- Display the ability to run reports for specific PSAPs, sources, providers, etc.
- Display the following elements:
    - Call processing time between elements
    - Payload processing time
    - Calls per circuit
    - Call distribution to PSAP circuits
    - Circuit utilization from OSP
    - Circuit utilization to PSAP
    - All Next Generation Core Services (NGCS) element usage volumes (all elements used in the NG911 Service Provider's NG911 system)
    - End-to-end call-flow analysis
    - Event by incoming Internet Protocol (IP) address
    - Network Operations Center (NOC)-to-NOC reporting, trouble reporting, and tracking
    - Root cause analyses
    - Service availability for each component including Emergency Services IP network (ESInet) segments
    - Monitoring, alarming, and logging
    - Mean Opinion Score (MOS)

Script 4 – Spatial Interface/GIS[2] (10 Minutes)

Description:

Demonstrate the use of GIS dashboard, portal, or other tool.

References:

SR-GI009	SI[3] GIS Data Uploads
SR-GI010	SI and NGCS Provisioning
SR-GI012	Exception Codes
DAT001	GIS Upload

Components:

The NG911 Service Provider shall demonstrate the following functions of their proposed solution:

- Log in (may require multiple accounts and log ins to show security controls and role-based access)
- Demonstrate the steps of the proposed upload procedures
- Demonstrate all tools necessary including:
  - GIS data upload
  - GIS data validation
  - Publishing to the NGCS
- Demonstrate the process for applying a persistent exception code to non-critical errors so that the same are not included in discrepancy reports and do not adversely affect legacy data to GIS match rates
- Demonstrate the ability to pull data from other systems (if available)

[2] Geographic information system
[3] Spatial Interface

Script 5 – Notifications (5 Minutes)

Description:

Demonstrate the methods used to notify the client for routine and emergent communications.

References:

SN017	User Notifications and Communications
SR-DL014	Call Delivery Monitoring and Notifications

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- System that performs outward notifications and updates of customer tickets through phone, email, and text
- System that performs outward notifications and updates of system, component, and service outages through phone, email, and text
- System can notify of infrastructure failures and/or outages within 15 minutes of discovery

Script 6 – Logging (10 Minutes)

Description:

Demonstrate the logging capabilities and how the County can access or request activity logs.

References:

SN010	System Logging
SN011	System Logging Repositories
SN012	System Log Retrieval
SR-DL014	Call Delivery Monitoring and Notifications

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- Locations of various system logs including:
  - Call information from the entry point of the system (Points of Interconnection [POI], Border Control Function [BCF], etc.)
  - Call information from the routing components (Emergency Services Routing Proxy [ESRP], Emergency Call Routing Function [ECRF], and Policy Routing Function [PRF])
  - Call information from the exit point to the PSAP
- Logs that are accessible directly by the County
- Logs that require a request to get
- Procedure to request logs
- Format of the logs
- Time limit on accessing the logs
- Ability to have devices at the PSAP report to the County's security information and event management (SIEM) solution

Script 7 – Security (10 Minutes)

Description:

Demonstrate the process and systems that are used to provide security to the system against Telephony Denial of Service (TDOS) and Distributed Denial of Service (DDOS) attacks.

References:

SN008	Proactive Cybersecurity Analysis
SN009	STIR/SHAKEN
SN020	TDOS and DDOS Prevention

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- Systems used to monitor the system
- How STIR/SHAKEN is used in the system
- Systems used to identify TDOS and DDOS attacks
- Systems used to respond to attacks
- Initial and recuring training on these types of attacks given to your staff and subcontractors

Script 8 – Call Types (10 Minutes)

Description:

Demonstrate the look of the various call types on an example CHE screen. If the provider has access to a VIPER 7 system in its lab, the preference is for it to be used in CHE demonstrations; however, other CHE solutions may be used if a VIPER 7 system is not available.

References:

SR-IN007	Integrated Text-to-911
SR-IT003	Multimedia Sessions

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- A wireline call presenting on a CHE screen
- Answering a wireline call on the CHE and changes to the screen

Repeat for:

- Wireless
- Text
- Multimedia

Script 9 – Call Functions (10 Minutes)

Description:

Demonstrate the look of call functions on the CHE and NGCS.

References:

SR-NR006	Maintain Active Calls
SR-DL010	Call Back and Bridging
SR-DL011	Call Back and Transfer
SR-DL012	Bridging
SR-DL015	Call Queuing
SR-CR012	Overflow Notification

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- A call being delivered and the circuit with the voice call failing
- Ability to bridge multiple calls
- Ability to transfer a call
- Queueing of a call(s) for a PSAP
- Maximum number of parties to a bridge
- Number of calls able to be queued

Script 10 – Call Routing (15 Minutes)

Description:

Demonstrate the call routing that would be used to meet the advanced call routing that the County is expecting.

References:

DAT002	Alternate Routing Data
DAT003	Data for the PRF
DAT005	Routing and Configuration Data
SR-CR003	Rules, Policies, and Algorithms
SR-CR004	Distribution of Calls to PSAPs
SR-CR006	Call Routing Configurations
SR-CR008	Regional PSAP Routing
SR-CR009	Non-Regional PSAP Routing
SR-CR010	Emergency Call Routing
SR-CR011	Geofencing

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- Creation of rules, policies, algorithms, and configurations
- Ability to put in multiple levels of rules, policies, algorithms, and configurations
- Systems applications or dashboards the County will have access to for editing these rules, policies, algorithms, and configurations
- Systems applications or dashboards the provider will have access to for editing these rules, policies, algorithms, and configurations
- Number of rules, policies, algorithms, and configuration levels available
- Reasons for the access levels for the provider and County
- Process to gather the data, implement, and test these rules, policies, algorithms, and configurations

Script 11 – Alternate Call Routing (10 Minutes)

Description:

The County has advanced alternate routing in place today as described in the RFP. Demonstrate the alternate routing solutions.

References:

SR-AF001	Activation of Alternate and Failover Routing
SR-AF002	Regional Environment Failover
SR-AF003	Non-Regional Environment Failover
SR-AF005	Activation of Call Routing to Other NG911 Systems

Components:

The NG911 Service Provider shall explain the following functions of their proposed solution:

- How the current routing can be performed in the NG911 solution
- A Regional environment failover
- A Non-Regional environment failover
- How the routing features of VIPER 7 will be supported by the NG911 solution (demonstrate or explain)
- What is needed to failover to other NG911 systems in the area
- Passive and active solutions available for all routing types

BID BONDS, PERFORMANCE AND PAY NT BONDS, AND SURETY QUALIFICATION REQUIREMENTS

A. **Bid Bonds or Alternate Bid Security**:

1. A Vendor must submit with its response a bid bond in the form of the County's approved bi b nd f , incl ing all s bstan ve te s set f th the ein, which shall be executed by a surety company eeting the **Surety Qualifications equirements** stated bel w. Fail e t s b it a bi b nd by the s licita n's cl sing date and time and in accordance with the solicitation's instructions will deem the Vendor nonresponsive.

   Unless an diffe ent bi f m is incl ed in the s licita n, the applicable County-approved **Bid Bond Form** is located at: https://www.broward.org/Purchasing/Pages/StandardTerms.aspx under the section "Standard Guaranty and Bond Forms."

2. **Alternate Bid Security**: In lie o f a bi b n , the Ven m ay f nish alternate f s f security in the form of oney er, ce fied check, cashie 's check, o unc n i nal lette of c e it (**Bid Security - Unconditional Letter of Credit)** awn f m any na nal o state bank (United States). S ch alternate f s of sec ity shall be s bject to the app val of the Di ect of P chasing. A pe s nal check o a company check of a Vendor is not a valid bid security.

3. The bid bond alternate bid security shall be in an amount eq al t five pe cent (5%) f the t tal p ice ffered by the Vendor, payable t Broward County, and conditioned pon the successful Vendor providing the req i e pe f ance an pay ent b n s (app ved alte nate security), evidence f insurance, and any other requirements exp essly set forth within the solicita n as req i e u p n or bef e awa , within 10 calendar days after notification of award of the contract.

4. The bid bond alternate bid security f the successful Vendor shall be f feite t the C nty, n t as a penalty but as liquidated damages for the cost and expense incurred by the County, if said Vendor fails to ely p vi e the req i e pe f ance an pay ent b n s (approved alternate security) and evi ence of ins ance, or fails t c ply with any othe req i e ents exp essly set f th in the s licita n as equired upon before award f the contract. Upon equest, bid securities f unsuccessful Vendors will be returned after award of c ntract or expiration of bid validity.

5. Vendors must either:
   a. Obtain an elect nically iss ed bi b n using S ety2000 and attach a .p f c py of the Surety2000-issued electronic bid b nd to Vendor's solicitation esponse through the County's electronic bidding system; or
   . Submit an original bid b nd riginal alternate bid security to the Purchasing Division, by the solicitation's closing date and time.

   Fail e t s b it a bi b n or alte nate bid sec ity by the s licita n's cl sing date an ti e, an in accordance with the instructions herein, will render the Vendor nonresponsive to the solicitation.

. Instructions:
   a. To obtain an electronically issued bid bond, the Vendor must use **Surety2000**. Vendors, bonding agents, and surety companies ust egister with Surety2000 t se the se vice; c ntact **Surety2000** t fin o t inf a n ega ing thei se vice (www.surety2000.com or 800-660-3263).

      i. The Vendor must provide their bonding agent with the following:
      Obligee Name: Broward County
      Obligee Address: 115 S. Andrews Avenue, Room 212, Fort Lauderdale, Florida 33301

      ii. The Vendor's submittal ust include a copy f the electronically issued Surety2000 bid bond as a pdf attachment in the electronic bidding system.

      iii. Vendors st allow enough time to secure a bid bond and submit a copy to their submittal in case there are any errors or issues. Contact Surety2000 for additional assistance.

iv. The C nty will ve ify, th S ety2000, that an elect nically issued Surety2000 bid bond is valid.

v. An riginal bid bond will not be req i ed when a c py of an electronically issued Surety2000 bid bond is submitted through the electronic bidding system.

. To submit an original bid bond or original alternate bid security to the Purchasing Division, the Vendor st s bm it the iginal bid bond original alternate bid sec ity in a sealed envel pe, with the solicitation number, solicitation title, date and me f bid opening, and Vendor's address listed on the envelope. A copy of the bid bond or alternate bid security should also be ploaded into the County's electronic bidding system. The ploaded copy f the bid bond alternate bid security is in addition to, and does not replace, the original bid bond or original alternate bid security submission requirement. Vendors must submit the required documents, by the solicitation's closing date and time, to:

Broward County Purchasing Division
115 South Andrews Avenue, Room 212
Fort Lauderdale, FL 33301

. **rformance and Payment Bonds** :

1. Within 10 calen a days afte n ce by the C nty of the rec ended contract award, the successful Vendor ust furnish a completed Performance Bond and a c plete Payment Bond containing all the provisions of the Performance Bond Form and Payment Bond Form.

2. For **fixed contracts**, the bonds must be in the amount of one hundred percent (100%) of the total contract amount; if the total contract amount changes, the Vendor ust ens e that at all ti es the a nt of the bonds is n less than one hundred percent (100%) of the total contract amount inclusive f any change ers, amendments, or other changes.

   For **open-end contracts**, the bonds must be in the amount of 100% (if none stated, then 50%) of the total expecte c nt act a nt f the then-c ent ann al c nt act term as stated in the solicitation (if not state in the s licita n, then as stated in w i ng by the C nty in c nnec n with n ce of awa o enewal); and the Ven m st ens e that at all ti es the a nt of the b n s is n less than the t tal of (a) all open work orders, and (b) the total value of work perfo ed within the immediately preceding ne- year period. Within 10 calendar days after any event ccurrence that increases the equired b nd amount, the Vendor must furnish an additional bond or rider in compliance with the requirements of this section to meet the increased bond requirements.

3. The bonds must guarantee t the County the completion and perfor ance of the w k c ve ed in s ch c nt act as well as f ll pay ent of all s pplie s, lab e s, an subcontractors e ployed pursuant t the project. Each bond must be with a surety company that is qualified pursuant to the **Surety Qualifications quirements** stated below.

4. For construction contracts only: Pursuant t the requirements f Section 255.05(1), Florida Statutes, the successful Vendor must ensure that the performance and payment bonds are promptly ecorded in the Official Records of Broward County and must provide the County with evidence of such recording.

5. In lieu of the required performance and payment bonds, the successful Ven r may f rnish an alte nate form of security, which may be in the form of money order, certified check, cashier's check, or an original **Unconditional Letter of Credit** n the County's form. Such alternate f s of sec ity shall be subject to the approval of the Director of Purchasing, shall be for the same purpose as the bonds and subject to the same conditions as those stated above, and shall be held by the C nty f one year afte final c ple n and acceptance of the work.

. The successful Vendor is required at all times to have valid performance and payment bonds (or approved alternate security) in force covering the work being performed. The successful Vendor must keep such performance and payment bonds (or approved alternate security) in effect f the d a n of the contract, and until ne year after final completion and acceptance f the w k at iss e. If the c nt act is extended enewed, it shall be subject to the same bonding (o approved alternate security) requirements.

. **Surety Qualification Requirements:**

BID BONDS, PERFO ANCE AND P AY NT BONDS, AND SURETY QUALIFICATION REQUIREMENTS

1. For all Bid Bonds, Performance Bonds, and Payment Bonds over $500,000:

   a. Each bond must be executed by a surety company of recognized standing, authorized to do business in the State of Fl i a as s ety, having a resi ent agent in the State of Florida, and having been in business with a record of successful continuous operation for at least the past five years.

   . The surety company shall hold a current Certificate of Authority as acceptable surety on federal bonds in acc ance with the Unite States Depa t ent of T eas y Ci cular 570, current evision. If the amount of the bond exceeds the underwriting limitation set forth in the circular, the net retention of the surety company ust not exceed the nderwriting limitation in the ci c lar and the excess risks must be protected by coinsurance, reinsurance, ther methods in accordance with Treasury Circular 297, Revised (31 CFR Sections 223.10 and 223.11). Further, the surety company must provide the County with evidence satisfactory t the County that such excess risk has been p tecte in an acceptable manner.

   A surety company that is ejected by the County may be substitute by the Ven r with a s ety company acceptable to the County, but only if the bid or contract amount does not increase.

   . All bonds shall be written through surety insurers authorized to do business in the State of Florida as s ety, with the f ll wing q alifica ns acc ing t the latest edition of Best's Insurance Guide, published by AM Best Company, Oldwick, New Jersey:

Amount of Bond	Minimum Policy Holder's Ratings Strength/Financial Size
$500,001 to $1,500,000	A / III
$1,500,001 to $2,500,000	A / VI
$2,500,001 to $5,000,000	A / VII
$5,000,001 to $10,000,000	A / VIII
Over $10,000,000	A / IX

2. For projects that do not exceed $500,000:

   a. The County shall accept bid bonds, performance bonds, and payment bonds f a surety company that has at least twice the inimum surplus and capital equire d by the Fl i a Office of Ins ance Reg la n at the ti e the s licita n is iss e , p vi e that the s ety c pany is othe wise in compliance with the provisions f the Florida Insurance Code an the surety company holds a currently valid Certificate of Authority issued by the United States Department of the Treasury under Section 9304 to 9308 of Title 31 of the United States Code.

   . A completed Certificate and Affidavit for Bonds $500,000 Less (F 007500-4, available at https://www.broward.org/Purchasing/Pages/StandardTerms.aspx) st also be s b itted with the applicable bid bond, performance bond, or payment bond.

3. If the surety company fails to eet the minimum standards, a bond from a surety that meets the mini standards must be timely provided to satisfy the bonding requirements.

Form Date 5/14/25

INSTRUCTIONS TO VENDORS
REQUEST FOR PROPOSAL, REQUEST FOR QUALIFICATION, OR REQUEST FOR LETTER OF INTEREST

Next Generation 911 (NG911)

Vendor is instructed to read and follow the instructions carefully, as any misinterpretation or failure to comply with instructions may lead to Vendor's submittal being rejected or may affect Vendor's evaluation.

Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in the electronic bidding system for the response to be deemed valid by the County. Refer to Submittal Instructions.

A. Responsiveness Criteria:

A responsive Vendor means a vendor who submits a response to a solicitation that the Director of Purchasing determines meets all solicitation requirements.

Information and applicable forms, are requested to be submitted by the solicitation's closing date and time, as instructed. Failure to timely submit may result in the Vendor being deemed nonresponsive per instructions.

The County reserves the right to waive minor technicalities or irregularities as is in the best interest of the County in accordance with Section 21.37(b) of the Broward County Procurement Code.

1. **Bond Requirement**
   A bid bond is required for this solicitation. Vendor must follow the instructions in **Bid Bonds, Performance and Payment Bonds, and Surety Qualification Requirements** and submit a bid bond in the form of the County's approved bid bond form, or Alternate Bid Security, per instructions. Failure to submit with a bid bond (or alternate security) by the solicitation's closing date and time, shall determine the Vendor to be nonresponsive to Bond Requirements.

2. **Criminal History Screening Practices Requirement**
   Broward County's Criminal History Screening Practices Ordinance applies to this solicitation. Vendor must follow the instructions and submit the completed **Criminal History Screening Practices Certification.** If not provided with the submittal, the Vendor must submit within three business days after the County's written request. Failure to submit within the stated timeframe may determine the Vendor to be nonresponsive to the Criminal History Screening Practices requirement.

3. **Domestic Partnership Act Requirement**
   Broward County's Domestic Partnership Act applies to this solicitation (as a requirement and a tiebreaker criteria). Vendor must follow the instructions and submit the completed **Domestic Partnership Act Certification**. If not provided with the submittal, the Vendor must submit within three business days after the County's written request. Failure to submit within the stated timeframe may determine the Vendor to be nonresponsive to the Domestic Partnership Act requirement. However, to be eligible for the Domestic Partnership tiebreaker, the Vendor must currently offer the Domestic Partnership benefit and the completed form must be returned at the time of solicitation submittal. Vendors who fail to comply with this submittal deadline will not be eligible for the Domestic Partnership tiebreaker.

4. **Federal Transit Administration (FTA) Requirements**
   Not applicable to this solicitation.

5. **Living Wage Requirements**
   Not applicable to this solicitation.

6. **Lobbyist Registration Requirement**
Broward County's Lobbyist Registration Act applies to this solicitation. Vendor must follow the instructions and submit the completed **Lobbyist Registration Requirement Certification**. If not provided with the submittal, the Vendor must submit within three business days after the County's written request. Failure to submit within the stated timeframe may determine the Vendor to be nonresponsive to the Lobbyist Registration requirement.

7. **Pricing Requirements and Submittal**
   a. Vendor is requested to submit pricing via electronic bidding system. It is solely the Vendor's responsibility to ensure pricing is submitted and received electronically through electronic bidding system by the solicitation's closing date and time. The County will not consider pricing received by other means.

   b. Pricing submittal is a matter of responsiveness. Failure to complete and electronically submit pricing per solicitation's instructions by the solicitation's end closing date and time shall determine the Vendor to be nonresponsive to the Pricing Requirements.

   c. Proposed pricing remains subject to negotiation, which may result in a reduction from the Vendor's proposed pricing. If scoring is applicable to the solicitation, scoring for price is set forth in the Evaluation Criteria, including the formula for calculation of pricing points.

8. **Additional Responsiveness Requirement**
   A. Mandatory Site Visits (Days 1 and 2)

      i. Broward County's Office of Regional Communications and Technology Division requires all participants of the mandatory sites visit to bring one of the following forms of valid government issued identification: 1) Passport; 2) State Driver's License; or 3) State Issued Identification and employee badge of company being represented.

      ii. Attendance at the site visits (for each day and location) is MANDATORY.

      iii. Failure to attend mandatory site visit (for each day and location) will deem Vendor non-responsive.

      iv. Once the site visit begins (any location), no one will be permitted to leave until the site visit is complete (for each day).

      v. This is a walking site visit; comfortable shoes are highly recommended.

      vi. No food or drinks are allowed in the Public Safey Answering Points.

      vii. If you require any auxiliary aids for communication, please call (954) 357-6066 so that arrangements can be made in advance.

B. Responsibility Criteria:
A responsible vendor means a vendor who is determined to have the capability in all respects to fully perform fully the requirements of a solicitation, as well as the integrity and reliability that will ensure good faith performance.

The Director of Purchasing or the Evaluation Committee (as applicable) may request additional information from any Vendor on matters that may affect a Vendor's responsibility. A Vendor may submit additional information regarding its responsibility, but such information will not be considered if it contradicts or materially alters the information provided in the original solicitation response.

A Vendor's failure to provide information requested in the manner required may result in a recommendation by the Director of Purchasing to, and/or a determination by an Evaluation Committee that the Vendor is nonresponsible.

1. **Affiliated Entities of the Principal(s)**
   a. Vendor is required to disclose the names of "affiliated entities" of the Vendor's principal(s) over the last five (5) years (from the solicitation's closing deadline) that have acted as a prime Vendor with the County. The Vendor is required to provide all information required on the **Affiliated Entities of the Principal(s) Certification**. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

   b. The County will review all affiliated entities of the Vendor's principal(s) for contract performance evaluations and the compliance history with the County's Small Business Program, including County Business Enterprise (CBE), and Disadvantaged Business Enterprise (DBE), goal attainment requirements in its review and determination of responsibility. "Affiliated entities" of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent, or sibling entity.

2. **Enterprise Technology Services (ETS) Vendor Security Questionnaire (VSQ)**
   ETS Vendor Security Questionnaire (VSQ): Vendor is required to submit a completed **ETS Vendor Security Questionnaire (VSQ)** (for applicable solution – services, hardware, and/or software). If a response requires additional information, attach additional pages with the required additional information with the additional pages and information labeled to match the applicable question number. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

   The Vendor Security Questionnaire (VSQ) assesses the Vendor's security policies and/or system protocol and to identify any potential security vulnerabilities. The County will review the Vendor's VSQ response; any identified security concerns will be disclosed to the Evaluation Committee. Unresolved security concerns shall be considered by the Evaluation Committee as part of its final evaluation and may affect the Vendor's evaluation.

3. **Financial Information/Financial Ability**
   a. Vendor is required to submit the Vendor's financial statements by the solicitation's closing date and time, to demonstrate the Vendor's financial capabilities. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

   b. Vendor shall submit its most recent two years of financial statements for review. The financial statements are not required to be audited financial statements. The annual financial statements shall be in the form of:

      i. Balance sheets, income statements and annual reports; or

ii. Tax returns; or
iii. SEC filings.

