County of Fairfax, Virginia

ADDENDUM

DATE: November 29, 2016

ADDENDUM NO. 5

TO: ALL PROSPECTIVE OFFERORS

REFERENCE: RFP2000002010

TITLE: Next Generation Core Services Solution (NGCS)

DUE DATE/TIME: **December 15, 2016 / 2:00 P.M.**

The referenced request for proposal is amended as follows:

1. Reference Page 56 of Appendix C, Section 4.11.3 SLAs for Incident Management: Delete this section and replace it with "It is expected that the Contractor will have processes and procedures for supporting a NOC/SOC that can rapidly triage calls. In the absence of reasonably proposed processes, the Contractor shall meet, at a minimum, the following requirements for tracking, responding to, and reporting on network and system outages or failures:

    - Severity Level 1 incidents responded to within 30 minutes and resolved within four hours of detection
    - Severity Level 2 incidents responded to within 30 minutes and resolved within eight hours of detection
    - Severity Level 3 incidents responded to within eight hours and resolved within 48 hours
    - Severity Level 4 incidents responded to within 16 hours and resolved within 96 hours

    These severity levels are defined as follows:

    Severity 1 Incident

    An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes: the incident (a) renders a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, or

Department of Procurement & Material Management
12000 Government Center Parkway, Suite 427
Fairfax, VA 22035-0013
Website: www.fairfaxcounty.gov/dpmm
Phone (703) 324-3201, **TTY:** 711, **Fax:** (703) 324-3681

seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 2 Incident

An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes: the incident (a) does not render a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 3 Incident

An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes: the incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

Severity 4 Incident

An incident shall be categorized as a "Severity 4 Incident" if the incident is characterized by the following attributes: the incident may require an extended resolution time, but does not prohibit the execution of productive work and a reasonable workaround is available.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:"

2. Reference Page 59 of Appendix C, Section 4.11.7 Incident Severity Level 1 and 2 Violation Damages: Change the title to read "Incident Severity Level 1 and 2 Credits".

3. Reference Page 59 of Appendix C, Section 4.11.7 Incident Severity Level 1 and 2 Violation Damages: Delete this section and replace it with "Contractor shall provide a monetary credit of the monthly recurring fee (MRF) to the NCR and its respective specified agencies, as applicable, for each event in which service levels are not maintained. The NCR expects that all of the Contractor's network devices and services will perform at a level equal to 99.999 percent uptime measured on a rolling, 12-month

calendar. Failure to meet service levels shall be measured per service-affecting outage. Respondent shall include how uptime information will be gathered, analyzed and provided to NCR.

Contractor shall meet the following requirements for tracking, responding to, and reporting on network and system outages or failures:

- Severity Level 1 incidents responded to within 30 minutes and resolved within four hours of detection.

- Severity Level 2 incidents responded to within 30 minutes and resolved within eight hours of detection.

The following severity levels are defined as follows:

Severity Level 1 Incident

An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes: the incident (a) renders a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity Level 2 Incident

An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes: the incident (a) does not render a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

For Severity Level 1 and 2 incidents, a 10-percent credit of the monthly recurring fee (MRF) shall be due to the NCR and its respective agencies, as applicable when the initial period of resolution is exceeded. If the resolution period length of time doubles, then the credit shall increase to 20 percent of the MRF. If the resolution period length of time quadruples the initial period, then 50 percent of the MRF shall be credited. The credited amount shall be included on the invoice of each affected NCR jurisdiction the month immediately following the violation."

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:"

4. Reference Page 26 of Special Provisions, Appendix A: Fairfax County DEPARTMENT OF INFORMATION TECHNOLOGY IT Services Provider CONSULTANT/CONTRACTOR AGREEMENT CONCERNING ACCESS TO AND USE OF INFORMATION SYSTEMS AND COMMUICATIONS TECHNOLOGY AT FAIRFAX COUNTY, VIRGINIA: Delete it and replace it with Attachment 2 of this addendum.

5. Refer to Attachment 1 for the answer to the question received after November 11, 2016.

All other terms and conditions remain the same.

Jamie Pun, VCO, CPPB
Contract Specialist II

THIS ADDENDUM IS ACKNOWLEDGED AND IS CONSIDERED A PART OF THE SUBJECT REQUEST FOR PROPOSAL:

_____
Name of Firm

_____ _____
(Signature) (Date)

A SIGNED COPY OF THIS ADDENDUM MUST BE INCLUDED IN THE TECHNICAL PROPOSAL OR RETURNED PRIOR TO DUE DATE/TIME.

Note: SIGNATURE ON THIS ADDENDUM DOES NOT SUBSTITUTE FOR YOUR SIGNATURE ON THE ORIGINAL PROPOSAL DOCUMENT. THE ORIGINAL PROPOSAL DOCUMENT MUST BE SIGNED.

Attachment 1

Q1: The offeror would like to provide description optional services listed on the pricing sheet. Does Fairfax have a preferred method for submitted these descriptions or can we submit them as an attachment to the pricing sheet?

A1: As an attachment to the pricing sheet but separate each optional services as a separate attachment.

Attachment 2

Fairfax County DEPARTMENT OF INFORMATION TECHNOLOGY

IT Services Provider CONSULTANT/CONTRACTOR AGREEMENT

CONCERNING ACCESS TO AND USE OF INFORMATION SYSTEMS and COMMUNICATIONS TECHNOLOGY AT FAIRFAX COUNTY, VIRGINIA

I / this firm_____ working as a consultant/contractor/services provider for Fairfax County Government with access to county technology and communications systems, recognize my/our firm's legal and ethical obligation to conduct work on any Fairfax County information or communications system using computer hardware and devices, and/or software (programming languages, operating systems, databases, third party applications software (COTS) and Web based or 'cloud' applications), system utilities, security solutions, monitoring systems, and, data or voice communications software and electronics, Internet capabilities, etc. and county data/content herein referred to as 'technology', in a responsible manner and within the guidelines of the County's IT Security Policy and/or firm's contract. My/our purpose in using computer based technology is to perform work for Fairfax County which includes accessing Fairfax County systems through the Internet, and therefore we are subject to the standards, IT Security and Privacy policies, and ethics and behavior policies of Fairfax County Government. As a condition for and in consideration of being given access to computer systems, data, the network, internet, and, Fairfax County computer center(s), IT galleries, server rooms, network core facilities, third party hosting centers and 'clouds' where county services are provided or supported, I/we affirm that:

I/our firm possess the professional credentials that I or my firm has represented in being hired to perform my/our duty and assignments, and that I/our firm representatives have successfully passed a certifiable criminal background check.

I/our firm will not use Fairfax County technology systems or our firm's systems to access any information available or acquired from the technology systems for any reason except for purposes directly related to our (firm's) job assignments and responsibilities as defined by my/my firm's contract and assignment with the County. I/we will not use Fairfax County technology systems to disclose any information available or acquired from Fairfax County systems for any reason except for purposes directly related to my/my firm's contract and job assignments and responsibilities for such use as defined by DIT and contract(s). I/we understand that any work I/we perform for Fairfax County that develops systems, logic, or data is the property of Fairfax County, and I/we cannot take or send such products or data without express permission of appropriate Fairfax County authority. I/we will exercise due diligence in providing policy and oversight of our firm's contractors and