If tax returns are submitted, ensure the documents do not include any personal information (as defined under Section 501.171, Florida Statutes), such as social security numbers, bank account or credit card numbers, or personal pin numbers. If any personal information is part of financial statements, redact information prior to submitting to the County.

c. If a Vendor has been in business for less than the number of years of required financial statements, then the Vendor must disclose financial statements for all years that the Vendor has been in business, including any partial year-to-date financial statements.

d. The County may consider the unavailability of the most recent year's financial statements and whether the Vendor acted in good faith in disclosing the financial documents in its evaluation.

e. Any claim of confidentiality on financial statements must be asserted at the time of submittal. Refer to Confidential Material/Public Records and Exemptions for instructions on submitting confidential financial statements. The Vendor's failure to provide the information as instructed may lead to the information becoming public.

4. **Foreign Country of Concern Requirements**
Foreign Country of Concern requirement applies to this solicitation, as resultant contract may give access to an individual's personal identifying information. Vendor submit completed **Foreign Country of Concern Attestation** as instructed. If not provided with the submittal, the Vendor must submit within three business days after County's written request.

5. **Insurance Requirements**
The **Minimum Insurance Requirement Form** reflects the insurance requirements deemed necessary for this project. Vendor is required to either submit insurance certificates indicating that the Vendor currently carries the level insurance coverages OR submit a letter from the insurance carrier indicating the Vendor can obtain the required insurance coverages if awarded this contract. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

6. **License, Pre-Qualification, or Certification Requirements**
   a. **License Requirement**:
   Not applicable to this solicitation.

   b. **FDOT Pre-Qualification:**
   Not applicable to this solicitation.

   c. **Certification Requirement:**
   Not applicable to this solicitation.

7. **Litigation History**
Vendor should submit **Litigation History** with its submittal. If not provided with submittal, the Vendor must submit form(s) and requested information within three (3) business days after County's request.

8. **Office of Economic and Small Business Development Program Requirements**
   Not applicable to this solicitation.

9. **Workforce Investment Program Requirements**
   Not applicable to this solicitation.

10. **Additional Responsibility Requirement**
    Project Questionnaire: Vendor is required to submit a completed **Project Questionnaire.** If a response requires additional information, attach additional pages with the required additional information with the additional pages and information labeled to match the applicable question number. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

    The Project Questionnaire assesses the Vendor's compliance to the Scope of Work. The County will review the Vendor's response; any identified concerns will be disclosed to the Evaluation Committee. Unresolved concerns shall be considered by the Evaluation Committee as part of its final evaluation and may lead to a Vendor being deemed nonresponsible or otherwise affect the Vendor's evaluation.

C. Additional Information and Certifications

The following forms and supporting information (if applicable) should be completed and provided with the solicitation response. If not provided with the submittal, the Vendor must submit within three business days after the County's written request. Failure to timely submit requested information and/or to certify to requirement may affect the Vendor's evaluation.

1. **Vendor Questionnaire and Standard Certifications**
   Refer to the **Vendor Questionnaire and Standard Certifications** and submit as instructed.
   a. Drug-Free Workplace Certification
   b. Non-Collusion Certification
   c. Public Entities Crimes Certification
   d. Scrutinized Companies List Certification

2. **Procurement Preference for SBE and CBE**
   Not applicable to this solicitation.

3. **General Compliance, Next Generation 911 (NG911)**
   Refer to the **General Compliance, Next Generation 911** and submit as instructed.

D. Standard Agreement Language Requirements

1. The solicitation's contract terms and conditions are:

   Standard Technology Agreement (BCF 301 7/1/24)

   Vendor is also required to review the following additional terms and conditions:

   a. Enterprise Technology Services Security Requirements Exhibit - HIGH Risk (10/17/23)

   b. Standard Service Level Agreement Form (10/17/23)

2. Vendor is required to review the terms and conditions and submit the **Agreement Exceptions**. The

completed form should be provided with the solicitation response. If not provided with solicitation response, it shall be deemed an affirmation by the Vendor that it accepts all the referenced contract terms and conditions and any additional terms listed above.

3. If exceptions are taken, the Vendor must specifically identify each term and condition to which it is taking an exception. Any exception not specifically listed is deemed waived. Simply identifying a section or article number is not sufficient to state an exception. The Vendor must provide either a redlined version of the specific change(s) or specific proposed alternative language. Additionally, a brief justification specifically addressing each provision to which an exception is taken must be provided.

4. The acceptance of or any exceptions taken to the terms and conditions of the County's agreement language is considered a part of the Vendor's response and will be considered by the Evaluation Committee. Submission of exceptions by the Vendor does not constitute acceptance of those exceptions by the County. Furthermore, taking exceptions to the County's terms and conditions may be viewed unfavorably by the Evaluation Committee and ultimately may impact the overall evaluation of a Vendor's submittal.

E. Procurement Authority

Pursuant to Section 21.33 of the Procurement Code, RFPs, RLIs, and RFQs with an anticipated total value of more than $500,000 require Board approval.

F. Project Funding Source

This project is funded in whole or in part by:
State Funds: Department of Management Services/ E911 State Fund

G. Cone of Silence

1. The County's Cone of Silence Ordinance, Section 1-266, of the Broward County Code of Ordinances, prohibits all communications, oral or written, relating to a competitive solicitation among vendors/vendor representatives, County Staff, and Commissioner Offices while the Cone is in effect.

2. Only communications with Purchasing Division employees, the solicitation's designated Project Manager(s) or designee(s), the Office of Economic and Small Business Development (OESBD) Small Business Development Specialist Supervisor (954) 357-6400, and others as specifically identified in the Cone of Silence Ordinance are permitted. Additionally, communication is permitted at pre-bid conferences and negotiation meetings, as applicable.

3. The Cone of Silence begins upon the advertisement of an ITB, RFP, RFQ, or RLI. The Cone of Silence terminates when the solicitation is awarded, all responses are rejected, or the Board takes other action which ends the solicitation, as more fully stated in the Cone of Silence.

4. Any violations of the Code of Silence Ordinance by any vendor or vendor representative may be reported to the County's Professional Standards. If the County's Professional Standards determines that a violation has occurred, a fine shall be imposed as provided in the Broward County Code of Ordinances. At the sole discretion of the Broward County Board of County Commissioners, a violation may void an award of the applicable competitive solicitation.

5. Review the Cone of Silence Ordinance, Section 1-266 of the Broward County Code of Ordinances, for more detailed information.

H. Vendor Questions

The County provides a specified time for Vendors to ask questions and seek clarification regarding the solicitation requirements. All questions or clarification inquiries must be submitted through BPRO by the Question due date. The County will respond to questions in BPRO (Messages section).

I. Addendum

The County reserves the right to amend this solicitation prior to the deadline for Vendor responses by issuing written addenda to the solicitation. If, upon review, a Vendor finds a nonclerical error in an addendum, that Vendor must contact the Purchasing Division immediately, prior to the deadline for submission of responses, to allow the County to review the alleged error and to issue any clarification, if the County determines that a clarification is necessary. Vendors are responsible for obtaining and reviewing each addendum prior to the deadline for submission of responses to the solicitation. The terms of all addenda are incorporated into the solicitation.

J. Committee Appointment and Project Manager

1. **Committee Members Information:**
   An Evaluation Committee is responsible for recommending the most qualified Vendor(s). The solicitation's appointed committee members are listed on the Purchasing Division's website under Committee Appointment. Committee Members are covered by the Cone of Silence.

2. **Project Manager Information:**
   Project Manager: Mohammad Ahmadpour, Information Systems Manager

K. Evaluation Criteria

1. The Evaluation Committee will evaluate Vendors as per the **Evaluation Criteria**. The County reserves the right to obtain additional information from a Vendor.

2. Unless the Evaluation Criteria is identified as a solicitation Responsiveness or Responsibility Requirement (i.e., pricing, certifications, etc.), a Vendor's failure to respond to Evaluation Criteria will not be considered a matter of responsiveness or responsibility. Vendors that fail to submit information and/or documentation required by an evaluation criterion by solicitation's closing date and time may receive no points (if applicable) for the corresponding Evaluation Criteria. The County is not required to request, consider, or analyze the Vendor's Evaluation Criteria responses received after the solicitation's closing date.

3. The County reserves the right to obtain clarifying information from a Vendor in writing for the Evaluation Committee.

4. For Request for Proposals - the following shall apply:
   a. The Evaluation Committee may shortlist the most qualified firms prior to the Final Evaluation, in accordance with the Procurement Code.
   b. The Evaluation Criteria identifies points available; a total of 100 points is available.
   c. If the solicitation includes a request for a pricing submittal, the formula for awarding points will be identified in the Evaluation Criteria.
   d. After completion of scoring, the County may negotiate pricing as in its best interest.

5. For Requests for Letters of Interest or Request for Qualifications - the following shall apply:
   a. The Evaluation Committee will create a shortlist of the most qualified firms.

b. The Evaluation Committee will either:
   i. Rank shortlisted firms; or
   ii. If the solicitation is part of a two-step procurement, shortlisted firms will be requested to submit a response to the Step Two procurement.

L. Review and Evaluation of Responses

The process for this procurement may proceed in the following manner:

1. Agency staff prepares a report, including a matrix of responses submitted by the Vendors. This may include a technical review, if applicable.

2. A solicitation may only be awarded to a Vendor determined responsive and responsible to the solicitation's requirements. The Director of Purchasing shall determine whether submissions are responsive. The Director of Purchasing's responsiveness determination is not binding on the Evaluation Committee; the Evaluation Committee may accept or reject the Director of Purchasing's responsiveness determination but must specifically state the basis for any rejection.

3. When making determinations of responsibility, the Director of Purchasing or the Evaluation Committee (as applicable) may request additional information from any Vendor on matters that may affect a Vendor's responsibility. The failure of a Vendor to provide information requested by the County may result in a determination of nonresponsibility. In addition, a Vendor may submit information regarding its responsibility; however, information shall not be considered if it contradicts or materially alters the information provided by the Vendor in its original response to the solicitation.

4. The Evaluation Committee, with assistance of the Purchasing Division and based on information provided by the applicable County Agencies and the Office of the County Attorney, shall determine whether Vendors who have submitted responsive submissions are responsible. The solicitation's awarding authority shall have the ultimate authority to determine whether Vendors who have submitted responsive submissions are responsible.

M. Local Preference

Broward County's local preference provisions shall apply except where otherwise prohibited by federal or state law or other funding source restrictions.

Refer to Section 1-75 of the Broward County Local Preference Ordinance and the **Location Certification Form** for further information.

For RFPs: upon the completion of final rankings (technical and price combined, if applicable) by the Evaluation Committee, if a nonlocal Vendor is the highest ranked Vendor and one or more Local Businesses (as defined by Section 1-74 of the Broward County Code of Ordinances) are within five percent (5%) of the total points obtained by the nonlocal Vendor, the highest ranked Local Business shall be deemed to be the highest ranked Vendor overall, and the County shall proceed to negotiations with that Vendor. If impasse is reached, the County shall next proceed to negotiations with the next highest ranked Local Business that was within five percent (5%) of the total points obtained by the nonlocal Vendor, if any.

The **Location Certification Form** will be used for local preference and location tiebreaker criteria.

N. Demonstrations

1. Vendors determined to be both responsive and responsible to the solicitation's requirements and shortlisted (if applicable), are required to demonstrate its offered solution for compliance to the **Demonstration Script**, which is subject to change by the County prior to Demonstrations.

2. All Vendors will have equal time for demonstrations. Subconsultants/subcontractors may only participate during one demonstration session, if partnering with multiple Prive Vendors.

3. A designated Technical Review Team ("TRT") will view all Vendor demonstrations. The TRT will review all Vendor demonstrations for compliance to the **Demonstration Script**. The Project Manager will provide a final TRT report to the Evaluation Committee members prior to the Final Evaluation Committee meeting.

4. In accordance with Section 286.0113, Florida Statutes, and pursuant to the direction of the Broward County Board of Commissioners, Demonstration Meetings are closed. Only the Vendor's team, County staff, and County's representative (if applicable) may attend.

O. Presentations

1. Vendors that are determined to be both responsive and responsible to the solicitation's requirements and shortlisted (if applicable) may make a presentation to the Evaluation Committee on the Vendor's submittal. The committee may provide a list of presentation topics. Each Vendor will have equal time to present; question-and-answer time may vary by Vendor.

2. In accordance with Section 286.0113, Florida Statutes, and the direction of the Broward County Board of Commissioners, presentations during Evaluation Committee meetings are closed. Only the Evaluation Committee members, County staff (and County's representative, if applicable), and the Vendor and their team scheduled for that presentation will be present in the meeting during the presentation and subsequent question and answer period. Subconsultants/subcontractors may only participate during one presentation/question and answer session, if partnering with multiple prime vendors.

P. Evaluation Committee Meetings, Committee Questions, Request for Clarifications, Additional Information

1. Evaluation Committee Meetings dates, times and locations are posted on Broward County's Sunshine Meetings website.

2. At any committee meeting, the Evaluation Committee members may ask questions, request clarification, or require additional information of any Vendor's submittal or proposal. It is highly recommended Vendors attend to answer any committee questions (if requested), including a Vendor representative that has the authority to bind the Vendor. Vendor's answers may impact evaluation (and scoring, if applicable).

Q. Confidential Material; Public Records and Exemptions

1. Broward County is a public agency subject to Chapter 119, Florida Statutes. Upon receipt, all submittals become "public records" and are subject to public disclosure consistent with Chapter 119, Florida Statutes. Submittals may be posted on the County's public website or provided by the County in a public records request response, except to the extent records are identified by the Vendor as confidential and/or exempt pursuant to the public records law and in accordance with the procedures in this section.

2. Any material(s) that the Vendor asserts are confidential and/or exempt from public disclosure under Florida Statutes must be conspicuously labeled at the time of submittal as "Confidential" and marked with the specific Florida statute and subsection permitting that exemption under Florida public records law.

3. To submit material as confidential and/or exempt, the Vendor must submit to "Broward County Purchasing Division, 115 South Andrews Avenue, Room 212, Fort Lauderdale, Florida 33301," in a sealed envelope labeled with the solicitation number and title, name and contact information for the Vendor, itemization of the contents, identification of the Florida statute(s) and subsection(s) permitting the applicable exemption(s), and the solicitation's closing date and time, the following:

    a. Three (3) hard copies of the materials, unredacted, with each page containing material that is confidential and/or exempt conspicuously labeled "Confidential"; and

    b. One (1) copy of the same materials, titled "Redacted Copy," redacted to remove/redact only those portions of the materials that are confidential and/or exempt under Florida law.

4. If the Vendor does not submit the materials in strict accordance with this section, then the Vendor may be deemed to have waived any claim that the materials are confidential and/or exempt and the County is deemed authorized to post the entire submittal on the County's public website and/or produce the entire submittal in response to a public records request for the materials.

5. By submitting materials marked as confidential and/or exempt, Vendor agrees to indemnify County and its employees and agents from any and all claims, fines, penalties, damages, judgments, and liabilities of any kind, including attorneys' fees and costs, relating to the County's nondisclosure of those materials in response to a public records request by a third party. The Vendor shall be responsible for defending its determination that the redacted portions are not subject to disclosure under applicable law.

6. Submitting material as confidential and/or exempt may impact discussion and consideration of the Vendor's submittal by the Evaluation Committee because the Evaluation Committee may be unable to fully discuss the confidential and/or exempt material at the public evaluation meeting.

R. Copyrighted Materials

Submittal of copyrighted material will constitute a license and permission for the County to use, reproduce, distribute, and publish (including both hard copy and electronic copies) as reasonably necessary for the evaluation of the solicitation response by County staff and agents, as well as to make the materials available for inspection or production pursuant to Public Records Law, Chapter 119, Florida Statutes.

S. Public Art and Design Program

Not applicable to this solicitation.

T. Tiebreaker Criteria

In accordance with Section 21.42(d) of the Broward County Procurement Code, the tiebreaker criteria shall be applied based upon the information provided in the Vendor's solicitation response at time of submittal. Complete and accurate information must be contained in the Vendor's initial submittal to ensure credit is received for any tiebreaker criterion. Except to the extent precluded by applicable funding or legal requirements, tiebreaker criteria are as follows:

1. Location Certification;
2. Domestic Partnership Act Certification;
3. Drug-Free Workplace Certification;
4. Volume of Previous Payments Attestation;

5. If the foregoing does not resolve the tie, the Evaluation Committee shall reconsider the responses and re-rank the tied vendors;
6. If the foregoing does not resolve the tie, the Vendor receiving the most first place votes from the Evaluation Committee's reranking.

U. Posting of Solicitation Results and Recommendations

The Broward County Purchasing Division's website is the location for the County's posting of all solicitations and recommendation for award and recommendation of rankings. It is the obligation of each Vendor to monitor the website in order to obtain complete and timely information.

V. Vendor Protest

Part X of the Broward County Procurement Code sets forth procedural requirements that apply if a Vendor intends to protest a solicitation or proposed award of a contract and states in part the following:

1. Any written protest concerning the specifications or requirements of a solicitation (or of any addenda thereto) must be received by the Director of Purchasing within five (5) business days after the applicable solicitation (or addenda) is posted on the Purchasing Division's website.

2. Any written protest concerning a proposed award or ranking must be received by the Director of Purchasing within five (5) business days after the proposed award or ranking is posted on the Purchasing Division's website.

3. Failure to file a written protest so that it is received by the Director of Purchasing within the timeframes set forth in Part X of the Broward County Procurement Code shall constitute a waiver of the right to protest. A protest submitted to anyone other than the Director of Purchasing shall not be a valid protest.

4. Except as to any protest of the specifications or requirements of a solicitation, as a condition of initiating any protest, the protestor must, concurrently with filing the protest, pay a filing fee for the purpose of defraying the costs in administering the protest in accordance with the scheduled provided below. The filing fee shall be refunded if the protestor prevails in the protest. Failure to timely pay the required filing fee shall render the protest invalid.

Estimated Contract Amount	Filing Fee
Mandatory Bid Amount up to $250,000	$500
$250,000 - $500,00	$1,000
$500,001 - $5 million	$3,000
Over $5 million	$5,000

The estimated contract amount shall be the total bid (proposal) amount offered by the protesting Vendor in its response to the solicitation, inclusive of any contract renewals or extensions. If no amount was submitted by the protestor, the estimated contract amount shall be the County's estimated procurement contract price. The County will accept a filing fee in the form of a money order, certified check, or cashier's check, payable to "Broward County," or other manner of payment approved by the Director of Purchasing.

W. Right To Appeal

The protestor may appeal the Director of Purchasing's denial of the protest with respect to the proposed award of a solicitation in accordance with Part XII of the Broward County Procurement Code. Decisions by the

Director of Purchasing with respect to the specifications or requirements of a solicitation may only be appealed to the County Administrator or their designee, who shall determine the method, timing, and process of the appeal and whose decision shall be final.

1. The appeal must be received by the Director of Purchasing within ten (10) days after the date of the determination being appealed.

2. The appeal must be accompanied by an appeal bond by a Vendor having standing to protest and must comply with all other requirements of Part XII of the Broward County Procurement Code. The appeal bond is based on the estimated contract amount, per Section 21.84 of the Procurement Code.

3. Except as otherwise provided by law, the filing of an appeal is an administrative remedy that must be exhausted prior to the filing of any civil action against the County concerning any subject matter that, had an appeal been filed, could have been addressed as part of the appeal.

X. Rejection of Responses

The Director of Purchasing may reject all responses to a solicitation, even when only one response is received, if the Director of Purchasing determines that doing so would be in the best interest of the County; provided, however, that only the Board may reject all responses to a solicitation where the issuance of the solicitation was approved by the Board.

Y. Negotiations

Once a ranking is deemed final, the County shall commence contract negotiations with the top-ranked Vendor (or, if provided in the solicitation, with multiple top-ranked Vendors simultaneously). If the negotiation does not result in mutually satisfactory contract terms within a reasonable time, as determined by the Director of Purchasing, then the Director of Purchasing may terminate negotiations with the applicable Vendor and commence (or continue, if the solicitation provided for negotiation with multiple top-ranked Vendors) negotiations with the next-ranked Vendor(s) or issue a new solicitation, as the Director of Purchasing determines to be in the best interest of the County.

Z. Submittal Instructions

1. Vendor MUST submit its solicitation response electronically through BPRO and receive a Submission Receipt. It is solely the Vendor's responsibility to ensure its response is submitted and received through BPRO by the closing date and time. The County will not consider solicitation responses received by other means. Vendors are encouraged to submit in advance of the closing date and time. Refer to the Purchasing Division website or contact support@gobonfire.com for submittal instructions. In the event that the Vendor is having difficulty submitting a document, immediately notify the Purchasing Agent and then contact support@gobonfire.com for technical assistance.

2. Vendor must view and download each of the documents in the electronic bidding system.

3. After all documents are viewed and downloaded from the electronic bidding system, the Vendor must upload additional information requested by the solicitation (i.e. Evaluation Criteria, certifications, etc.) in the Provide Submission Information section in the electronic bidding system, Evaluation Criteria responses should be non-locked file format.

4. If a Vendor is declaring any material confidential and exempt from Public Records, refer to Confidential Material; Public Records and Exemptions section for submittal instructions.

5. After all files are uploaded, Vendor must submit and finalize submission for offer to be received electronically through the electronic bidding system.

6. If a solicitation includes a Bond Requirement (Responsiveness Criteria), the Vendor must submit in a sealed envelope, labeled with the solicitation number, title, by the solicitation's closing date and time, to:

   Broward County Purchasing Division
   115 South Andrews Avenue, Room 212
   Fort Lauderdale, FL 33301

   A copy of the bond should also be uploaded into the electronic bidding system; this does not replace the requirement to submit an original bond by the solicitation's closing date and time.

7. Broward County does not require any personal information (as defined under Section 501.171, Florida Statutes), such as social security numbers, driver license numbers, passport, military ID, bank account or credit card numbers, or any personal pin numbers, in order to submit a response for ANY Broward County solicitation. DO NOT INCLUDE any personal information data in any document submitted to the County. If any personal information data is part of a submittal, this information must be redacted prior to submission to the County.

Form Date 7/1/25

Sign-In Sheet for Optional Pre-Proposal - Day 1
Central Public Safety Answering Point
Thursday, July 24, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/24/25 9:16:28	Holly Peacock	INdigital	334-796-3686	hpeacock@indigital.net	No	Prime Contractor;
7/24/25 9:16:39	Brent Savill	INdigital	5749521547	Bsavill@indigital.net	No	Prime Contractor;
7/24/25 9:16:42	William Bassett	INdigital	260-403-8009	Bbassett@indigital.net	No	Prime Contractor;
7/24/25 9:18:56	Lisa Madden	Motorola Solutions Connectivity Inc	207-468-5461	Lisa.madden@motorolasolutions.com	No	Prime Contractor;
7/24/25 9:22:04	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasolutions.com	No	Prime Contractor;
7/24/25 9:24:01	Charles Ronshagen	Motorola Solutions Connectivity Inc.	951-378-3175	Chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/24/25 9:32:08	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/24/25 9:33:40	Mario Ruiz	AT&T	9548062467	mr2673@att.com	No	Prime Contractor;
7/24/25 9:37:40	RIchard Johnston	Intrado - In Support of AT&T	303-888-5194	rjohnston@intrado.com	No	Subcontractor/Subconsultant;
7/24/25 9:41:10	Shawn P Harris	AT&T Public Safety	9189783535	Shawn.P.Harris@att.com	No	Prime Contractor;
7/24/25 9:54:28	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/24/25 10:00:13	Jenine Jasso	AT&T	346-373-6062	jj788y@att.com	No	Prime Contractor;

Sign-In Sheet for Mandatory Site Visit - Day 1
Central Public Safety Answering Point
Thursday, July 24, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/24/25 10:36:26	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/24/25 10:36:45	Holly Peacock	INdigital	3347963686	hpeacock@indigital.net	No	Prime Contractor;
7/24/25 10:36:54	Brent Savill	INdigital	5749521547	Bsavill@indigital.net	No	Prime Contractor;
7/24/25 10:36:56	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasolutions.com	No	Prime Contractor;
7/24/25 10:37:07	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/24/25 10:37:08	Mario Ruiz	AT&T	954-806-2467	mr2673@att.com	No	Prime Contractor;
7/24/25 10:37:30	Gordon Vanauken	MCP	8145741186	GordonVanauken@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/24/25 10:37:57	William Bassett	INdifital	260-403-8009	Bbassett@indigital.net	No	Prime Contractor;
7/24/25 10:38:14	Charles Ronshagen	Motorola Solutions Connectivity inc.	9513783175	Chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/24/25 10:39:03	Robert Horne	MCP	2403578296	RobertHorne@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;

Sign-In Sheet for Mandatory Site Visit - Day 1
North Public Safety Answering Point
Thursday, July 24, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/24/25 13:27:52	Brent Savill	INdigital	5749521547	Bsavill@indigital.net	No	Prime Contractor;
7/24/25 13:27:53	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/24/25 13:27:58	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/24/25 13:27:58	Charles Ronshagen	Motorola Solutions Connectivity inc.	9513783175	chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/24/25 13:27:58	Charles Ronshagen	Motorola Solutions Connectivity inc.	9513783175	chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/24/25 13:28:08	Vanauken Gordon	MCP	8145741186	GordonVanauken@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/24/25 13:28:10	Holly Peacock	INdigital	3347963686	hpeacock@indigital.net	No	Prime Contractor;
7/24/25 13:28:13	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasutions.com	No	Prime Contractor;
7/24/25 13:28:21	William Bassett	Indigital	260-403-8009	Bbassett@indigital. Net	No	Prime Contractor;
7/24/25 13:28:25	Mario Ruiz	AT&T	954-806-2467	Mr2673@att.com	No	Prime Contractor;

BROWARD COUNTY FLORIDA

Finance and Administration Services Department
PURCHASING DIVISION

Day 1 - Mandatory Site-Visit Sign-In Sheet(s)
(Vendors – Please leave a business card if you have one available)

Date: Thursday, July 24, 2025

Time: 2:30 PM

Location: Coral Springs Regional Public Safety Answering Point
2801 Coral Springs Drive
Coral Springs, FL 33065

Project: RFP No. GEN2129421P1, Next Generation 911

Please complete all of the information below and print legibly as Vendors may be contacted for information. Please note that an attendees can only represent one Vendor.

Name of Attendee: Jarrod Shupe Phone: 386-227-7675
Name of Vendor: Motorola Solutions Email: jarrod.shupe@motorolasolutions.com
Are you a lobbyist? (No) or Yes, I am representing (name of client): /
Circle all that apply:
(Prime Contractor) Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Jennifer Downs Phone: 401.826.8116
Name of Vendor: AT&T Email: jd2316uc@att.com
Are you a lobbyist? (No) or Yes, I am representing (name of client): _____
Circle all that apply:
(Prime Contractor) Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Holly Peacock Phone: 334-796-3686
Name of Vendor: INdigital Email: hpeacock@indigital.net
Are you a lobbyist? (No) or Yes, I am representing (name of client): _____
Circle all that apply:
(Prime Contractor) Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: William BASSETT Phone: 260-403-5009
Name of Vendor: INDIGITAL Email: BBASSETT@INDIGITAL.NET
Are you a lobbyist? (No) or Yes, I am representing (name of client): _____
Circle all that apply:
(Prime Contractor) Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Brent Savill Phone: 574-952-1547
Name of Vendor: INdigital Email: bsavill@indigital.net
Are you a lobbyist? No or Yes, I am representing (name of client): _____
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Joshua Payne Phone: 260 415 7613
Name of Vendor: INdigital Email: jpayne@indigital.net
Are you a lobbyist? No or Yes, I am representing (name of client): _____
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Charles Ronshagen Phone: 951-378-3175
Name of Vendor: Moto Sol. Connectivity inc. Email: Chuck.Ronshagen@MotorolaSolutions.com
Are you a lobbyist? No or Yes, I am representing (name of client): _____
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Mario Ruiz Phone: 954-806-2467
Name of Vendor: AT&T Email: _____
Are you a lobbyist? No or Yes, I am representing (name of client): _____
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: ROBERT HORNE Phone: 240 357 8246
Name of Vendor: MCP Email: [illegible]@mcpgl.com
Are you a lobbyist? No or Yes, I am representing (name of client): NO
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Name of Attendee: Gordon Vanauken Phone: 814-574-1181
Name of Vendor: MCP Email: _____
Are you a lobbyist? No or Yes, I am representing (name of client): _____
Circle all that apply:
Prime Contractor Subcontractor/Subconsultant Supplier
Broward County certified SBE Broward County CBE Broward County ACDBE Federal DBE

Sign-In Sheet for Mandatory Site Visit - Day 2
South Public Safety Answering Point
Friday, July 25, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/25/25 9:44:47	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/25/25 9:44:50	Vanauken Gordon	MCP	8145741186	GordonVanauken@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 9:44:56	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/25/25 9:45:05	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasolutions.com	No	Prime Contractor;
7/25/25 9:45:10	Mario Ruiz	AT&T	9548062467	mr2673@att.com	No	Prime Contractor;
7/25/25 9:45:12	Robert Horne	MCP	2403578296	Roberthorne@missikncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 9:45:15	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/25/25 9:45:25	Charles Ronshagen	Motorola Solutions Connectivity inc.	951-378-3175	Chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;

Sign-In Sheet for Mandatory Site Visit - Day 2
Plantation Public Safety Answering Point
Friday, July 25, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/25/25 10:48:46	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/25/25 10:48:52	Vanauken Gordon	MCP	8145741186	GordonVanauken@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 10:49:02	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/25/25 10:49:14	Charles Ronshagen	Motorola Solutions Connectivity inc.	951-378-3175	chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/25/25 10:49:16	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasolutions.com	No	Prime Contractor;
7/25/25 10:49:21	Robert Hirne	MCP	2403578296	Roberthorne@mission critical partners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 10:49:26	Mario Ruiz	AT&T	954-806-2467	mr2673@att.net	No	Prime Contractor;

Sign-In Sheet for Mandatory Site Visit - Day 2
EOC Public Safety Answering Point
Friday, July 25, 2025
GEN2129421P1, Next Generation 911

Completion time	Name of Attendee:	Name of Vendor (County staff: list your department here):	Attendee's Phone Number:	Attendee's Email:	Are you a lobbyist?	Select all that apply:
7/25/25 11:23:28	Jennifer Downs	AT&T	6018268116	jd236u@att.com	No	Prime Contractor;
7/25/25 11:23:40	Robert Horne	MCP	2403478296	Roberthorne@mcp911.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 11:23:41	Charles Ronshagen	Motorola Solutions Connectivity inc.	951-378-3175	chuck.ronshagen@motorolasolutions.com	No	Prime Contractor;
7/25/25 11:23:48	Vanauken Gordon	MCP	8145741186	GordonVanauken@missioncriticalpartners.com	No	Broward County Staff or Consultant Representing Broward County ;
7/25/25 11:24:01	Mario Ruiz	AT&T	954-806-2467	mr2673@att.com	No	Prime Contractor;
7/25/25 11:24:05	Josh Payne	INdigital	2604157613	jpayne@indigital.net	No	Prime Contractor;
7/25/25 11:24:08	Jarrod Shupe	Motorola Solutions	3862277675	Jarrod.shupe@motorolasplutions.com	No	Prime Contractor;

PURCHASING DIVISION
broward.org/Purchasing
BPRO Electronic Procurement System

Addenda No.: **1**
Solicitation No.: **GEN2129421P1**
Solicitation Title: **Next Generation 911 (NG911)**

Attention Vendors:
Note the following changes and clarifications.

1. The solicitation's closing date has been revised to August 22, 2025 by 2:00 p.m.

2. The following documents have been revised and replaced in their entirety. Any words in ~~strikethrough~~ type are deletions from existing text. Words in **bold underlined** type are additions to existing text.

    a. Scope of Work
    b. Evaluation Criteria
    c. Project Questionnaire
    d. Functionality Checklist

3. The following document(s) have been added:
    a. Addendum No. 1, Regional PSAP Diagram, GEN2129421P1, Next Generation 911
    b. Addendum No. 1, Non-Regional PSAP Diagram, GEN2129421P1, Next Generation 911

All other terms, conditions and specifications remain unchanged for this solicitation.

NEXT GENERATION 911 (NG911) SCOPE OF WORK

INTRODUCTION

Overview

Broward County is the second most populous County in the State of Florida with a population of ~~almost two million~~ **2,037,472** residents covering an area of thirteen hundred and twenty-three square miles.

The Broward County (County) Office of Regional Communications and Technology (ORCAT) is responsible for the engineering, implementation, operations, and strategic direction of the County's Regional Public Safety Communications Infrastructure, Public Safety Applications and the Consolidated Regional E-911 Call Taking/Dispatching System. Responsibilities for the Consolidated Regional E-911 Call Taking/Dispatching System include the management, administration, and oversight of the program, with a focus on ensuring established goals and performance targets are achieved. The County also provides E-911 technology services and support to the Non-Regional PSAPs.

The County relies on ORCAT for mission-critical public safety communications and applications used daily for Call Taking/Dispatching within the Public Safety Answering Points (PSAPs) for emergency response. On October 1, 2014, the County transitioned 28 cities into three Regional PSAPs (outlined below), operating with common call-taking and dispatching protocols and a centralized technology platform. The PSAPs currently answer approximately 2.3 million calls annually.

Three cities also operate PSAPs outside of the Regional PSAPs; they are Coconut Creek, City of Coral Springs, and City of Plantation, which comprise the Non-Regional PSAPs.

The 911 Phone System, Voice Recording System, and 911 Voice and Broadband Network are maintained and supported by ORCAT.

1.0 PROJECT REQUEST

The County seeks to procure and migrate to a market-ready National Emergency Number Association (NENA) i3-compliant Next Generation 911 (NG911) System, which includes an Emergency Services Internet Protocol (IP) Network (ESInet) and Next Generation Core Services (NGCS), to support the Regional and Non-Regional PSAPs within Broward County. The NG911 System will also enable the County to comply with Florida House Bill (HB) 441 (2019). The NG911 Service Provider shall be responsible for designing, documenting, installing, securing, operating, maintaining, monitoring, and enhancing the NG911 System in alignment with ongoing industry standards.

The technology changes associated with the NG911 System are expected to provide vast improvements over the current analog system, which include the following:

- Provides a network to support voice, data, text, pictures, video, telematics, and multimedia applications from any wired, wireless, or IP device.
- Enhanced survivability and network resiliency through the distributed design of NG911 System (e.g., delivery of calls to virtual PSAPs, Network-to- Network Interfaces [NNI], etc.)
- Faster call set-up time. The ability for NG911 Systems to provide end-to-end IP connectivity will eventually eliminate the use of the current Centralized Automatic Message Accounting (CAMA) trunks and reduce the circuit switch call set-up time.
- Provides the capability for the public to access the PSAP from anywhere, at any time, and from multiple devices.
- Interoperability for call delivery, transfer capability, and call processing across agencies, counties, and regions with predefined routing capability, which will enable the County to comply with HB 441 (2019). HB 441 requires that each county in the state have the ability to transfer 911 calls and text within its jurisdiction and outside its jurisdiction.
- Improved location information from the 911 caller at the mobile device level.

Response to this Request for Proposal (RFP) should not include marketing materials or generic text. The response should be responsive to the specific requirements stated herein.

General Information about the County's PSAPs

The County PSAPs are at the following locations with two different instances of Intrado VIPER®[1] 9-1-1 7:

- Regional PSAPs

[1] Voice over Internet Protocol for Emergency Response

- North (4900 West Copan's Road, Coconut Creek, FL)[2]
- Central (10440 W Oakland Park Blvd, Sunrise, FL)
- South (6057 SW 198th Terrace, Pembroke Pines, FL)
- Emergency Operation Center (EOC) – Backup PSAP (201 NW 84th Ave, Plantation, FL)

- Non-Regional PSAPs
  - Coral Springs (2801 Coral Springs Drive, Coral Springs, FL)
  - Plantation (451 NW 70th Terrace, Plantation, FL)
  - Emergency Operations Center (EOC) – Unmanned Backup PSAP (201 NW 84th Ave, Plantation, FL)

Metrics

PSAP Call Data FY24 (10/1/2023 9/30/2024)	Regional	Non Regional	Total
Total Incoming 911, Text, Alarm, Incoming Non-Emergency Requests	1,909,347	323,401	2,232,748
Total 911 Calls Incoming – Includes TTYs[3], TTY Challenges, and Abandoned Calls	1,187,528	134,117	1,321,645
Total Text-to-911 Incoming	4,084	585	4,669
Total Transfer Calls	101,794	19,634	121,428
Total Number of Call Taking Position	~~91~~ **97**	~~60~~**53**	~~151~~**150**

Technology and Call Data Breakdown

Number	Information Area	North Regional	Central Regional	South Regional	Coral Springs	Plantation	EOC
Technology							
1	Primary or Secondary PSAP	Primary	Primary	Primary	Primary	Primary	Backup
2	Computer-aided Dispatch (CAD) System	Motorola P1	Motorola P1	Motorola P1	Central Square	Hexagon	N/A
3	NICE X.X Voice Recording System	9.2	9.2	9.2	9.2	9.2	9.2
4	RapidSOS	Yes	Yes	Yes	Yes	Yes	Yes
5	Remote **911** VIPER Laptops	N/A	30	N/A	8	8	N/A
6	911 Incoming CAMA Trunks	55	50	21	28	6	26
7	Automatic Location Identification (ALI) Circuits	2	2	2	2	2	2

[2] North Regional PSAP will be relocated to the 1801 N.W. 49 Street, Fort Lauderdale 33309 by 4Q2026 or 1Q2027.

[3] Teletypewriters

8	Geographic Information System (GIS) Repository	N/A	Primary	N/A	N/A	N/A	Backup
9	Internet Circuit for VIPER 7	2	2	2	2	2	2

Current Environment:

Refer to Appendix A for more information regarding County's current environment.

a) 911 Call Ingress

Call ingress is how telephone providers send 911 calls to the 911 Service Provider. Today, these calls are sent over dedicated legacy CAMA or Signaling System 7 (SS7) trunks. The carrier calculates the number of trunks needed. The trunks are between the Originating Service Provider (OSP) and the selective router of the 911 Service Provider.

b) Call Routing

The 911 Service Provider's selective router receives the 911 calls and routes those calls to the selected PSAP using either the incoming trunk identification (ID) or the phone number provided with the call. The selective router has limited routing options, usually only normal, alternate (if the call cannot get to the normal route), and default (if the provider does not know where to send the call).

c) 911 Call Egress/Call Delivery

911 call egress or call delivery is how the calls are delivered to the PSAPs. The calls are split into multiple incoming trunk groups (wireline and wireless) to the Call-Handling Equipment (CHE) for each PSAP location. In addition, the trunk groups contain individual trunks that are terminated at multiple CHE hosts for diversity. The VIPER CHE then delivers the call to the proper PSAP for the Non-Regional PSAPs and to the automatic call distribution (ACD) system for the Regional PSAPs. The location information is then requested by the CHE at the PSAP via dedicated ALI circuits.

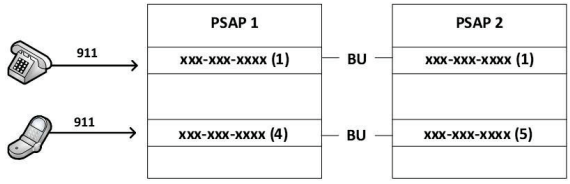


Figure 1: 911 Example Call Egress Trunk Diversity

d) Alternate Call Routing/Failover

The legacy 911 system provides limited alternate routing, so the County implemented contingency plans to overcome these limitations. While there are several scenarios developed, the remediation of them is accomplished by the two methods described below.

i. VIPER CHE Configurations

The alternate routing of calls between PSAPs within one environment and the Regional PSAP CAD failover (local mode) when VIPER is fully functional is accomplished via VIPER features.

ii. Manual Trunking Changes

If calls must be sent from one environment to another, the trunking must be switched to the new destination PSAP trunks. The 911 staff must contact the 911 provider to redirect calls from the current environment to the alternate environment, which takes a significant amount of time in the current environment. For example, the calls that normally go into the trunks of a PSAP that has been abandoned need to be redirected to the trunks of the new destination PSAP. This involves making changes to the routing table in the selective router and takes significant time to complete by the 911 service provider.

NEXT GENERATION 911 (NG911) SCOPE OF WORK

With the implementation of NG911 System, the County is planning for an additional level of alternate routing that may go to alternate environments (i.e., Regional versus Non-Regional) or neighboring counties to answer calls. This has not been implemented in the legacy environment due to the limitations of the current system. The time to alternate route calls is significantly reduced in an NG911 environment.

e) Security

Security in the legacy 911 system has been limited due to the restricted access to the 911 system. Only authorized providers can access the 911 system, and then, in most cases, only using specific types of traffic such as CAMA or SS7.

The County implemented dedicated trunk groups for TDoS remediation.

f) Network Redundancy and Resiliency

The legacy system has limited redundancy and resiliency. The County instituted additional trunking to diverse locations to help provide resiliency. Being connected and limited to a single primary selective router does limit this resiliency.

g) Call Processing

The VIPER CHE is used to process 911 calls and retrieve location information. For the Regional PSAPs, calls are routed to the three PSAPs, processed by the hosted VIPER, and delivered to the appropriate PSAPs by the VIPER ACD. For the Non-Regional PSAPs, calls are sent to the PSAPs, processed by VIPER, and delivered to the appropriate PSAP via ring groups.

VIPER also provides the ability to reroute calls between the PSAPs within each system environment (Regional or Non-Regional) but not between system environments.

h) Interfaces

The current 911 system is interconnected to the VIPER CHE. VIPER has interfaces to the CAD system and the Voice Recording System (VRS), replicated database servers for reporting, and Power Management Information System (MIS).

i) Reporting

The CHE Power MIS Reporting System provides preformatted and ad hoc reports for VIPER CHE statistics. PSAP managers have access to these reports. The CHE also has an ePrinter that captures the Call Detail Record (CDR).

General Overview of Desired System

This is a high-level overview of the desired NG911 System. The NG911 Service Provider should be deploying components and applications to accomplish the following:

a) 911 Call Ingress

OSPs shall deliver calls to at least two Points of Interconnection (POIs) that will provide resiliency in the call ingress to the NG911 System. The NG911 Service Provider shall be required to implement at least four POIs, two of which ~~must~~ **should** be **at least within 100 miles of the** ~~within~~ Broward County **border**. There shall be no single point of failure during the entire routing process of a County 911 call.

b) Call Routing

The NG911 Service Provider should have at least three geographically diverse data centers provisioned to route the calls for the County. GIS data from the County repository shall be used for geospatial routing. NG911 uses IP-based transport and not the point-to-point circuits of legacy 911, which allows for faster routing across the systems.

In most cases, location information is provided to the CHE during the call setup, not after the call is received. There shall be no single point of failure during the entire routing process of a County 911 call.

c) 911 Call Egress/Call Delivery

For each environment (Regional and Non-Regional), each PSAP shall have two circuits that will terminate at the VIPER load balancer. These circuits shall be sized to handle all calls for each environment, plus a 25% growth factor. In addition, each environment shall have two additional backup circuits that terminate directly into VIPER servers to provide alternate delivery paths if the primary circuits fail, or the load balancers do not function. Each PSAP shall have network equipment installed to interconnect to the ESInet. This equipment is typically a router and switch. There shall be no single point of failure during the entire 911 call egress and call delivery process of a County 911 call.

d) Alternate Call Routing/Failover

Rerouting calls based on the call type, geographic location of the caller, or specific error conditions is all possible with NG911. The existing routing within the environment (with VIPER in service) and local mode scenarios will be managed by VIPER as it is now. For the failure of a single- or two-PSAP load balancer or VIPER server, the NG911 Service Provider shall be able to detect the failure and institute predefined or default alternate routing immediately. The need to transfer calls to the other environment should be automatically implemented by the NG911 Service Provider by using pre-planned rules and not require manual changes to the circuits when VIPER is in one environment (Regional or Non-Regional), and unable to take calls (e.g., no users logged in, equipment failure, manual switch, etc.).

Routing outside of Broward County will be implemented using interconnectivity to the neighboring counties. This should be implemented either automatically or manually by switches or calls to the NG911 Service Provider to trigger pre-planned rules. There shall be no single point of failure during the alternate call routing and failover process of all 911 calls. The NG911 Service Provider should set up tertiary backup circuits using wireless or satellite technology to deliver 911 calls in the event of an ESInet failure.

e) Security

NG911 uses standards-based systems and IP protocols, which present a higher risk than legacy analog technology. To protect the system, NG911 uses the Border Control Function (BCF) between the NG911 system and all outside interfaces or interconnections. Compliance with the *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)* is expected for the NG911 System.

Many agencies rely on Certification Authorities for authentication and preventing security risks. According to NENA/NIOC[3] 01-002, *NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines*, "Certification Authorities (CAs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing assurance of identity. The widely placed trust in CAs is at the heart of security mechanisms used to protect sessions and transactions for Next Generation 9-1-1 (NG9-1-1). National Emergency Number Association's i3 and associated standards *(and the County)* require Transport Layer Security (TLS) throughout the ecosystem to allow for secure communications and a single shared root of trust to assist with *(the operation and)* interoperability *(of the NG911 System)*. TLS relies on CAs to identify Servers and Clients. The root of trust in the NG9-1-1 Public Key Infrastructure (PKI) is the PCA."[4]

In addition, many NG911 systems use a complex group of monitoring, scanning, and controls including virus protection, intrusion detection, intrusion prevention, configuration management password requirements, Multifactor Authentication (MFA), and lab testing before changes are made to protect the network and components of the NG911 system.

To help reduce or eliminate TDoS attacks, the NG911 Service Provider should implement the newer protocols of Secure Telephone Identity Revisited (STIR) and Signature- based Handling of Asserted Information Using toKENs (SHAKEN). STIR/SHAKEN is used to verify callers on the systems. Calls that fail this verification should be identified to the CHE based on attestation information from the NGCS in the NG911 system so they can be processed in the event there is a valid emergency. This process will be used to reduce the number of swatting incidents.

f) Network Redundancy and Resiliency

Network redundancy and resiliency are the basis of the NG911 System and are built in from the beginning. There shall be geographic and carrier-diverse components to prevent a disaster from impacting the entire NG911 System. There shall be no single point of failure during the entire routing process of a County 911 call.

g) Call Processing

The VIPER CHE is used to process 911 calls and retrieve location information. For the Regional PSAPs, calls are routed to the three PSAPs, processed by the hosted VIPER, and delivered to the appropriate PSAPs by the VIPER ACD. For the Non-Regional PSAPs, calls are sent to the PSAPs, processed by VIPER, and delivered to the appropriate PSAP via ring groups.

VIPER also provides the ability to reroute calls between the PSAPs within each system environment (Regional or Non-Regional) but not between system environments.

h) Interfaces

The NG911 System shall be interconnected to the VIPER CHE. The VIPER CHE interfaces to (Power MIS, the CAD system, VRS, replicated database servers, and the data warehouse (future). The NG911 Service Provider shall also be able to interconnect with the NG911 systems of neighboring jurisdictions to transfer calls and to provide the ability to use neighboring jurisdictions and backup PSAPs, if needed, using NNIs.

i) Reporting

[3] NG9-1-1 Interoperability Oversight Commission
[4] NENA 01-002 (ng911ioc.org)

NEXT GENERATION 911 (NG911) SCOPE OF WORK

Power MIS will provide preformatted and ad hoc reports of the data from the VIPER CHE. PSAP managers will have access to these reports. In addition, a dashboard provided by the NG911 Service Provider shall gather and present additional information such as call volumes, call types, abandoned calls, network processing times, logs from each NGCS functional element, transfer dates/times, alternate routing counts, and ESInet-to-ESInet counts. Vendor reporting on service requests for response and resolution times, and call delivery to the PSAPs from the NG911 System provide capabilities for analytical analysis of available data dependent on the vendor's capabilities.

The following documents referenced below are a part of the Scope of Work and all requirements outlined in each document shall be delivered as a part of the implementation phase (Go-Live) of the project:

- Functionality Checklist
- General Compliance
- Project Questionnaire

2.0 NG911 SERVICE PROVIDER REQUIREMENTS

This section provides the County's General Requirements. Vendors will be asked to indicate their ability to comply with each requirement listed in the Functionality Checklist, the Project Questionnaire, or General Compliance.

2.1 Vendor General Requirements

Proposing vendors will need to provide a response to each requirement listed in the Vendor General Requirements section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

2.2 Professional Services Requirements

Proposing vendors will need to provide a response to each requirement listed in the Professional Services Requirements section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

3.0 EQUIPMENT AND HARDWARE

This section provides the County's Equipment and Hardware Requirements. Proposing vendors will need to provide a response to each requirement listed in the Equipment and Hardware section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

4.0 GENERAL SYSTEM REQUIREMENTS

This section provides the County's General System Requirements. Proposing vendors will need to provide a response to each requirement listed in the General System Requirements section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.0 TECHNICAL REQUIREMENTS

This section provides the County's Technical Requirements. Vendors will be asked to indicate their ability to comply with each requirement listed in the Functionality Checklist, the Project Questionnaire, or General Compliance.

5.1 General Technical Requirements

Proposing vendors will need to provide a response to each requirement listed in the General Technical Requirements section of the Functionality Checklist, Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.1.1 Security/Notifications

Proposing vendors will need to provide a response to each requirement listed in the Security/Notifications section of the Functionality Checklist, Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.2 911 Inputs

5.2.1 911 Call Ingress

Proposing vendors will need to provide a response to each requirement listed in the 911 Call Ingress section of the Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.3 NG911 Processing

5.3.1 GIS

Proposing vendors will need to provide a response to each requirement listed in the GIS section of the Functionality Checklist, Project Questionnaire, and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.3.2 Data Processing

Proposing vendors will need to provide a response to each requirement listed in the Data Processing section of the Functionality Checklist and Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.3.3 Call Routing

Proposing vendors will need to provide a response to each requirement listed in the Call Routing section of the Functionality Checklist, Project Questionnaire, and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.3.4 Network Redundancy and Resiliency

Proposing vendors will need to provide a response to each requirement listed in the Network Redundancy and Resiliency section of the Functionality Checklist and Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.4 NG911 Call Delivery

5.4.1 911 Call Egress/Call Delivery to all PSAPs

Proposing vendors will need to provide a response to each requirement listed in the 911 Call Egress/Call Delivery section to all PSAPs section of the Functionality Checklist and Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

5.4.2 Alternate Call Routing/Failover

Proposing vendors will need to provide a response to each requirement listed in the Alternate Call Routing/Failover section of the Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

6.0 FUNCTIONAL REQUIREMENTS

This section provides the County's Functional Requirements. Vendors will be asked to indicate their ability to comply with each requirement listed in the Functionality Checklist, the Project Questionnaire, and General Compliance.

6.1 NG911 Call Delivery

6.1.1 Call Processing

Proposing vendors will need to provide a response to each requirement listed in the Call Processing section of the Functionality Checklist, Project Questionnaire, and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

6.1.2 Interfaces

Proposing vendors will need to provide a response to each requirement listed in the Interfaces section of the Functionality Checklist, Project Questionnaire, and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

6.2 Reports

Proposing vendors will need to provide a response to each requirement listed in the Reports section of the Functionality Checklist and Project Questionnaire, that fall under this section. All responses will need to be submitted with the vendor's proposal.

7.0 NG911 SYSTEM DEPLOYMENT

This section provides the County's System Deployment Requirements. Vendors will be asked to indicate their ability to comply with each requirement listed in the Functionality Checklist, the Project Questionnaire, and General Compliance.

7.1 Initial Deployment

Proposing vendors will need to provide a response to each requirement listed in the Initial Deployment section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

7.2 Testing

Proposing vendors will need to provide a response to each requirement listed in the Testing section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

7.3 Go-Live and Post Go-Live

Proposing vendors will need to provide a response to each requirement listed in the Go-Live and Post Go-Live section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

8.0 TRAINING

This section provides the County's Training Requirements. Proposing vendors will need to provide a response to each requirement listed in the Training section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

9.0 MAINTENANCE AND SUPPORT REQUIREMENTS

This section provides the County's Maintenance and Support Requirements. Vendors will be asked to indicate their ability to comply with each requirement listed in the Functionality Checklist, the Project Questionnaire, and General Compliance.

9.1 Maintenance and Support

Proposing vendors will need to provide a response to each requirement listed in the Maintenance and Support section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

9.2 Service Level Expectations

Proposing vendors will need to provide a response to each requirement listed in the Maintenance and Support section of the Project Questionnaire and General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

Table 1: Severity Levels

NEXT GENERATION 911 (NG911) SCOPE OF WORK

Severity Level	Description	Examples
Level 1 – Critical	An incident shall be categorized as Severity Level 1 if it meets any of the following criteria: a) Renders a business-critical system, Functional Element, call routing to the proper egress point, or NG911 Service Provider infrastructure unavailable or substantially unavailable b) Failure of system failover c) Cybersecurity incident that impedes the ability to route or process 911 calls d) Seriously impacts normal business operations e) Voice quality with an MOS of less than 3.5	1. Isolation of one or more PSAPs from the rest of the ESInet 2. Inability to route calls to the designated PSAP for each environment TDoS/DDoS attacks 3. Loss of any ESInet circuit 4. Decrease in throughput greater than or equal 5. to 2.5% of the capacities at any data center Failure of PRF routing as defined 6. Audio degradation for 911 calls 7.
Level 2 – Major	An incident shall be categorized as Severity Level 2 if it meets any of the following criteria: a) Causes the failure or loss of functionality of a single or multiple Functional Elements, components, or features, while the NG911 System itself remains operational b) Causes a loss of 2.5% of call taking capacity overall for either Regional or Non-Regional PSAPs, or 5% of call taking capacity at any individual PSAP c) Causes the loss of all call taking capability d) Critical or major alarm condition by component or Functional Element f) Voice quality with an MOS between 3.5 and 3.9 g) Transactional logs for functional elements and overall call processing become unavailable h) Inability to transfer 911 calls within and outside of Broward County via the NG911 System i) Failure of the NG911 System's ability to route calls from one environment to the other based on routing rules or on demand j) Impedes the work of one or more individuals performing a critical business function (Portal Function)	1. Loss of redundant connectivity for any data center connection 2. Loss of redundancy at a PSAP 3. System or component problem that could result in loss of connectivity to a PSAP 4. Decrease in throughput equal to or greater than 5% on any one circuit 5. Loss of ANI or ALI for 911 calls 6. Misrouting of one or more calls in an hour 7. Audio degradation for 911 calls Loss 8. of transactional logs on the PRF element 9. Call transfer failures 10 Unable to reroute calls from Non-Regional to Regional
Level 3 – Minor	An incident shall be categorized as Severity Level 3 if it meets any of the following criteria: a) Causes any performance degradation b) Causes loss of access to any system, service, software, equipment, or network component, or a key feature thereof c) Call delivery failure greater than 1% per hour d) Results in malfunction or loss of any hardware or software component e) Results in a major alarm condition	1. Individual circuit failure or degradation 2. Loss of ANI for non-emergency calls 3. Audio degradation for non-emergency calls 4. Reports of a call delivery failure by the PSAP
Severity Level	**Description**	**Examples**
Level 4 – Maintenance	Severity 4 incidents are non-service-affecting and include: a) Enhancement requests b) Inquiries c) Maintenance d) CMR requests	

Table 2: Severity Levels Response and Repair Timeframes

NEXT GENERATION 911 (NG911) SCOPE OF WORK

Trouble Category	Remote Response Time for reported issues or Critical Major Alarm	Onsite Response Time	Repair Time
Severity Level 1	5 minutes	30 minutes	If failover from redundant Functional Element environments or the network is available, the NG911 Service Provider shall conduct a remote failover within five minutes of verifying that the active environment, network, or Functional Element is in a failed state, or conduct remote failover within ten minutes of alarm condition, or report from the County of the Severity 1 issue, whichever is earlier. If the NG911 Service Provider successfully conducts a remote failover, the NG911 Service Provider will not be required to meet the onsite response time after notice. The NG911 Service Provider shall dedicate resources onsite or at its data center 24/7/365 to resolve the issue or reduce the impact of the issue to a Severity Level 3 within five minutes.
Severity Level 2	5 minutes	1 hour	The NG911 Service Provider shall dedicate resources onsite or at its data center 24/7/365 to resolve the issue or reduce the impact of the issue to a Severity Level 3 or below within ten minutes.
Severity Level 3	2 hours	8 hours	The NG911 Service Provider shall work on the issue onsite or at its data center until the issue is resolved, which may include a configuration, rule, or routing change in a future maintenance release.
Severity Level 4	Next Business Day	Next Business Day	Based on the estimate of effort to complete the request, which will be prioritized and scheduled as agreed upon between the NG911 Service Provider and the County.

Table 3: Service Performance

Service	Performance Measures
Uptime	99.999% measured at the PSAP
Voice Quality	Meets or exceeds ITU-T-P.830 and must be able to maintain an MOS standard rating of 4.0 or higher.
Service	**Performance Measures**
Call Delivery Time **Measured from presentation of call or invite at the POI to delivery to the CHE**	Less than 500 ms and 95% of the calls less than 300 ms
Network traffic convergence	Network convergence of less than 54 ms
Latency	Less than or equal to 50 ms

Jitter	Less than or equal to 5 ms one way, end to end
Packet Loss	Less than 0.1%

Table 4: Service Credits

Trouble Category	Remote Response Time	Service Credit
Severity Level 1	5 minutes	10% of monthly invoice for each 5-minute increment past the remote response time per incident
Severity Level 2	5 minutes	5% of monthly invoice for each 15-minute increment past the response time per incident
Severity Level 3	2 hours	5% of monthly invoice for each 2-hour increment past the response time per incident
Overall Performance	**System Availability**	**Service Credit**
Service Performance (Based on availability of the System)	99.999%	Based on the duration of the failure to meet the service performance: • 30 seconds to 5 minutes – 75% of monthly invoice • > 5 minutes – 100% of monthly invoice

10.0 PROPOSED TIMELINE

This section provides the County's Timeline Requirements. Proposing vendors will need to provide a response to each requirement listed in the Timeline section of the General Compliance that fall under this section. All responses will need to be submitted with the vendor's proposal.

11.0 FINAL ACCEPTANCE CRITERIA

This section provides the County's Final Acceptance Criteria Requirements. Proposing vendors will need to provide a response to each requirement listed in the Training section of the Project Questionnaire that fall under this section. All responses will need to be submitted with the vendor's proposal.

Appendix A: Current environment:

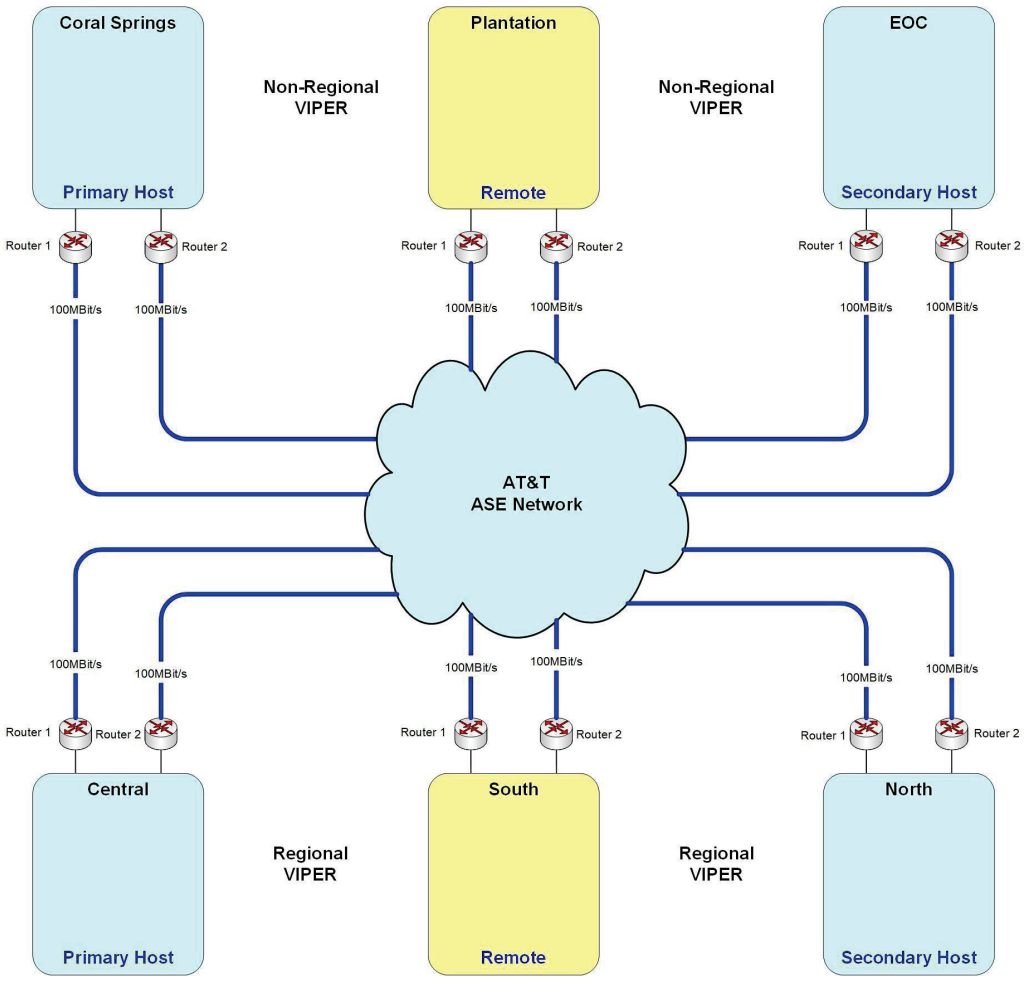


Figure 2: High-level Current 911 System

Currently, the Originating Service Providers (OSPs) deliver their calls to a primary 911 selective router. A single selective router delivers most 911 calls to the two environments (Regional and Non-Regional) using multiple trunk groups of wireline and wireless traffic from geographic areas. Each trunk group is split between the three PSAPs and three hosts in each environment for diversity. Annexations by the County have required additional trunks from two other selective routers (Palm Beach County and Dade County) to be implemented.

Appendix B: Adopted Standards and Best Practices

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[5]
APCO/TMA	2.101.3-2021	Alarm Monitoring Company to Emergency Communications Center (ECC) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)	Provides detailed information on data elements and structure standards for electronic transmission of new alarm events from an alarm monitoring company to an ECC.	Version 3.4 2021
APCO/NENA	1.102.3.2020	Emergency Communications Center (ECC) Service Capability Criteria Rating Scale	APCO and NENA jointly have developed an assessment tool to evaluate current capabilities of the ECC against models representing the best level of preparedness, survivability, and sustainability amidst a wide range of natural and manmade events.	Version 3 2020
ATIS/TIA	ATIS J-STD-110.01.V002	Joint ATIS/TIA Native SMS/ MMS Text To 9-1-1 Requirements and Architecture Specification	The purpose of this Standard is to define the requirements, architecture, and procedures for text messaging to 9- 1-1 emergency services using native CMSP SMS or MMS capabilities for the existing generation and next generation (NG9-1-1) Public Safety Answering Points (PSAPs).	Release 2 May 1, 2015
ATIS	ATIS-0500017	Considerations for an Emergency Services Next Generation Network (ES-NGN)	Identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next-generation telecommunications networks.	Version 1 June 2009
U.S. Department of Justice/ Federal Bureau of Investigation	CJISD-ITS-DOC-08140-5.9	Criminal Justice Information Services (CJIS) Security Policy	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information.	Version 5.9 June 1, 2020

[5] For any standards, if a newer version is available at the time of publication of this RFP, compliance will be judged relative to the latest version. The exception to this being NENA/APCO-INF-005.1-2014 for which compliance will be judged relative to NENA's updated Emergency Incident Data Object STA document

IETF	RFC 3261	SIP: Session Initiation Protocol	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	June 2002

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date
IETF	RFC 6874	Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers	Extends RFC 3986 to include IPv6 to include zone identifiers and address literals	February 2013
IETF	RFC 8865	T.140 Real-Time Text Conversation over WebRTC Data Channels	Specifies how a Web Real-Time Communication (WebRTC) data channel can be used as a transport mechanism for real-time text.	January 2021
NENA/APCO	REQ-001.1.2-2018	Next Generation 9-1-1 PSAP Requirements Document	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP	Version 1.1.2 June 10, 2018
NENA	NENA-STA-006.2-2022	Standard Data Formats for 9-1-1 GIS Data Model	This document defines the GIS data information, formats, requirements and related information used in NENA Next Generation 9-1-1 (NG9-1-1) Core Services (NGCS)	Revised September 23, 2022
NENA	STA-008.2-2014 (originally 70-001)	Registry System Standard	Describes how registries (lists of values used in NG911 functional element standards) are created and maintained	Version 2 October 6, 2014
NENA	STA-010.3b-2021	NENA i3 Standard for Next Generation 9-1-1	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards	Version 3b October 7, 2021
NENA	INF-016.2-2018 (formerly 08-506)	Emergency Services IP Network Design Information Document (ESIND) for NG9-1-1	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInet	Version 2 April 5, 2018

NEXT GENERATION 911 (NG911) SCOPE OF WORK

NENA	08-751	i3 Technical Requirements Document	Provides requirements for ESInet architecture and security, among other i3 PSAP functions, and establishes a foundation for future i3 standards development	Version 1 September 28, 2006
NENA	54-750	NENA/APCO Human Machine Interface & PSAP Display Requirements (ORD)	Prescribes requirements for the human machine interface (HMI) display for the Next Generation 9-1-1 (NG9- 1-1) System	Version 1 October 20, 2010

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date
NENA	75-001 (Currently being updated) will become NENA-STA-040.2	Security for Next Generation 9-1-1 (NG-SEC)	Establishes the minimal guidelines and requirements for levels of security applicable to NG9-1-1 entities	February 6, 2010
NENA	75-502	Next Generation 9-1-1 Security (NG-SEC) Audit Checklist	Provides the educated user a method to document an NG-SEC Audit	Version 1 December 14, 2011
NENA	NENA-INF-015.1-2016	NG9-1-1 Security (NG-SEC) Information Document	Provides mechanisms and best practices for cybersecurity for i3 systems	Version 1 December 8, 2016
NENA	NENA-INF-040.2-2022	NENA Managing & Monitoring NG9-1-1 Information Document	Provides guidance on best practices for monitoring and managing NG9-1-1 services and infrastructure.	Version 2 July 27, 2022
NENA	NENA-STA-021.1a-2022	NENA Standard for Emergency Incident Data Object (EIDO)	Provides standard format for exchanging emergency incident data between disparate systems and agencies	Version 1a April 19, 2022
NENA	NENA STA-031.1-2021	NENA Standard for Interconnecting Emergency Services IP Networks and Public Safety Broadband Networks	Establish standards for interconnections between ESInets and other broadband networks used by first responders.	October 14, 2021
NENA/NIOC	NIOC V1.0.0	NG9-1-1 Interoperability Oversight Commission (NIOC) (PSAP) Credentialing Authority (PCA) Certification Validation Guidelines	Provides the security requirements needed to support the secure validation for issuance of Certificates in NG9-1-1 by the PCA Certification Authorities (CAs) in the NG9-1-1 Public Key Infrastructure.	V1.0.0 February 9, 2022

NIST	FIPS 140-3	Security Requirements for Cryptographic Modules	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information	Version 2 March 22, 2019
NIST	Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure	Version 1.1 April 16, 2018
TIA	TIA-942-B	Telecommunications Infrastructure Standard for Data Centers	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers	Revision B July 12, 2017

Appendix C: Acronyms

Acronyms	Terms
AAR	After-action Review
ACD	Automatic Call Distribution
ACL	Access Control List
AI	Artificial Intelligence
ALI	Automatic Location Identification
ANI	Automatic Number Identification
APCO	Association of Public-Safety Communications Officials International
ASAP	Automated Secure Alarm Protocol
ASE	AT&T Switched Ethernet
ATIS	Alliance for Telecommunications Industry Solutions
BGP	Border Gateway Protocol
BCF	Border Control Function
CA	Certification Authority
CAD	Computer-aided Dispatch
CAMA	Centralized Automatic Message Accounting
CDR	Call Detail Record
CHE	Call-handling Equipment
CJIS	Criminal Justice Information Services

CLDXF	Civic Location Data Exchange Format
CMSP	Commercial Mobile Service Provider
COO	Chief Operating Officer
COOP	Continuity of Operations
COS	Class of Service
CS	Committee Substitute
CSF	Cybersecurity Framework
CSR	Client Service Representative
CTD	Communications and Technology Division
DDoS	Distributed Denial of Service
DOJ	Department of Justice
DSCP	Differentiated Service Code Point
ECC	Emergency Communications Center

Acronyms	Terms
ECRF	Emergency Call Routing Function
EF	Enhanced Fujita Scale
EIDO	Emergency Incident Data Object
EOC	Emergency Operations Center
ESIND	Emergency Services IP Network Design Information Document
ESInet	Emergency Services IP network
ES-NGN	Emergency Services Next Generation Network
ESN	Emergency Services Number
ESRP	Emergency Services Routing Proxy
ETL	Extract, Transform, Load
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FirstNet	First Responder Network Authority
FY	Fiscal Year
GIS	Geographic Information System
HB	House Bill

HMI	Human Machine Interface
IAM	Identity and Access Management
ICA	Intermediate Certificate Authorities
ICD	Interface Control Document
ID	Identification
IETF	Internet Engineering Task Force
IM	Instant Message
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization of Standards
IVR	Interactive Voice Response
LDB	Location Database
LNG	Legacy Network Gateway
LoST	Location to Service Translation
LSRG	Legacy Selective Router Gateway
LTE	Long-term Evolution
LVF	Location Validation Function
MCS	MSAG Conversion Service

Acronyms	Terms
MFA	Multi-factor Authentication
MIS	Management Information System
MLTS	Multiline Telephone System
MMS	Multimedia Service
MOP	Method of Procedure
MOS	Mean Opinion Score
ms	Millisecond
MSA	Metropolitan Statistical Area
MSAG	Master Street Address Guide
MSRP	Message Session Relay Protocol
NAD83	North American Datum of 1983

NENA	National Emergency Number Association
NG911 or NG9-1-1	Next Generation 911 (9-1-1)
NGCS	Next Generation Core Services
NG-SEC	Next Generation Security
NIOC	NG9-1-1 Interoperability Oversight Commission
NIST	National Institute of Standards and Technology
NNI	Network-to-network Interface
NOC	Network Operations Center
NPSBN	Nationwide Public Safety Broadband Network
NTP	Network Time Protocol
OCIF	Outbound Call Interface Function
ORCAT	Office of Regional Communications and Technology
OSI	Open Systems Interconnection
OSP	Originating Service Provider
pANI	Pseudo Automatic Number Identification
PBX	Private Branch Exchange
PCA	PSAP Credentialing Agency
PKI	Public Key Infrastructure
PL	Phone Line
PM	Project Manager
POI	Point of Interconnection
PRF	Policy Routing Function
PRR	Policy Routing Rules

Acronyms	Terms
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RCA	Root Cause Analysis
RFC	Request for Comment
RFO	Reason for Outage

RFP	Rrquest for Proposal
RTT	Real-time Text
SDO	Standards Development Organization
SHAKEN	Signature-based Handling of Asserted Information Using toKENs
SI	Spatial Interface
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SOI	Service Order Input
SOW	Statement of Work
SS7	Signaling System 7
STIR	Secure Telephone Identity Revisited
TCC	Text Control Center
TDD	Telecommunications Device for the Deaf
TDM	Time Division Multiplex
TDoS	Telephony Denial of Service
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TMA	The Monitoring Association
toKENS	
TSP	Telecommunications Service Priority
TTY	Teletypewriter
UI	User Interface
UL	Underwriters Laboratory
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier

NEXT GENERATION 911 (NG911) SCOPE OF WORK

Acronyms	Terms
URN	Uniform Resource Name
VoIP	Voice over IP
VIPER	
VRS	Voice Recording System
WebRTC	
WGS84	World Geodetic System 84

EVALUATION CRITERIA

Next Generation 911 (NG911)

Submit responses to all evaluation criterion as outlined below. Vendors that fail to submit information and/or documentation required by an evaluation criterion by solicitation's closing date and time may receive no points (if applicable) for the corresponding Evaluation Criteria. Refer to Instructions to Vendors for additional information. Vendors should structure their proposal to align with the order of the Evaluation Criteria.

	Total Points
1) Ability of Professional Personnel (Maximum 8 Points)	
A. **Ability of Professional Personnel:** Describe the qualifications and relevant experience of the Project Manager and all key staff, including subconsultants, intended to be assigned to this Project. Include resumes for the Project Manager and all key staff described. Refer to General Compliance sections for requirements: i. Professional Services Requirements: PS001.a, PS001.b, PS001.c, PS002.b, PS006.b, PS007.b, and PS008.b ii. Organizational Chart: PS009	**3**
B. **General Vendor Information:** Describe Vendor's operation providing these types of solutions. Refer to General Compliance sections for requirements: i. Vendor General Requirements: VN001 and VN003 – VN005	**5**
2) Project Approach: General System Requirements and Overall Approach (Maximum 15 Points)	
Describe Prime Vendor's approach to the project, per the Scope of Work. Refer to the General Compliance sections listed below for requirements: i. System Requirements: SR-GN001, SR-GN002b, SR-GN003 - SR-GN005, SR-GN007.b, SR-GN008b, SR-GN009, SR-GN010.b, SR-GN011, SR-GN012, SR-GN013.b, SR-GN017.b, SR-GN018, SR-GN021, SR-GN024, SR-GN025, SN001.b, SN003.b, SN006, SN007, SN015, SN016, SN019 ii. NG911 Processing: SR-GI001.b iii. Call Routing: SR-CR002.b iv. NG911 Call Delivery (Call Processing): SR-CP002.b v. Network Redundancy and Resiliency: SR-NR005 vi. Implementation Timeline: TIME001. vii. Hardware and Equipment: SR-EH001 and SR-EH002 viii. Initial Deployment: SD004.b ix. Testing: TS005 x. Go-Live: GL001.b xi. Training: TRN007, TRN008.b, TRN009 - TRN012	**15**
3) Project Approach: NG911 Solution (Maximum 25 Points)	
A. **Functionality Checklist:** Refer to the Functionality Checklist and submit as instructed. Points will be allocated based on Vendor's Functionality Checklist response. i. Security/Notification: SN003.b, SN009, SN010.b, SN011 – SN013, SN020 ii. **911 Call Ingress: SR-IN003.b** iii. NG911 Processing: SR-GI013 iv. Data Processing: DAT001.b and DAT003.b v. Call Routing: SR-CR003.b, SR-CR004, SR-CR006.b, SR-CR008, Sr-CR009, SR-CR010.b, and SR-CR011	**15**

EVALUATION CRITERIA

vi. Network Redundancy and Resiliency: SR-NR007, and SR-NR008.b vii. NG911 Call Delivery (Call Egress/Call Delivery to All PSAPs): SR-DL001, SR-DL004, SR-DL005.b, SR-Dl006, SR-DL007, SR-DL014.b, and SR-DL015 viii. NG911 Call Delivery (Call Processing): SR-CP003 – SR-CP005 ix. Interfaces: SR-IT003 x. Reports: RPT001, RPT002.b, RPT003 – RPT005	
B. **Demonstration Script:** Points will be allocated based on the results of the Technical Review Team Vendor's Demonstration Report for Vendor Demonstrations. Refer to the Instructions to Vendors for additional information.	**10**
4) Project Approach: Maintenance and Support Services, Service Level Experiences (Maximum 15 Points)	
Describe Vendor's approach to providing Maintenance and Support Services as per the General Compliance sections below: a) Maintenance and Support Services: i. SR-MR002, SR-MR004, SR-MR005, and SR-MR009 ii. SN001.b and SN019 Describe Vendor's approach and willingness to meet the Service Level Expectations as per the General Compliance sections below: b) Service Level Expectations i. SR-SLA003.b, SR-SLA004, SR-SLA005.b, SR-SLA007, and SR-SLA008	**15**
5) Project Approach: Evidence, Knowledge, and Experience (Maximum 10 Points)	
A. Describe Prime Vendor's experience on projects of similar nature, scope and duration, along with a detailed description of satisfactory completion, both on time and within budget, for the past three years. Provide a minimum of five (5) projects with references. Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed or within three business days after County's request. Only provide references for non-Broward County Board of County Commissioners contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance. Including, but not limited to, the information outlined in the General Compliance section VN006	**6**
B. Provide actual performance results for the metric below on solutions in production. Refer to the General Compliance for requirements: i. Solution Performance: VN007 and VN008	**4**

EVALUATION CRITERIA

6) Workload of Firm (Maximum 2 Points)	
For the Prime Vendor only, list all completed and active projects that the Prime Vendor has managed within the past five (5) years. In addition, list all projected projects that Prime Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Prime Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Prime Vendor worked on concurrently. Describe Prime Vendor's approach to managing these projects. Were there or will there be any challenges for any of these listed projects? If so, describe how Prime Vendor dealt or will deal with projects' challenges.	**2**
7) Location (Maximum 5 Points)	
Refer to **Location Certification** and submit as instructed. The maximum points shall be assigned to each Locally Based Business and to each joint venture that is composed solely of Locally Based Businesses. Points shall be allocated as follows based on the Prime Vendor's selection of one of the five options in the Location Certification Form: Option 1 (0 points); Option 2 (5 points); Option 3 (3 points); Option 4 (points range from 0-5 depending on the composition of the joint venture); and Option 5 (0 points).	**5**
8) Pricing (Maximum 20 Points)	
Refer to the electronic bidding system and submit as instructed. Vendor's total proposed price submitted in the **Bid Table titled Next Generation (NG911) Proposed Solution** will be used for scoring purposes as per the formula set forth below. Pricing must reflect all recurring and non-recurring fees as defined in the Scope of Work. Refer to **Instructions to Vendors** for additional information. Total points awarded for price will be determined by applying the following formula: **(Lowest proposed price/Proposer's price) x 20 = Price Score** Note: **Bid Table titled Optional Renewal Terms** will not be used in the calculation of points for price.	**20**
TOTAL NUMBER OF POINTS	**100**

Project Questionnaire

Next Generation 911 (NG911)

INSTRUCTIONS: Respond to each requirement with the appropriate selection by indicating a "**Yes**" under the "Complies" column if the proposed solution "Complies" with the requirement as stated and the information requested is also provided or indicate "**Yes**" under the "Does Not Comply" column if the proposed solution "Does Not Comply" for each requirement in this document. Vendors may be deemed non-responsible if they fail to demonstrate compliance with each "**yes**" response in the Project Questionnaire.

Insert Vendor Name:

NG911 System			**Complies (All requested information associated with the requirements below must also be provided)**	**Does Not Comply**
No.	**NG911 Service Provider Requirements**			
Vendor General Requirements				
1	VN002	The NG911 Service Provider shall have experience providing		

	NG911 systems for at least five years: The NG911 Service Provider shall describe the specific NG911 services provided and the year those services were first provided. If subcontractors are to be used for this project, they shall also meet the same requirement.		
Professional Services Requirements			
1	PS001.1 Project Management Responsibilities: The NG911 Service Provider shall assign a dedicated PM who, for the duration of the project, the PM shall: 1. Ensure the Scope of Work (SOW) is completed (includes a Project Schedule of key milestones). a) Equipment delivery b) Installation and configuration c) Testing schedule d) Go-live schedule 2. Ensure that the NG911 Service Provider-assigned resources are scheduled for the activities and deliverables outlined in the		

	Project Plan and Project Schedule. 3. Perform comprehensive risk assessment and mitigation planning. 4. Ensure project status meetings are scheduled, led, and documented, and meeting minutes are distributed within 24 hours of all meetings. 5. Maintain an issues log and ensure all issues are prioritized and worked in a timely manner during the life of the project. 6. Maintain all project-related communications and documentation.		
2	PS002 Project Plan and Schedule: PS002.a The NG911 Service Provider shall provide a draft project plan and timeline (a task-oriented Gantt chart based on the project plan and delivered in Microsoft Project) that shows the entire project calculated from the date of contract signature to go-live. Minimum required elements of the project plan include at a minimum:		

	• Installation all equipment on premise and within the NGCs domain • Schedule and strategy for connecting other ESInets (such as Miami Dade and Palm Beach counties) • Buildout of operational NGCS • Buildout of OSP meet points • Schedule and strategy for connecting OSPs • Operational network operations center (NOC)/security operations center (SOC) • Fully functional spatial routing of calls • Implementation of multimedia (e.g. video, picture, sensor, etc.) • Final Design Review Sessions based on Statement of Work • All phases of testing (e.g. NG911 Provider testing, Preliminary Acceptance Testing, Final Acceptance Testing after Go-Live) • Cutover by environment and PSAP (i.e. Regional PSAPs and the Non-Regional PSAPs)		
3	PS003 Final Project Plan: A final project plan, timeline, and a Gantt chart in Microsoft Project		

	format shall be provided by the NG911 Service Provider to the County within ten (10) business days of comments received from the County regarding the initial plan submitted.		
4	PS004 Project Kickoff Meeting: The Project Kickoff meeting shall be held no later than fifteen (15) business days after issuing the Notice to Proceed. The NG911 Service Provider shall provide a detailed agenda and presentation of the Project Overview, Key Milestones, Key Benefits, Implementation Strategy, Operational, and Technical Resource requirements at this meeting at least five (5) business days prior to the Project Kickoff meeting. The NG911 Service Provider Technical Project Lead and Project Manager shall be onsite during this meeting.		
5	PS005 Weekly Project Calls: The NG911 Service Provider shall conduct weekly project calls. These project calls shall include an agenda before the meetings and cover, at a minimum, work to date, work for the next two (2) weeks, and any issues that may impact the project along with risk and mitigation actions to		

	address risk. The NG911 Service Provider PM should provide weekly written reports, distributed within 24 hours of the project call, that capture the minutes and action items from the call.		
6	PS006 Project Monthly Status Reports: PS006.a The NG911 Service Provider shall provide monthly progress reports before the 15th of the next month, until the equipment delivery milestone of the project. Weekly reports will be due following equipment delivery.		
7	PS007 Technical Project Lead: PS007.a The NG911 Service Provider shall identify a single Technical Project Lead. This person shall be the primary point of contact for technical issues and lead the technical aspects of the planning, design, installation, migration, and operation of the NG911 System. The County will review and approve the Technical Lead and, if the Technical Lead needs to be replaced, the County will review and approve the replacement.		
8	PS008 Client Services Representative:		

	PS008. a The NG911 Service Provider shall provide a Client Service Representative (CSR) after final acceptance. This person shall be the primary point of contact for all issues for the operation of the NG911 System for the period of performance. The County will review and approve the CSR and, if the CSR needs to be replaced, the County will review and approve the replacement.		
9	PS010 Staff CJIS Certification Requirements: All NG911 Service Provider's staff and subcontractors with access to the components of the NG911 System shall have a background check and Criminal Justice Information Services (CJIS) Level 1 basic security awareness certification. All staff that will be onsite at a County PSAP shall also have CJIS Level 4 advanced security awareness certification which requires Levels 1, 2, and 3 certifications.		
Equipment and Hardware			
1	SR-EH003 Onsite Equipment Requirements: All components installed by the NG911 Service Provider in the PSAPs		

	shall meet the following requirements:
	• All components shall be locally redundant at the hardware and software application layers
	• All hardware and software shall be:
	  – New not used
	  – Currently available on the open market
	  – Not identified as end of life by the manufacturer during the period of performance
	• All powered devices shall include a minimum of two redundant power supplies (each of which shall be able to power the device alone and which would be connected to separate circuits) OR be connected to a power-transfer device that allows a single power supply to be connected to two isolated power sources (i.e., circuits) with automatic, uninterrupted failover if the primary circuit fails		

	• Failure of any single instance of a hardware or software element or physical connection shall not negatively impact the overall System performance • All network-connected elements shall support at least two redundant network interfaces • Capacity to handle 50% growth without requiring the replacement of any hardware or software components • Voice and data circuits delivered from diverse providers to each call-handling host location • Must properly flag emergency services circuits and provide Telecommunications Service Priority (TSP) for repair and installation of voice and data circuits		
2	SR-EH004 Onsite Equipment Spare Parts: All spare parts for onsite equipment shall be located within Broward		

	County to allow the replacement of critical parts not functioning within the response times listed in the Service Level Agreements (SLAs). The NG911 Service Provider shall describe the process to determine which parts are needed, and how they are stored and replaced as needed. The NG911 Service Provider shall provide a list of all spare part inventory items maintained at the nearby facility within ten business days after installation for each environment.		
General System Requirements			
1	SR-GN002 NENA I3 Standard-Based Systems: SR-GN002.a All components and systems provided by the NG911 Service Provider shall be standards-based systems that comply with nationally accepted standards and requirements applicable to NG911 IP network architecture, security, and interface functionality, including the NENA i3 standards.		
2	SR-GN006 Multi-factor Authentication (MFA): MFA should be implemented for any access to externally accessible		

	portals, user interfaces (UIs), and functional elements of NG911 (e.g., Policy Routing Function [PRF] portal, reporting portal, system dashboards, etc.). The NG911 Service Provider shall describe the types of MFA (e.g., text, email, token, etc.) that will be used and the process to manage access and devices for the NG911 System proposed for the County.		
3	SR-GN007 Change Control Process: SR-GN007.a A formal change control process shall be documented for both scheduled and emergency changes with rollback procedures, notifications, and management approvals that are strictly followed by technicians to prevent unnecessary and/or uncontrolled changes from negatively impacting the 911 system in the County.		
4	SR-GN008 Implementation and Change Method of Procedure:		

	SR-GN008.a The NG911 Service Provider shall provide a step-by-step method of procedure (MOP) with a backout plan for review by the County a minimum of 60 calendar days prior to initial go-live for each PSAP and seven calendar days for all other changes.		
5	SR-GN010 All Changes Tested in Lab: SR-GN010.a The NG911 Service Provider shall test all new features, functions, equipment, and software (including patches and upgrades) in the lab environments before being deployed.		
6	SR-GN013 As-Built/System Documentation: SR-GN013.a Prior to beginning installation, the NG911 Service Provider shall provide an architecture diagram depicting the network and all components for the Regional and Non-Regional PSAP environments, detailed network design drawings reflecting the physical and virtual IP paths, all NG911 System components, and devices provided to		

	each PSAP, including what is provided by subcontracted last-mile providers and/or resellers. This documentation shall remain current for the contract period.		
7	SR-GN014 Not a First Application Site: The County does not want to be a first application site to introduce new applications, components, or features. The NG911 Service Provider shall use the new applications, components, and features in a production environment for at least 30 business days and provide documentation of the results before being provisioned in the County system.		
8	SR-GN015 Avoid PSAP Disruption: The NG911 Service Provider shall schedule all activities to avoid PSAP disruption or impacts to the County's PSAP operation for all changes. This includes onsite work as well as availability of systems. The NG911 Service Provider shall describe the process to prioritize, schedule, and		

	coordinate work with the County and PSAPs.		
9	SR-GN016 Terminate Legacy 911 components: The NG911 Service Provider shall manage the termination of the legacy systems at the direction of the County. The NG911 Service Provider shall describe the step-by-step process used in other implementations to speedily terminate legacy systems.		
10	SR-GN017 Spare Parts: SR-GN017.a Spare parts to restore service shall be located to allow the replacement of parts not functioning within the response times listed in the SLAs.		
11	SR-GN019 System and Network Time Changes: The NG911 Service Provider shall ensure that all software, firmware, functional elements, and components of the proposed NG911 System are configured to ensure that		

	there are no adverse impacts to the systems, software or the operation as a result of date and time changes.		
12	SR-GN020 Single Points of Failure: The NG911 Service Provider shall ensure there is no single point of failure in the design and implementation of the NG911 equipment and network within or outside of Broward County.		
13	SR-GN022 System Backups: The NG911 Service Provider shall maintain backups of the entire System and every associated component for the County with a minimum of two copies maintained at geo diverse sites. The NG911 Service Provide shall provide a copy of the proposed backup plan.		

14	SR-GN023 System Restoration: The NG911 Service Provider shall provide a documented restoration process for the NG911 System for the Regional and Non-Regional environments. A test run of the restoration process should be executed semi-annually. The NG911 Service Provide shall provide a copy of the proposed restoration plan.		
	Technical Requirements		
General Technical Requirements			
Security/Notification			
1	SN001 Network Operation Center (NOC)/Security Operation Center (SOC): SN001.a The NG911 provider shall provide a NOC/SOC staffed 24 X 7 X 365 to support for the proposed NG911 System for the County PSAPs.		
2	SN002 U.S.-Based Support: All access to the County systems shall be U.S.-based; there shall be no offshore remote access into the		

	systems installed within the County network for monitoring, general system administration, maintenance, or troubleshooting.		
3	SN003 All System Changes Tested: SN003.a All routine patches, updates, or new application software, hardware or configurations shall be tested in the lab environment before being put into production. Detailed reports of the testing shall be available to the County.		
4	SN004 All Systems Monitored: All networks, hardware, and software shall be monitored and have alarms to notify of out-of-normal operations.		
5	SN005 Edge Security: The NG911 Service Provider shall deploy Border Control Function (BCFs) at all network edges to		

	include intrusion detection and prevention Systems.		
6	SN008 Proactive Cybersecurity Analysis: The NG911 Service Provider shall perform proactive analysis of the network for vulnerabilities regularly. The NG911 Service Provider shall provide the frequency at which routine full and partial assessments are done.		
7	SN010 System Logging: SN010.a The NG911 Service Provider shall maintain logs of all changes made in the policy store with information of the user who made each change. The information logged should be available for up to one year with the option for the County to purge the logs on demand without additional costs.		
8	SN014 Meet Florida CS/HB 7055 (2022)		

	Cybersecurity Requirements: All cybersecurity on the systems used by the County shall meet Florida CS/HB 7055 Cybersecurity Operating Procedures Standard Operating Procedure (SOP) (following objectives stipulated as Florida Statute Section 282.3185, cited as the "Local Government Act" [any county or municipality]), which will be adopted as operating procedures and processes by the County.		
9	SN018 NENA NG-SEC Compliance: The NG911 Service Provider shall be NENA NG-SEC-compliant. The NG911 Service Provider shall provide a completed NENA NG-SEC compliance matrix.		
SR-IN 911 Call Ingress			
1	SR-IN002 OSP Integration: For the integration of all OSPs' connectivity for wireline, wireless, and VoIP traffic, as well as multiline		

	telephone systems (MLTSs), the NG911 Service Provider shall: • Coordinate with the County to obtain a letter of authority/agency • Establish interconnection, commercial agreements, and trunking • Provide interface control documents (ICDs) for all OSPs, CHE, and other third-party providers requiring ESInet connectivity • Coordinate with all telecommunications providers and manage circuit order processes, including testing and integration • Analyze current trunk engineering for 911 traffic and validate any trunk rebalancing for public-safety-grade service • Provide updates to the County on the migration status and interface types for all OSPs		

	The NG911 Service Provider shall provide proposed examples of OSP tracking and ICDs.		
2	SR-IN003 Multiple POIs: **SR-IN003.a** The NG911 Service Provider shall provide multiple POIs for OSPs both locally and nationally with a minimum of four POIs~~—at least two within Broward County. Having local and national POIs will provide OSPs with interconnection choices.~~ The NG911 Service Provider shall list the locations of all POIs that will be used.		
3	SR-IN004 OSP Connections to POIs: The NG911 Service Provider shall interconnect each OSP with at least two POIs for call receipt. POIs shall permit all OSPs to interconnect to more than two POIs for diversity at an OSP's discretion. The NG911 Service Provider shall describe the		

	process used to interconnect OSPs to the NGCS.		
4	SR-IN005 ALI Migration: The County is seeking a true NENA i3 system but understands that there will be some transitional steps. The NG911 Service Provider shall manage the ALI transition, including the following as needed: • Master Street Address Guide (MSAG) maintenance during the migration of OSPs • MSAG Conversion Service (MCS) • Service order input (SOI) process for subscriber records to include and moves, adds, and changes of ALI records • Integration and provisioning for MLTS databases • Pseudo automatic number identification (pANI) provisioning and shell records management • Coordination of all provider records from the legacy ALI database to the replacement		

	LDB and any dual provisioning necessary during the transitional phases of the project • Provide reporting for all data within the LDB via a web-based tool • Migration plan and migration to i3 call ingress The NG911 Service provider shall describe the step-by-step process used to accomplish all required items above.		
5	SR-IN006 Manage OSP Migration: The County is seeking a true NENA i3 system but understands that there will be some transitional steps. The NG911 Service Provider shall manage all adds, moves, changes, and deletions of connections to OSPs, both Time Division Multiplex (TDM) and IP-based; monitor these connections; and proactively work with the respective OSPs to resolve problems as they occur. The NG911 Service Provider shall provide weekly progress reports associated with the transition. Please describe the step-		

	by-step process used to accomplish this requirement.		
6	SR-IN007 Integrated Text to 911 The NG911 Service Provider shall integrate with the Text Control Center (TCC) to provide text-to-911 via the NG911 System, including the ability to process Real-Time Text (RTT), transfer text sessions, and bridge text sessions. Please provide a list of sites implemented with Text-to-911 with VIPER 7 CHE.		
SR-GI NG911 Processing			
1	SR-GI001 Governing GIS Standards: SR-GI001.a The NG911 Service Provider shall comply with all applicable NENA standards and technical documents pertaining to GIS, including but not limited to (in the event a standard is updated between authoring this document and release by the County, the latest version of the standard shall apply): • NENA Standard for NG9-1-1 GIS Data Model, NENA-STA-006.2a-2022		

	• NENA Standard for NG9-1-1 Additional Data, NENA-STA-012.2 2017 • NENA NG9-1-1 United States Civic Location Data Exchange Format (CLDXF) Standard, NENA-STA 004.1.1-2014 • NENA GIS and Data Collection Standards, NENA 02-014 • NENA Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI, NENA 71-501 • NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1, NENA-INF-014.1 2015 • NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping, NENA-STA-015.10-2018		
2	SR-GI002 GIS Datum: The NG911 Service Provider shall accept GIS data in the datum and projection used by the County. The		

	County currently maintains GIS data in World Geodetic System 84 (WGS84) (NG911 GIS data layers) and Florida State Plane North American Datum of 1983 (NAD83) for multi-use GIS data layers.		
3	SR-GI003 GIS Transformations and Projections: Transformations between datums require complex calculations and can seriously degrade the accuracy of the GIS data. The County shall retain oversight of all transformations and reprojection of GIS data. The NG911 Service Provider shall coordinate all datum transformations with the County and shall defer to the County on every transformation setting to ensure the most accurate transformation possible.		
4	SR-GI004 GIS Schema: The County will not update the native schema for any GIS dataset used by other applications or agencies within Broward County.		

	The NG911 Service Provider shall provide field mapping or Extract, Transform, Load (ETL) scripts required to convert the County's GIS data into the NG911 schema if needed.		
5	SR-GI005 GIS Data Validation Settings: The NG911 Service Provider shall make available to the County all validation settings; x, y cluster tolerances; topology tolerances; and all transformation pathways and shall notify the County prior to any changes in these settings or the validation process.		
6	SR-GI006 Legacy Location Data: The County has invested heavily in improving the GIS data necessary for the NG911 transition. The County certifies that as of the release of this RFP, the match rate between the County's GIS data and the legacy location tables meets or exceeds NENA recommendations. The NG911 Service Provider shall work with the		

	legacy Service Provider(s) to acquire ALI and MSAG records as necessary for NGCS GIS and legacy data validation as required by the NG911 Service Provider. The NG911 Service Provider shall assume all costs associated with legacy data acquisition.		
7	SR-GI007 Orphaned ALI Records: The NG911 Service Provider shall resolve orphaned ALI records (invalid civic address) with the ALI provider. The NG911 Service Provider understands that the County shall not be responsible for updating or deleting ALI records.		
8	SR-GI008 Transition-Related Costs: The NG911 Service Provider shall assume all costs associated with transitioning to geospatial call routing and location validation and shall plan for such costs in the original proposal. This includes GIS-based MSAG conversion and		

	maintenance during the transition period.		
9	SR-GI009 SI GIS Data Uploads: The County maintains GIS data in Esri file geodatabase format. The NG911 Service Provider shall accept Esri file geodatabase uploads from the County through the SI.		
10	SR-GI010 SI and NGCS Provisioning: The NG911 Service Provider shall include all tools necessary for the GIS data upload, validation, and publishing to the NGCS. This shall include licensing and maintenance fees (where necessary, not including Esri software already in use at the County) for the term of the agreement and migration to NG911.		
11	SR-GI011 Nonduplicative GIS Data: The County intends to continue maintaining a single set of GIS data for NG911 and the CAD system. The		

	NG911 Service Provider shall work with the County to ensure all fields necessary to support both applications are contained and maintained in the GIS dataset attribution tables. Where NG911 requirements contradict CAD requirements, CAD standards shall be considered (e.g., one-way streets versus drawing centerlines in the direction of increasing addresses).		
12	SR-GI012 Exception Codes: The NG911 Service Provider shall provide a means for applying a persistent exception code to non-critical errors so that the same are not included in discrepancy reports and do not adversely affect legacy data to GIS match rates.		
13	SR-GI014 SI Message Logging: The NG911 Service Provider shall provide and retain message logging of all SI transactions, success and failures, caller phone numbers, caller addresses, and date and time stamps for 30 days at a minimum.		

14	SR-GI015 GIS Database: The NG911 Service Provider's GIS database shall support updates from Esri geodatabases.		
15	SR-GI016 GIS Database Verification and Validation: The NG911 Service Provider's SI shall validate GIS database changes before they are implemented. Exceptions should be produced from the SI of any records that failed the validation process.		
16	SR-GI017 GIS Data: The NG911 Service Provider understands that all GIS data is the property of the County and none of the data shall be shared with anyone without the County's consent.		
DAT - Data Processing			
1	DAT001 GIS Upload: DAT001.a The NG911 Service Provider shall provide a user-friendly		

	method to upload GIS files as well as the data requirements from the County's GIS repository.		
2	DAT002 Alternate Routing Data: Routing configurations for all alternate routing plans and decisions may require additional GIS layers. The NG911 Service Provider shall provide a method to upload GIS files with clearly documented data requirements from the County's GIS repository. The NG911 Service Provider shall describe the upload process.		
3	DAT003 Data for the PRF: DAT003.a The NG911 Service Provider shall provide a process and portal to manage the PRF routing plans.		
4	DAT004 Call Handling Equipment Configuration Data: The NG911 Service Provider shall provide a process to manage the configuration data for the CHE		

	needed to implement and operate the NG911 System. The NG911 Service Provider shall describe the process to manage the configuration data for the CHE.		
5	DAT005 Routing and Configuration Data: The NG911 Service Provider shall provide a process to manage the configuration data from the NG911 systems needed by the CHE and other PSAP systems to interoperate on the NG911 System. The NG911 Service Provider shall describe the process to manage the configuration data from the NG911 System.		
SR-CR Call Routing			
1	SR-CR001 Legacy systems connectivity: The NG911 Service Provider shall coordinate and execute connectivity to legacy selective routers to support transfers to neighboring agencies not served by the County's or another NG911 System. The NG911 Service Provider shall describe how the connectivity will be accomplished and estimate how many legacy systems will need to be interconnected.		

2	SR-CR002 NG911 Systems Connectivity: SR-CR002.a The NG911 Service Provider shall coordinate and execute connectivity to all neighboring ESInets (i.e. Collier, Miami Dade, Palm Beach, Monroe, Orange, and Hillsborough counties) not served by the County's NG911 System to support i3 transfers to neighboring agencies and future backup plans.		
3	SR-CR003 Rules, Policies and Algorithms: SR-CR003.a The NG911 Service Provider shall provide all the rules, policies, and algorithms that will be available to route calls similar to the routing groups currently in place.		
4	SR-CR005 Credentialing: The NG911 Service Provider shall provide or acquire credentialing that will permit the exchange of data and calls with surrounding jurisdictions. Credentialing is an important component for interoperability with other systems. Some ways to accomplish this are:		

	• Capability to acquire certificates from a NIOC PCA-vetted Intermediate Certificate Authority (ICA) and ability to validate NIOC PCA Certificates for authenticity • Interoperate with the NIOC PCA for credentialing (vendor NIOC PCA implementation through its own ICA or a state or regional NIOC ICA) • Provide a system that utilizes certificate-based role authentication in accordance with the PCA outlined in NENA-STA-010.3 2021 and in deployment with the NIOC Certificate Policy • Support the authentication of roles using the certificate obtained from the NIOC PCA • Support credentialing with the Forest Guide and hierarchical ECRFs when integrated with state or adjacent NG911 systems		

5	SR-CR006 Call Routing Configurations: SR-CR006.a The NG911 Service Provider shall implement call-routing configurations, rules, policies, and algorithms to distribute calls to the two environments (Regional and Non-Regional) and multiple hosts, similar to the current distribution model.		
6	SR-CR007 Services, Applications, and/or Functional Elements Anticipated: The NG911 Service Provider shall provide the following NENA i3-compliant Functional Elements as part of the overall NG911 System: *SR-CR007.1 Legacy Network Gateway (LNG)/Legacy Selective Router Gateway (LSRG)* – An LNG provides a signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the i3 architecture. The LNG logically resides between the		

	originating network and the ESInet and allows i3 PSAPs to receive emergency calls from legacy originating networks. An LSRG provides an interface between a 911 selective router and an ESInet, enabling calls to be routed and/or transferred between legacy and NG911 networks. Both an LNG and an LSRG are transitional elements and are decommissioned once all legacy routing systems have transitioned to SIP-based traffic. *SR-CR007.2 Border Control Function (BCF)* – A BCF provides secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of sessions and media as well as other security mechanisms to		

	prevent deliberate or malicious attacks. *SR-CR007.3 Emergency Services Routing Proxy (ESRP)* – An ESRP provides a SIP proxy service that selects the next-hop routing within the ESInet based on location, service Uniform Resource Name (URN), and policy. The Originating ESRP receives calls from the BCF at the edge of the ESInet and one or more Intermediary ESRPs may exist that route to the Terminating ESRP. *SR-CR007.4 Policy-based Routing Function (PRF)* – A PRF stores Policy Routing Rules (PRRs) that are used by the ESRP to make policy-based call routing decisions in the delivery of a call to a PSAP. The PRF shall be used to dynamically modify call routing based on various conditions, including network state, PSAP state, caller		

		location, media type, and/or language preference. *SR-CR007.5 Emergency Call Routing Function (ECRF)* – An ECRF provides a Location-to-Service Translation (LoST) protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a Uniform Resource Identifier (URI) used to route an emergency call to the appropriate PSAP for the caller's location or to a responder agency. *SR-CR007.6 Location Validation Function (LVF)* – A LVF provides a LoST protocol server where civic location information is validated against the authoritative GIS database information. *SR-CR007.7 Spatial Interface (SI)* – The SI provides a standardized interface between the GIS		

	data and the functional elements that consume GIS data (i.e., ECRF, LVF, and mapping data service). *SR-CR007.8 Location Database (LDB)* – The LDB provides the current information, functionality, and interfaces of legacy 911's ALI database but can also use the new protocols required in an NG911 deployment. *SR-CR007.9 Network Time Protocol (NTP) and Time Source* – An NTP service synchronizes network time between servers, clients, and applications across a network. The time source provides consistent, credible, and accurate time synchronization to ensure system performance. This time shall also be synchronized with the internal CHE. *SR-CR007.10 Master Street Address Guide (MSAG) Conversion Service (MCS)* –		

	An MCS is a service that provides conversion between Presence Information Data Format – Location Object (PIDF-LO) and MSAG data. *SR-CR007.11 Network-to-Network Interface (NNI) to Other Neighboring NG911 Systems* – An NNI enables the interconnection and exchange of data between different distinct networks or NG911 systems typically operated by different service providers or organizations. An NNI allows disparate networks to seamlessly communicate with each other, facilitating the transmission of voice, data, and multimedia traffic. The NG911 Service Provider shall provide all services, applications, and functions as described above for the County, inclusive of all routing and call handling requirements outlined in the SOW.		

7	SR-CR010 Emergency Call Routing: SR-CR010.a The NG911 Service Provider shall implement call-routing configurations, rules, policies, and algorithms to change the distribution of calls to the two environments (Regional and Non-Regional) and multiple hosts for the emergency routing scenarios.		
8	SR-CR012 Overflow Notification: The NG911 System shall provide overflow notification to backup/alternate PSAPs that an incoming call is being routed to the alternate PSAP due to the primary PSAP(s) being unable to handle the incoming call load. The NG911 Service Provider shall describe what information will be displayed to the call taker with call delivery.		
SR-NR Network Redundancy and Resiliency			
1	SR-NR001 Redundant Circuits into the VIPER Load Balancers: The NG911 Service Provider shall provision two redundant circuits into		

	each location to terminate at the VIPER load balancers.		
2	SR-NR002 Redundant Circuits into the VIPER Servers: The NG911 Service Provider shall provision two circuits into two locations in each environment (Regional and Non-Regional) to terminate at the VIPER servers.		
3	SR-NR003 Diverse Power: All power shall be redundant and diverse (i.e., at least two separate circuits) with a UPS system and generator backup for each component of the NG911 System.		
4	SR-NR004 Diverse and Redundant Circuits: All voice and data circuits shall be redundant and delivered via diverse entrances into all facilities.		
5	SR-NR006 Maintain Active Calls: When the IP circuits between the NGCS and PSAPs fail for any reason during an active call, the voice or data shall failover to the redundant IP circuit without dropping the call.		
6	SR-NR008 Circuits Monitored:		

	SR-NR008.a All circuits shall always be monitored to ensure they are available when needed.		
NG911 Call Delivery			
SR-DL 911 Call Egress/Call Delivery to All PSAPs			
1	SR-DL002 NG911 Circuit Bandwidth: The NG911 Service Provider shall provide bandwidth to the CHE at each host to be capable of operating the entire system plus 25% growth. The NG911 Service Provider shall ensure that in the event of a failure of the ESInet or CHE, a single connection to a single host will be large enough to handle all traffic.		
2	SR-DL003 Interface to VIPER: The NG911 Service Provider shall interface the NGCS into the County's VIPER 7 platform to allow the NGCS and CHE to exchange routing and activity data, including all configurations and settings needed. The County's VIPER system includes the use of ACD and interactive voice response (IVR) capabilities. The NG911 Service Provider shall work cooperatively with the CHE vendor (Intrado) to interface and test these		

	connections and interconnect the NGCS to the CHE in each environment. The NG911 Service Provider shall provide a list of similar projects that interfaced with VIPER 7.		
3	SR-DL005 Policy-based Rules: SR-DL005.a The NG911 Service Provider shall provide a policy-based rules function and a user-accessible tool to manage the policy rule's function.		
4	SR-DL008 Early Media and Ring Back: To permit the functions in the VIPER, the NGCS shall support early media and ring back from the CHE. The NG911 Service Provider shall provide at least three other VIPER 7 implementations where the proposed NG911 System has been successful.		
5	SR-DL009 Early Media and Ring No Answer: The NG911 Service Provider shall coordinate configuration of the		

	Regional environment to include early media and ring no answer to not impact the ACD in use. The NG911 Service Provider shall provide at least three other VIPER 7 implementations where the proposed NG911 System has been successful.		
6	SR-DL010 Call Back and Bridging: The NGCS shall support the ability to call back 911 callers and to bridge the calls to various agencies within and outside of Broward County.		
7	SR-DL011 Call Back and Transfer: The NG911 Service Provider shall provide an Outbound Call Interface Function (OCIF) to permit the call back and transfer of calls. The NG911 Service Provider shall describe how this function has been integrated to VIPER 7 implementations to enable the transfer of calls to various agencies within and outside Broward County.		
8	SR-DL012 Bridging:		

	The NG911 Service Provider shall provide a bridging function that will allow the conferencing of at least five callers. The NG911 Service Provider shall describe how this function has been integrated to VIPER 7 implementations.		
9	SR-DL013 Legacy Selective Router Retirement: The NG911 Service Provider shall coordinate and execute plans to remove the legacy selective routers from the call delivery call flow to reduce future costs. The NG911 Service Provider shall describe the process used to accomplish this.		
10	SR-DL014 Call Delivery Monitoring and Notifications: SR-DL014.a The NG911 Service Provider shall monitor the processing of 911 calls through the Functional Elements of the NG911 System to the PSAPs.		
SR-AF Alternate Call Routing/Failure			

1	SR-AF001 Activation of Alternate and Failover Routing: The NG911 System provided by the NG911 Service Provider shall permit the activation of alternate and failover routing to, at a minimum, mirror the current County routing by using passive (e.g., CHE status, etc.) and active (e.g., abandonment switch) methods. The NG911 Service Provider shall describe the proposed methods to accomplish this requirement.		
2	SR-AF002 Regional Environment Failover: The NG911 System provided by the NG911 Service Provider shall support the activation of a Regional PSAP failover for a single PSAP or two PSAP failures with VIPER in service. Calls shall have tags or other methods of identification for the VIPER to be able to route the call appropriately. CAD failure scenarios will be managed by VIPER as it is now. The NG911 Service Provider shall describe the method of marking the calls and list other		

	locations where this has been accomplished.		
3	SR-AF003 Non-Regional Environment Failover: The NG911 System provided by the NG911 Service Provider shall support the activation of a Non-Regional PSAP failover for a single PSAP not functioning with VIPER in service; it will be managed by VIPER as it is now. Calls shall have tags or other methods of identification for the VIPER to be able to route the calls appropriately. The NG911 Service Provider shall describe the method of marking the calls, and list other locations where this has been accomplished.		
4	SR-AF004 Automatic Activation of Call Routing to the Other Environment: The NG911 System provided by the NG911 Service Provider shall permit the automatic activation of call routing from one environment to the other environment when VIPER in		

	one environment (Regional or Non-Regional) is unable to process 911 calls (e.g., no users logged in, equipment failure, manual switch, etc.). The NG911 Service Provider shall describe the method of accomplishing this requirement to include how the routing is signaled to the NG911 System from the PSAP and list where this has been implemented.		
5	SR-AF005 Activation of Call Routing to Other NG911 Systems: The NG911 System provided by the NG911 Service Provider shall permit the activation of call routing to other jurisdictions and can be implemented using interconnectivity to neighboring counties. The NG911 Service Provider shall describe the method of marking the calls and routing the calls to other jurisdictions and list other locations where this has been accomplished.		

6	SR-AF006 Legacy Selective Router Connectivity to Neighboring Agencies: The NG911 Service Provider shall coordinate and execute connectivity to legacy selective routers to support call transfers to neighboring agencies not served by the County's or other NG911 Systems. The NG911 System should support the use of star codes and provide the ability to modify star codes. A list of star codes will be provided by the County. The NG911 Service Provider shall describe how this requirement will be accomplished.		
7	SR-AF007 NG911 System Connectivity to Neighboring Agencies: The NG911 Service Provider shall coordinate and execute connectivity to neighboring NG911 systems to support call transfers and alternate routing to neighboring agencies not served by the County's NG911 System. The NG911 Service Provider		

	shall describe how this requirement will be accomplished.		
	Functional Requirements		
NG911 Call Delivery			
SR-CP Call Processing			
1	SR-CP001 Integrate with VIPER 7: The NG911 Service Provider shall integrate with VIPER 7 in both environments (Regional and Non-Regional).		
2	SR-CP001.1 Integrate with VIPER 7 in the Regional Environment: The NG911 Service Provider shall integrate with the VIPER 7 in the Regional environment to ensure that all current functions of VIPER continue to function, including the load sharing and ACD functions. The NG911 Service Provider shall describe how this is accomplished.		
3	SR-CP001.2 Integrate with VIPER 7 in the Non-Regional Environment:		

	The NG911 Service Provider shall integrate with the VIPER 7 in the Non-Regional environment to ensure that all current functions of VIPER continue to function, including the load sharing functions. The NG911 Service Provider shall describe how this is accomplished.		
4	SR-CP002 Data Supports VIPER 7 Functions: SR-CP002.a The NG911 Service Provider shall work cooperatively with the CHE vendor to ensure that the data provided meets the needs of the CHE to continue to provide all current functions. The NG911 Service Provider shall provide documentation on the configurations and data exchanges to the CHE vendor and work cooperatively to interconnect.		
SR-IT Interfaces			
1	SR-IT001 Interface Documentation: The NG911 Service Provider shall provide interface documentation on the configurations and data exchanges to the other interface vendors and work		

	cooperatively to interconnect. These include but may not be limited to: • Incoming POIs • Legacy Systems • Other NG911 Systems • PSTN, Wireless and VoIP systems • VIPER EIDO Server • TCC The NG911 Service Provider shall provide an example of interface documentation and list all interfaces that have been implemented from the proposed NG911 System.		
2	SR-IT002 Interfaces: The following interfaces are expected to be impacted by the NG911 implementation. For each interface, the NG911 Service Provider shall describe the process used to implement and test. *SR-IT002.1* Incoming POIs *SR-IT002.2* Legacy systems *SR-IT002.3* Other NG911 systems		

	SR-IT002.4 PSTN, wireless, and VoIP systems *SR-IT002.5* VIPER EIDO server *SR-IT002.6* *TCC*		
RPT - Reports			
1	RPT002 Reporting Platform PSAP Functions: RPT002.a The single reporting platform shall have a dashboard and portal for access by each PSAP manager, County staff, and others as approved by the County to run the below reports. All reports shall be able to be run for specific dates and times. These reports shall be able to run for specific PSAPs and be able to limit to specific PSAPs for specific users.		
	NG911 System Deployment		
Initial Deployment			
1	SD001 General Requirements: All installation and setup of hardware, software, and interfaces shall be completed without impact to PSAP operations. The NG911 Service		

	Provider staff shall ensure that all activities associated with this project are completed without disrupting PSAP daily operations. All work areas assigned to NG911 Service Provider staff must be maintained and kept in working order throughout the entire project.		
2	SD002 Site Survey: The NG911 Service Provider shall perform a site survey at each PSAP (South, Central, North, Coral Springs, Plantation, and EOC) within seven business days following the Project Kickoff meeting. During the site survey, the NG911 Service Provider shall: • Determine the interface cable lengths • Determine the power requirements • Determine hardware installation requirements at each PSAP—six (6) total • Provide a copy of the site survey, site summary, and recommendations within five (5) business days after		

	completion of all sites surveys and data gathering meetings. • Determine rack usage space at each PSAP—six (6) total Any recommended or remediation actions by the NG911 Service Provider shall be completed before beginning hardware installations. The NG911 Service Provider shall gather configuration and other data inputs for system design, configuration, and installation. The NG911 Service Provider shall gather this information by conducting onsite meetings within 14 business days of the Project Kickoff meeting with the County's E911 and Operation staff.		
3	SD003 Design Meetings: The NG911 Service Provider shall conduct onsite in-depth design session meetings with the County ORCAT E911 team to develop and formalize the NG911 system design.		

4	SD004 Design Specifications: SD004.a The NG911 Service Provider shall provide a design specifications document to the County. This document shall include the hardware, software, and networking required to implement the design requirements along with updated architecture diagrams. This document shall be reviewed by the County and approved by the County before being implemented.		
5	SD005 Implementation Strategy: The NG911 Service Provider shall provide an implementation strategy document for each environment (Regional and Non-Regional). The implementation strategy shall include a step-by-step implementation plan with specific locations of components. The implementation strategy shall be cooperatively developed with the County. This document shall be reviewed by the County and		

	approved by the County before being implemented.		
6	SD006 NGCS Preparation and Configuration: The NG911 Service Provider shall configure the hardware and software required for the NG911 System in accordance with the agreed-to design document.		
7	SD007 Engineering and Ordering of IP Circuits as Necessary: The NG911 Service Provider shall design, order, and implement IP circuits to the various required PSAPs and POIs.		
8	SD008 Procurement and Pre-configuration of Equipment to be Installed at the PSAPs: The NG911 Service Provider shall procure and pre-configure equipment to be installed at the PSAPs.		

9	SD009 Site Preparation and Circuit Delivery: The NG911 Service Provider shall prepare the site and deliver the circuits into the PSAPs.		
10	SD010 Equipment Delivery to the PSAPs: The NG911 Service Provider shall be responsible for the delivery and installation of the equipment. The County is not responsible for equipment shipped to a County facility. The equipment to be installed at the PSAPs will need to be shipped to a location for the NG911 Service Provider to access and then install at each PSAP.		
11	SD011 Installation at the Regional PSAPs: The NG911 Service Provider shall install the required equipment at the Regional PSAPs.		

12	SD012 Connectivity between the PSAP and NGCS at the Regional PSAPs The NG911 Service Provider shall interconnect, configure, and test the Regional PSAP installed equipment to communicate with the NGCS data centers.		
13	SD013 Configuration of the CHE and Other Interfaced Systems at the Regional PSAPs: The NG911 Service Provider shall interconnect the NG911 components to the Regional CHE that receives call data and are both configured to receive new data.		
14	SD014 Installation at the Non-Regional PSAPs: The NG911 Service Provider shall install the required equipment at the Non-Regional PSAPs.		
15	SD015 Connectivity between the PSAP and NGCS at		

	the Non-Regional PSAPs: The NG911 Service Provider shall interconnect, configure, and test the Non-Regional PSAP installed equipment to communicate with the NGCS data centers.		
16	SD016 Configuration of the CHE and Other Interfaced Systems at the Non-Regional PSAPs: The NG911 Service Provider shall interconnect the NG911 components to the Non-Regional CHE that receives call data and are both configured to receive new data.		
Testing			
1	TS001 System Testing: NG911 System Testing confirms that the new NG911 System has been installed and configured as requested by the County. This testing is performed by the NG911 Service Provider prior to the commencement of the Preliminary Acceptance Testing. The NG911 Service Provider		

	shall provide the County with the System Test plan 60 calendar days prior to testing and written testing results within five calendar days of completion.		
2	TS002 Preliminary Acceptance Testing (PAT): Preliminary Acceptance Testing will allow the County to verify all configuration requirements, interfaces, and functional specifications. Preliminary Acceptance Testing will be conducted by the County and commence immediately after installation and notification by the NG911 Service Provider that the system has successfully passed System Testing, coupled with the actual test results. The County will develop a comprehensive test plan and strategy with consultation and onsite meeting participation from the NG911 Service Provider's designated technical project lead. The NG911 Service Provider shall provide written notification that the system is ready for Preliminary Acceptance Testing.		

	The NG911 Service Provider shall provide the onsite technical lead and project manager during the entire Preliminary Acceptance Testing- allocated time to ensure that issues are resolved in a timely manner.		
3	TS003 Provide Test Environment: The NG911 Service Provider shall provide access to the NG911 System in a testing environment. This should be the actual hardware and software that is not interconnected to the live environment.		
4	TS004 Final Acceptance Testing (FAT): Final Acceptance Testing shall be performed by NG911 Service Provider resource(s) and the County. The NG911 Service Provider shall be responsible for resolving any issues encountered during this phase. After successful Preliminary Acceptance Testing and Go-Live, the County shall conduct Final Acceptance Testing		

	alongside NG911 Service Provider personnel. Final acceptance will not be granted until the respective PSAPs operates for sixty (60) calendar days without encountering Severity Level 1-through-Level 3 events on the NG911 System. If a Severity Level-1-through-3 event occurs, the 60 calendar-day period shall restart from the successful resolution of the event.		
Go-Live and Post Go-Live			
1	GL001 Go-Live (Cut Over): GL001.a Cutover shall occur after the successful completion of Preliminary Acceptance Testing. The NG911 Service Provider technical lead and project management resources shall be onsite during this phase. The NG911 Service Provider shall provide a cutover plan (i.e., MOP) a minimum of 60 calendar days prior to the Go-Live for each PSAP to allow the County time to review and approve. The plan must be a step-by-step event plan with every activity along		

	with the expected duration of each activity. • The NG911 Service Provider will coordinate all required parties for the cutover • PSAP and County representatives will make the final determination to back out or tentatively accept the Go-Live. • The County reserves the right to determine when a backout procedure is initiated.		
2	GL002 Go-Live by Environment: The NG911 Service Provider shall perform cut over for each environment (Regional and Non-Regional) separately. After the Regional PSAPs are cut over successfully, the NG911 system will be in place for a period to be determined by the County. The County will notify the NG911 Service Provider when the Non-Regional PSAP cut over may occur.		

3	GL003 Post Go-Live Support: The NG911 Service Provider shall provide onsite and remote support during the post Go-Live period to meet all SLAs. For up to the first 15 business days, support shall be onsite for the Regional and Non- Regional environments. This period may restart at the discretion of the County if there are any issues during the post Go-Live period.		
Training			
1	TRN001 Train-the-Trainer Training: The NG911 Service Provider shall provide minimum three onsite train-the-trainer training sessions of up to fifteen (15) people per session on the dashboard/portal, PRF, incident reporting, ticketing tools, and other provided interfaces and applications to County staff.		
2	TRN002 Dashboard/Portal Training: The NG911 Service Provider shall provide minimum three onsite user		

	training sessions on the dashboard/portal to County and PSAP staff.		
3	TRN003 GIS Tool Training: The NG911 Service Provider shall provide minimum one onsite training session on the GIS tools provided.		
4	TRN004 Incident Reporting and Ticketing Tool Training: The NG911 Service Provider shall provide minimum three onsite training sessions on incident reporting, the retrieval of service request data, and ticketing tools.		
5	TRN005 PRF Management Training: The NG911 Service Provider shall provide minimum two onsite training sessions on PRF management.		
6	TRN006 Change Management Training: The NG911 Service Provider shall provide minimum one onsite training session on change management		

	requests, processes, and tools, including SOI updates and ALI discrepancy procedures.		
7	TRN008 Training Materials and Curriculum: TRN008.a Training materials and curriculum shall be provided minimum 60 business days prior to the respective training.		
	Maintenance and Support Requirements		
Maintenance and Support			
1	SR-MR001 Maintain Compliance with the Current Industry Standards: As industry standards evolve, the NG911 System shall be upgraded to maintain compliance with the current version of established industry standards. The NG911 System should support applicable new IP network and security industry standards within twenty-four (24) months of ratification. Compliance requirements apply to the supporting standards referenced within each standard. As updates are made to maintain compliance, the NG911 System shall not abandon services or		

	feature functionalities in place at the time of the upgrade. The NG911 Service Provider shall uncover any performance or feature changes prior to the upgrade and report them to the County for approval. The NG911 Service Provider shall describe the process used to identify, develop, test, and implement new standard components, functions, and applications.		
2	SR-MR003 Configuration Management: The configuration management process shall include the following: • Frequency of scheduled software releases and the decision-making processes involved in determining what features and defect resolutions to include in a scheduled release. • Maintenance releases and feature releases shall be provided to the County at no cost while a maintenance agreement is in place. The NG911 Service Provider shall describe the frequency of defect-resolution software		

	releases, and the decision-making processes involved in selecting which software defects to fix. • The NG911 Service Provider shall provide access to the defect tracking system to allow the County to track the progress of defect resolutions. • The NG911 Service Provider shall provide a detailed description of the defect tracking and resolution process and provide training to County staff prior to final NG911 System acceptance. • The NG911 Service Provider must have a procedure to manage and track changes made to the system. This is especially important when changes affect the performance of a particular device that needs to be returned to its former configuration. The configuration management procedure shall be available		

	to maintenance personnel and County staff. The NG911 Service Provider shall describe the process used or provide example notifications and procedures.		
3	SR-MR006 Manage OSP Moves, Adds, and Changes: The NG911 Service Provider shall manage all adds, moves, changes, and deletions of connections to OSPs, both TDM and IP-based, in accordance with the Federal Communications Commission (FCC) Report and Order Facilitating Implementation of NG911 Services (FCC 24-178); monitor these connections; and proactively work with the respective OSPs to resolve problems as they occur. The NG911 Service Provider shall describe the process used to accomplish this requirement.		
4	SR-MR007 Legacy System Monitoring: After completion of Final Acceptance Testing, the legacy systems shall remain in place for at least 30 additional days. The legacy systems shall be monitored from Go-Live to ensure no traffic is processed by the		

	legacy systems. If traffic is processed by the legacy systems, the NG911 Service Provider shall troubleshoot and identify the OSP and migrate the traffic to the NG911 System, and the 30-day period will begin again.		
5	SR-MR008 Removal of Legacy Systems and Circuits (Move to Maintenance and Support): After 30 days of no traffic, the NG911 Service Provider shall manage the termination of the unused legacy systems and circuits. The NG911 Service Provider should coordinate the removal of unused equipment from the PSAPs.		
6	SR-MR010 Scheduled Maintenance: The NG911 Service Provider shall coordinate all scheduled maintenance using the change management process. This shall include: • Scheduled downtime • Preventative maintenance		
7	SR-MR011 Mandatory Meetings:		

	The NG911 Service Provider shall attend the following meetings with the County in person: • Executive Meetings – Semi-annual to review performance with the NG911 Service Provider's executive team. • Performance Review Meetings – Monthly or quarterly to review performance.		
8	SR-MR012 GIS Maintenance: The NG911 Service Provider shall provide a method to upload regularly scheduled County GIS data updates to the NGCS with clearly documented data requirements. The NG911 Service Provider shall describe the process.		
Service Level Expectations			
1	SR-SLA001 Availability: The NG911 Service Provider shall maintain 99.999% availability for all components of the NG911 System for each PSAP. Availability will be calculated by the total downtime at the PSAP divided by the total available time per month.		

2	SR-SLA002 Equipment and Support Staff Availability: The NG911 Service Provider shall maintain adequate equipment including spares, and trained staff available remotely and/or onsite as required 24/7/365 to resolve issues and failures within the response and resolution times outlined in the SLA in Tables 1 and 2 shown in Scope of Work document. The NG911 Service Provider shall list the locations where equipment and staff will be located during the terms of the contract.		
3	SR-SLA003 Response and Resolution Times: SR-SLA003.a The NG911 Service Provider shall resolve all issues and failures within the agreed upon response and resolution times.		
4	SR-SLA004 Supply Chain: Due to events with the pandemic, the County seeks confirmation that any committed plan and/or schedule communicated within the NG911 Service Provider's response should be maintained regardless of supply chain impacts. The NG911 Service Provider shall describe processes put		

	in place to limit the impact of supply chain issues.		
5	SR-SLA005 Reason for Outage and Root Cause Analysis (RCA): SR-SLA005.a After any issues are reported, the NG911 Service Provider shall provide a preliminary reason for outage (RFO) and restore service immediately through failover options. The final RFO/RCA report shall include detailed outage causation, callers impacted, duration of outage, date and time of the outage, and any short- and/or long-term countermeasures implemented to prevent a recurrence.		
6	SR-SLA006 RFO/RCA Follow Up: RFO/RCA reports that include any short- and/or long-term remedies, including implementation schedules, shall include follow-up reporting. The County shall be notified by the NG911 Service Provider regularly (at minimum daily or weekly until fully resolved) and as actions are completed.		
Final Acceptance Criteria			
1	FAC001 Final Acceptance:		

	After successful Preliminary Acceptance Testing and Go-Live, the County shall conduct Final Acceptance Testing alongside NG911 Service Provider personnel. Final acceptance should not be granted until the PSAPs in both Regional and Non-Regional environments operate for 60 calendar days without encountering Severity Level 1 through Level 3 events on the NG911 System. If a Severity Level 1 through Level 3 event occurs, the sixty (60) calendar-day period shall be restarted from the successful resolution of the event.		

The information on this Project Questionnaire remains subject to County review and verification during the evaluation process.

Functionality Checklist
Next Generation 911 (NG911)

INSTRUCTIONS: Respond to each requirement with the appropriate selection by indicating a "**Yes**" under the "Complies" column if the proposed solution "Complies" with the requirement as stated and the information requested is also provided, or indicate a "**Yes**" under the "Comply with Exception" column if the proposed solution "Comply with Exception" and provide details of the exception to the stated requirement under the "Comments" column or indicate a "**Yes**" under the "Does Not Comply" column if the proposed solution "Does Not Comply" for each requirement in this document. If the comment is lengthy, please use a separate page and reference the Item Number before each response.

Insert Vendor Name:

	NG911 System	Complies (All requested information associated with the requirements below must also be provided)	Comply with Exception	Does Not Comply	Comments (Associated with requirements noted below as "Comply with Exception")
No.	**NG911 Service Provider Requirements**				
	Technical Requirements				
General Technical Requirements					
SN - Security/Notifications					
1	SN009 STIR/SHAKEN: The NG911 Service Provider should implement STIR/SHAKEN and pass information including attestation to the CHE. The NG911 Service Provider shall describe how this has been accomplished in other locations with VIPER 7.				
2	SN010.b The NG911 Service Provider should provide transactional logging information for each functional element (i.e., Emergency Services Routing Proxy [ESRP], Legacy Network Gateway [LNG], BCF, PRF, Location Validation Function [LVF], Legacy Selective Router Gateway				

	[LSRG], Spatial Interface [SI], and Emergency Call Routing Function [ECRF]). The transactional database logs for 911 calls should include calling number, SIP header information, routing destination, call or record process success/failures, transfers, ALI database transactions, and alternate routing, which includes call counts. The log retention period should be a minimum of thirty (30) calendar days.				
3	SN011 System Logging Repositories: The NG911 Service Provider should provide transactional logging repositories at two different data centers for each functional element (i.e., ESRP, LNG, BCF, PRF, LVF, LSRG, SI, and ECRF). The log retention period should be a minimum of thirty (30) calendar days.				
4	SN012 System Log Retrieval: The NG911 Service Provider should provide a user-friendly portal to retrieve transactional logs in near real-time for each functional element (i.e., ESRP, LNG, BCF, PRF, LVF, LSRG, SI, and ECRF). The NG911 Service Provider should provide a process to retrieve the logs.				
5	SN013 Security Information and Event Manager (SIEM): The NG911 Service Provider should integrate with the County's SIEM Splunk Tool (when deployed) for onsite logging events. The log retention period should be a minimum of 30 calendar days. The NG911 Service Provider should provide the County access to the logs of other systems and devices in the NG911 System for tracking the calls and issues. The log retention period should be a minimum of thirty (30) calendar days.				

6	SN017 User Notifications and Communications: The NG911 Service Provider should have a system that performs outward notifications and updates of customer tickets through phone, email, and text. The NG911 Service Provider shall notify the County via the contact methods provided of all NG911 Service Provider infrastructure failures and/or outages within 15 minutes of discovery. For all outages, the NG911 Service Provider must also contact the 911 Coordinator via phone.				
7	SN020 TDOS and DDOS Prevention: The NG911 Service Provider should implement hardware, software, and training to identify, respond, and prevent TDOS and DDOS attacks as a part of the proposed NG911 System. The NG911 Service Provider shall describe the process to identify respond and prevent TDOS and DDOS attack.				
SR-IN 911 Call Ingress					
1	**SR-IN003.b The NG911 Service Provider should provide at least two POIs within 100 miles of the Broward County border. Having local and national POIs will provide OSPs with interconnection choices.** **The NG911 Service Provider shall list the locations of all POIs that will be used.**				
SR-GI NG911 Processing					
1	SR-GI013 SI Provisioning:				

	The NG911 Service Provider should pull GIS data from the County GIS data repository rather than require the County to push (upload) GIS data to the SI. The data pull can be automated by the NG911 Service Provider or scheduled by the County. The NG911 Service provider shall describe the process used and how the County's preference can be integrated into the proposed NG911 System.				
DAT – Data processing					
1	DAT001.b The NG911 Service Provider should describe the GIS upload process to include the access, steps, and ease of use.				
2	DAT003.b The NG911 Service Provider should describe the process to manage PRF routing plans.				
SR-CR Call Routing					
1	SR-CR003.b The NG911 Service Provider should work with the County to design all the rules, policies, and algorithms that will be available to route calls similar to the routing groups currently in place. Describe how this process will be accomplished.				
2	SR-CR004 Distribution of Calls to PSAPs: The NG911 Service Provider should route calls similar to the routing groups currently in place, including call labels/tags required by the CHE for various call functions and distribution rules currently in place. The NG911 Service Provider should describe the method that is proposed to route calls similar to the routing groups currently in place, such as additional circuits, call labels/tags, or setting distribution rules.				
3	SR-CR006.b All calls should be routed based on data received. The NG911 Service Provider should develop procedures and processes to distribute				

	calls to the hosts in the Regional and Non-Regional environments. Please provide examples of how this was done for other implementation.				
4	SR-CR008 Regional PSAP Routing: The CHE has been implemented to provide advanced routing capabilities. These capabilities are expected to remain. Regional PSAP routing should include: • Ability for all calls to be load-balanced across the three hosts similar to how it is balanced today • Ability for the VIPER load balancers to distribute calls to the VIPER servers regardless of the proper PSAP • Ability for the VIPER CHE to distribute calls to all PSAPs regardless of the proper PSAP • Ability of the VIPER CHE to identify the proper PSAP and distribute to the proper PSAP when needed (CAD failure operations) The NG911 Service Provider should describe the system that is proposed and how these capabilities will be accomplished.				
5	SR-CR009 Non-Regional PSAP Routing: Non-Regional PSAP routing should include: • Ability for all calls to be load-balanced across the three hosts similar to how it is balanced today • Ability for the VIPER load balancers to distribute calls to the VIPER servers regardless of the proper PSAP				

	• Ability for the VIPER CHE to distribute calls to the proper PSAP The NG911 Service Provider should describe the system that is proposed and how these requirements will be accomplished.				
6	SR-CR010.b The NG911 Service Provider should develop procedures and processes to distribute calls to the hosts in each environment for the following predetermined emergency scenarios at a minimum: • Loss of primary route to a host load balancer • Loss of primary and secondary route to a host load balancer • Loss of all routes to a single host in a single environment • Loss of all routes to two hosts in a single environment • Abandonment of a PSAP • Abandonment of a single PSAP with transfer to another environment • Abandonment of two PSAPs with transfer to another environment • Loss of single environment • Use of out-of-county PSAPs as backup PSAPs The NG911 Service Provider should describe how each scenario above can be processed by the proposed system with limited or no human intervention.				
7	SR-CR011 Geofencing: Geofencing and routing calls to specific call takers/positions/queues/ring groups are needed as part of the County's requirements. The NG911 Service Provider should ensure selected positions, PSAPs, or resources can be dynamically removed from receiving non-				

	incident/event 911 calls. The NG911 Service Provider should describe the process, signaling, or tagging that would be used in the proposed NG911 System to accomplish this requirement.				
SR-NR Network Redundancy and Resiliency					
1	SR-NR007 All Circuits Used: To ensure all connectivity is always available, all primary circuits should be used in normal operation to process traffic. Secondary and tertiary circuits should be active daily. The active secondary and tertiary circuits will demonstrate that the circuits are available and can support live traffic. The NG911 Service Provider should describe the method that will be used to accomplish this requirement and describe any types or specific circuits that may not be used in normal operation and why.				
2	SR-NR008.b The NG911 Service Provider should describe the monitoring methods and the process to provide notifications to the County when circuits are unavailable.				
NG911 Call Delivery					
SR-DL 911 Call Egress/Call Delivery to All PSAPs					
1	SR-DL001 Call Egress/Call-Delivery Circuits: The NG911 Service Provider should provide the call egress/call-delivery circuits and associated infrastructure to meet the following requirements: • Diverse entrance facilities for core sites • Diverse entrance facilities to all call-handling host locations that the County deploys, whether local, remote data center, or cloud-based • No single point of failure • Use open standards • IPv4 and IPv6 dual protocol stacks				

	• Border Gateway Protocol (BGP) utilizing bidirectional forwarding detection • Multicast routing and switching • Quality of service (QoS) marking using Differentiated Service Code Point (DSCP) to ensure the highest voice quality for all 911 calls • Have a network traffic convergence of less than 54 milliseconds (ms) • Maintain an MOS of 4.0 or better at the handoff to the CHE				
2	SR-DL004 Abandonment Switches: The NG911 Service Provider should provision one or more abandonment switches at each PSAP, which, when activated, will automatically reroute calls to the pre-defined alternate endpoint for that PSAP based on the required routing configurations used today. Strict administrative policies and procedures will be put in place by the County. The NG911 Service Provider should describe how abandonment switches will be used in the proposed NG911 System.				
3	SR-DL005.b The NG911 Service Provider should describe the functions of the policy based rules tool and types of rules that can be provisioned by the PSAP, County, and NG911 Service Provider.				
4	SR-DL006 Emergency Incident Data Object (EIDO): The NGCS and ESInet should support the exchange of EIDO over the ESInet between PSAPs and across NNIs to neighboring jurisdictions. The NG911				

	Service Provider should describe any actions by the County or CHE vendor to accomplish this requirement.				
5	SR-DL007 EIDO Access: The NGCS and ESInet should support access from other jurisdictions to the EIDO message servers deployed in the County's Regional and Non-Regional environments to exchange data. The NG911 Service Provider should describe any actions by the County or CHE vendor to accomplish this requirement.				
6	SR-DL014.b As part of the call delivery monitoring, the following situations should result in a trouble ticket being generated automatically for dispatch and resolution, and a notification to the County: • Call delivery between Functional Elements causes an error processing should generate an alarm. • When all calls are not able to be delivered to the PSAP, the NG911 Service Provider generates an alarm and notifies the appropriate parties at the County as well as the field personnel to confirm that alternate routing is activated. • When there is a failure to deliver the 911 call, the alternate call routing plans are automatically used to route the calls. In the event the NG911 alternate routes are not available, the calls are routed to an alternate public switched telephone network (PSTN) path				

	using a 10-digit number associated with the destination PSAP. If the primary path is unavailable, the calls should be routed to the backup 10-digit number. The logging of such routing should be available to the County. The NG911 Service Provider should provide examples of how these will be managed and performed in the proposed solution.				
7	SR-DL015 Call Queuing: The NG911 Service Provider should provide call queuing at the network level. If the network is unable to deliver the calls to the PSAP due to increased volume, the calls should be queued and tracked at the network level. The NG911 System should be able to process two hundred (200) calls simultaneously for each environment (Regional and Non-Regional).				
	Functional Requirements				
NG911 Call Delivery					
SR-CP Call Processing					
1	SR-CP003 Call Processing by Type: The NG911 Service Provider should be able to process and deliver wireline, wireless, VoIP, text (RTT, Short Message Service [SMS], Rich Communication Services [RCS], Message Session Relay Protocol [MSRP], Instant Messaging [IM]), and Multimedia Service (MMS) calls/requests for emergency response seamlessly. The system should support the use of Telecommunications Device for Deaf (TDD) and TTY.				

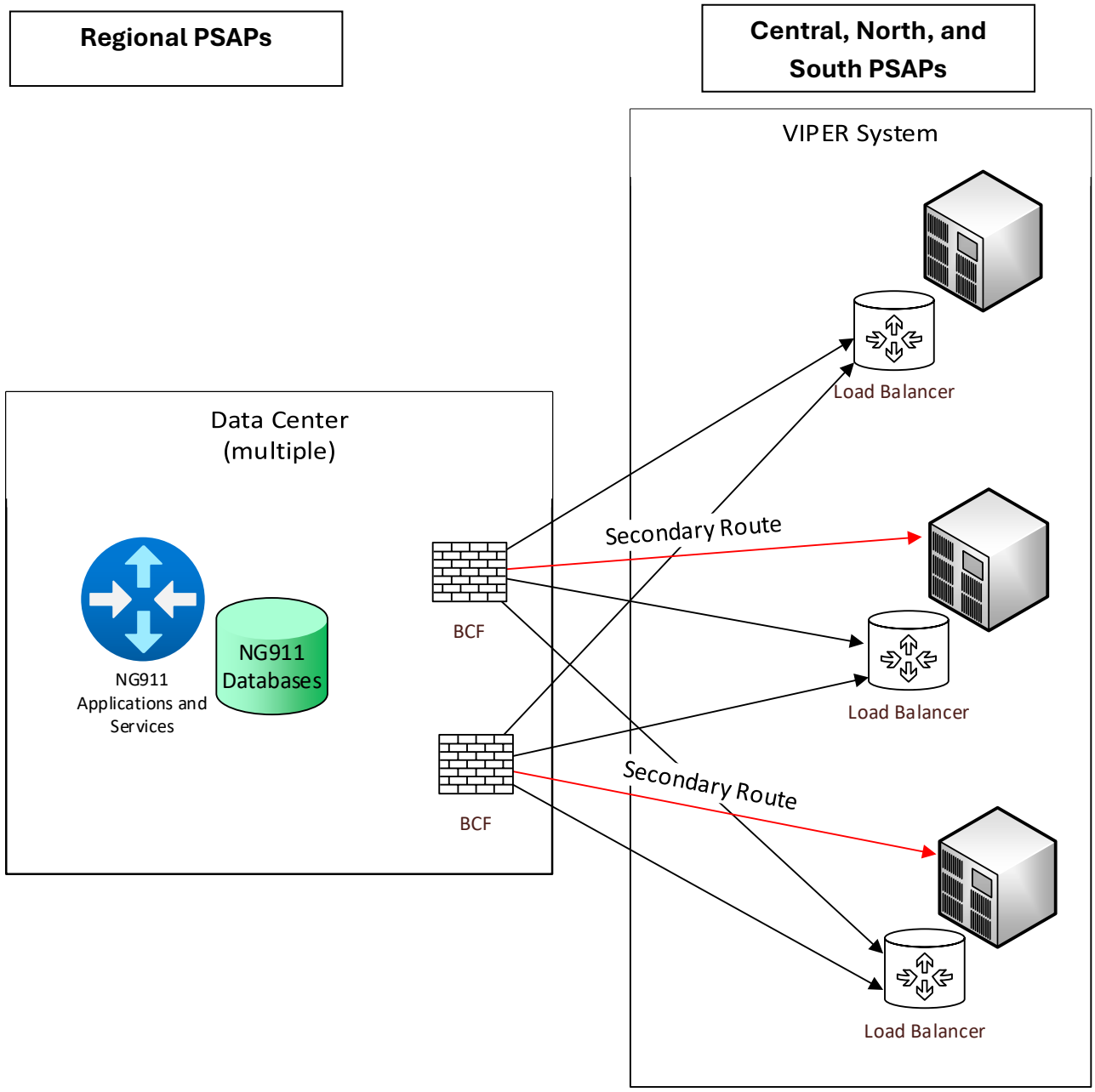
2	SR-CP004 Caller Location Information: The NG911 Service Provider should provide the location information for each 911 call at the handheld device-level for call routing and call processing.				
3	SR-CP005 NGCS Media Recording: The NG911 Service Provider should provide call and media recording in the NGCS. The PSAP and other County staff should have access to the recordings.				
SR-IT Interfaces					
1	SR-IT003 Multimedia Sessions: The NG911 Service Provider should interface the wireless providers to be capable of delivering multimedia such as video and pictures as a part of the proposed NG911 System. Deployment of this function to the PSAP will be determined on an individual PSAP basis.				
RPT - Reports					
1	RPT001 Single Reporting Platform: The NG911 Service Provider should provide a single reporting platform that can be configured based on each user's role, unique USERID, and access permissions. The portal should support at least sixty (60) users.				
2	RPT002.b The reporting platform for the PSAPs should include, at a minimum the following reports: • Date and time stamp • Call delivery time (hh:mm:ss) • Call answer time (hh:mm:ss) • Call disconnect time (hh:mm:ss)				

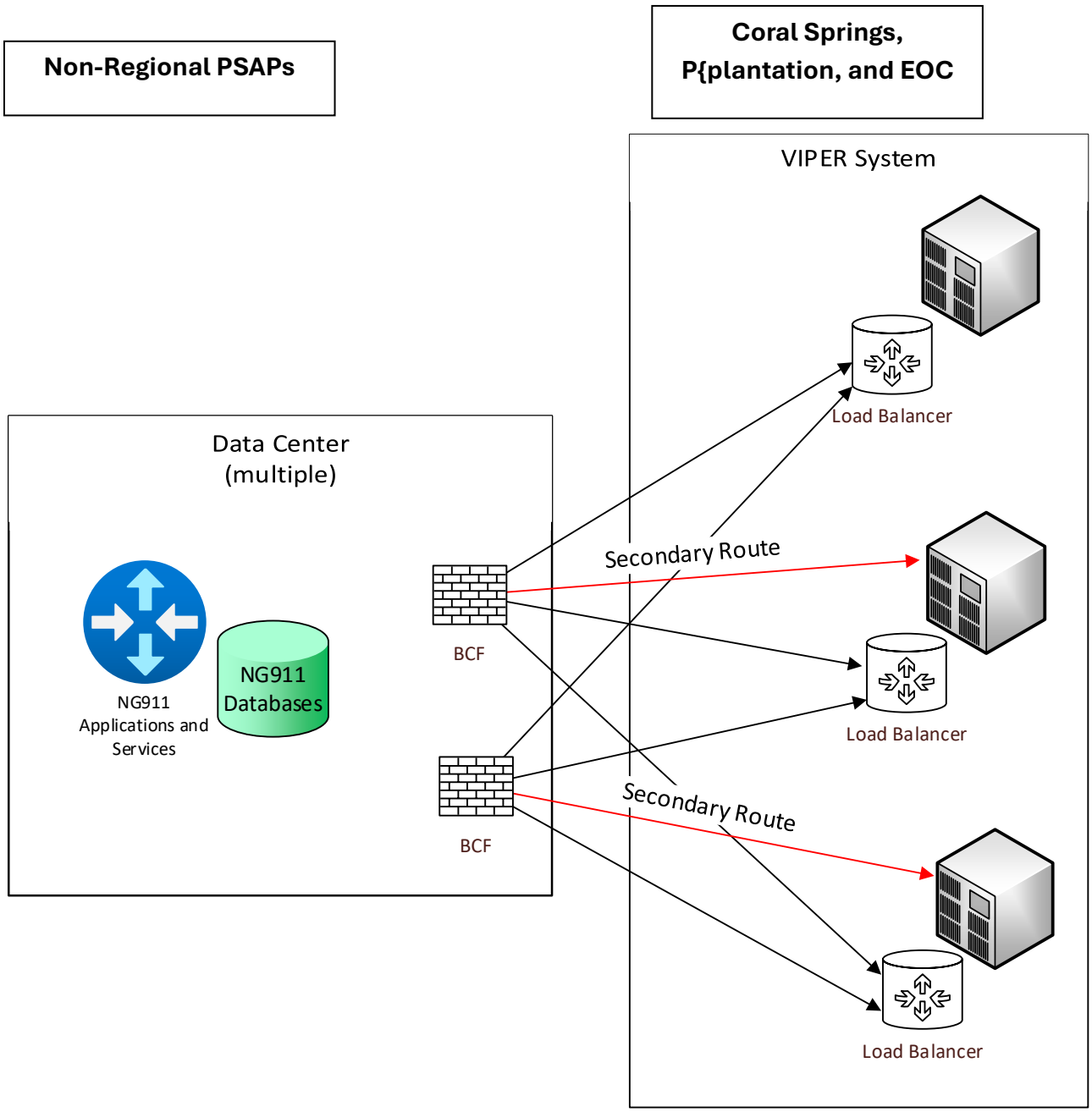
	• Call duration (hh:mm:ss) • Average call duration (hh:mm:ss) • Average call answer time (hh:mm:ss) • Seizure time (hh:mm:ss) • Call volumes by call type • Alternate-routed calls • Text-to-911 instances • Abandoned calls • Call volume by hour • Call volume by day of the week • Individual call information • Summary of call volumes • Call transfers/bridges • Call conferences • Agent availability • Call volumes by OSP • Repeat callers • Routing method (e.g., geospatial, Federal Information Processing Standard [FIPS]/emergency service number [ESN], default, etc.) The NG911 Service Provider should provide a list of all available reports and provide at least three report examples.				
3	RPT003 Reporting Platform County Staff Functions: RPT003.a The NG911 Service Provider should provide a dashboard and portal for access by County staff and others as approved by the County to run the below SLA reports. All reports should be able to run for specific dates and times.				
4	RPT003.b The reporting platform for County staff should include at a minimum:				

	• Call processing time between elements (hh:mm:ss) • Payload processing time (hh:mm:ss) • Calls per circuit • Call distribution to PSAP circuits • Circuit utilization from OSP • Circuit utilization to PSAP • All NGCS element usage volumes (all elements used in the NG911 Service Provider's NG911 System) • End-to-end call-flow analysis • Event by incoming IP address • NOC-to-NOC reporting, trouble reporting, and tracking • Root cause analyses • Service availability for each component including ESInet segments • Monitoring, alarming, and logging • MOS The NG911 Service Provider should provide a list of all available reports and provide at least three report examples.				
5	RPT004 Access to logs via Reporting Platform: The NG911 Service Provider should provide access to the system logs using the existing platform or another similar platform. This should include: • Transactional database log associated with each SIP header and URI, and additional information provided to access by the County				

	• Retrieval of log information should include calling number, SIP header information, call destination, successful, failures, transfers, ALI database transactions, and alternate routed calls (e.g., default, PSTN gateway, special processing, or overflow), which includes call counts • Log retrieval should be available by groups of calls (e.g., 911 versus non-emergency) and date range of calls.				
6	RPT005 Real Time System Monitoring: The NG911 Service Provider should provide access to real time system monitoring to the County using the existing platform or another similar platform. The platform should provide real time web-based monitoring of County traffic into the System at the functional element level and facilities (network connections). The status should be updated every 15 seconds, which includes, active, slow response, and failures.				

The information on this Functionality Checklist remains subject to County review and verification during the evaluation process.


Regional PSAPs
Central, North, and South PSAPs
VIPER System
Data Center (multiple)
NG911 Applications and Services
NG911 Databases
BCF
BCF
Secondary Route
Secondary Route
Load Balancer
Load Balancer
Load Balancer


Non-Regional PSAPs
Coral Springs,
P{plantation, and EOC
VIPER System
Load Balancer
Data Center
(multiple)
Secondary Route
NG911
Databases
NG911
Applications and
Services
BCF
Load Balancer
Secondary Route
BCF
Load Balancer

PURCHASING DIVISION
broward.org/Purchasing
BPRO Electronic Procurement System

Addenda No.: **2**
Solicitation No.: **GEN2129421P1**
Solicitation Title: **Next Generation 911 (NG911)**

Attention Vendors:
Note the following changes and clarifications. Any words in ~~strikethrough~~ type are deletions from existing text. Words in **bold underlined** type are additions to existing text.

1. Evaluation Criteria, Section 2, Project Approach: General System Requirements and Overall Approach has been revised as follows:

   Describe Prime Vendor's approach to the project, per the Scope of Work.
   Refer to the General Compliance sections listed below for requirements:
   i. System Requirements: SR-GN001, SR-GN002b, SR-GN003 - SR-GN005, SR-GN007.b, SR-GN008b, SR-GN009, SR-GN010.b, SR-GN011, SR-GN012, SR-GN013.b, SR-GN017.b, SR-GN018, SR-GN021, SR-GN024, SR-GN025, SN001.b, SN003.b, SN006, SN007, SN015, SN016, SN019
   ii. NG911 Processing: SR-GI001.b
   iii. Call Routing: SR-CR002.b
   iv. NG911 Call Delivery (Call Processing): SR-CP002.b
   v. Network Redundancy and Resiliency: SR-NR005
   vi. Implementation Timeline: TIME001.
   vii. Hardware and Equipment: SR-EH001 and SR-EH002
   viii. Initial Deployment: SD004.b
   ix. Testing: TS005
   x. Go-Live: GL001.b**, GL004**
   xi. Training: TRN007, TRN008.b, TRN009 - TRN012

All other terms, conditions and specifications remain unchanged for this solicitation.

PURCHASING DIVISION
broward.org/Purchasing
BPRO Electronic Procurement System

Addenda No.: **3**
Solicitation No.: **GEN2129421P1**
Solicitation Title: **Next Generation 911 (NG911)**

Attention Vendors:
Note the following changes and clarifications. Any words in ~~strikethrough~~ type are deletions from existing text. Words in **bold underlined** type are additions to existing text.

1. Evaluation Criteria, Section 2, Project Approach: General System Requirements and Overall Approach has been revised as follows:

   Describe Prime Vendor's approach to the project, per the Scope of Work.
   Refer to the General Compliance sections listed below for requirements:
   i. System Requirements: SR-GN001, SR-GN002b, SR-GN003 - SR-GN005, SR-GN007.b, SR-GN008b, SR-GN009, SR-GN010.b, SR-GN011, SR-GN012, SR-GN013.b, SR-GN017.b, SR-GN018, SR-GN021, SR-GN024, SR-GN025, ~~SN001.b~~, ~~SN003.b~~, SN006, SN007, SN015, SN016, **VN007** ~~SN019~~
   ii. NG911 Processing: SR-GI001.b
   iii. Call Routing: SR-CR002.b
   iv. NG911 Call Delivery (Call Processing): SR-CP002.b
   v. Network Redundancy and Resiliency: SR-NR005
   vi. Implementation Timeline: TIME001.
   vii. Hardware and Equipment: SR-EH001 and SR-EH002
   viii. Initial Deployment: SD004.b
   ix. Testing: TS005
   x. Go-Live: GL001.b, GL004
   xi. Training: TRN007, TRN008.b, TRN009 - TRN012

2. Evaluation Criteria, Section 3, NG911 Solution, Subsection A, Functionality Checklist has been revised as follows:

   A. **Functionality Checklist:** Refer to the Functionality Checklist and submit as instructed. Points will be allocated based on Vendor's Functionality Checklist response.
      i. Security/Notification: SN003.b, SN009, SN010.b, SN011 – SN013, **SN017**, SN020
      ii. 911 Call Ingress: SR-IN003.b
      iii. NG911 Processing: SR-GI013
      iv. Data Processing: DAT001.b and DAT003.b
      v. Call Routing: SR-CR003.b, SR-CR004, SR-CR006.b, SR-CR008, Sr-CR009, SR-CR010.b, and SR-CR011
      vi. Network Redundancy and Resiliency: SR-NR007, and SR-NR008.b
      vii. NG911 Call Delivery (Call Egress/Call Delivery to All PSAPs): SR-DL001, SR-DL004, SR-DL005.b, SR-Dl006, SR-DL007, SR-DL014.b, and SR-DL015
      viii. NG911 Call Delivery (Call Processing): SR-CP003 – SR-CP005

ix. Interfaces: SR-IT003
x. Reports: RPT001, RPT002.b, RPT003 – RPT005

3. Evaluation Criteria, Section 5, Project Approach: Evidence, Knowledge, and Experience, Subsection B, has been revised as follows:

   B. Provide actual performance results for the metric below on solutions in production. Refer to the General Compliance for requirements:
      i. Solution Performance: VN007~~7~~**8** and VN008~~8~~**9**

4. The General Compliance questionnaire has been revised and replaced in its entirety. Refer to the Vendor General Requirements section, Nos. 7 and 8.

All other terms, conditions and specifications remain unchanged for this solicitation.

PURCHASING DIVISION
broward.org/Purchasing
BPRO Electronic Procurement System

Addenda No.: **4**
Solicitation No.: **GEN2129421P1**
Solicitation Title: **Next Generation 911 (NG911)**

Attention Vendors:
Note the following changes and clarifications. Any words in ~~strikethrough~~ type are deletions from existing text. Words in **bold underlined** type are additions to existing text.

1. Evaluation Criteria, Section 3, NG911 Solution, Subsection A, Functionality Checklist has been revised as follows:

    A. **Functionality Checklist:** Refer to the Functionality Checklist and submit as instructed. Points will be allocated based on Vendor's Functionality Checklist response.
        i. Security/Notification: SN003.b, SN009, SN010.b, SN011 – SN013, SN017, SN020
        ii. 911 Call Ingress: SR-IN003.b
        iii. NG911 Processing: SR-GI013
        iv. Data Processing: DAT001.b and DAT003.b
        v. Call Routing: SR-CR003.b, SR-CR004, SR-CR006.b, SR-CR008, Sr-CR009, SR-CR010.b, and SR-CR011
        vi. Network Redundancy and Resiliency: SR-NR007, and SR-NR008.b
        vii. NG911 Call Delivery (Call Egress/Call Delivery to All PSAPs): SR-DL001, SR-DL004, SR-DL005.b, ~~SR-Dl006~~ **SR-DL006**, SR-DL007, SR-DL014.b, and SR-DL015
        viii. NG911 Call Delivery (Call Processing): SR-CP003 – SR-CP005
        ix. Interfaces: SR-IT003
        x. Reports: RPT001, RPT002.b, RPT003 – RPT005

All other terms, conditions and specifications remain unchanged for this solicitation.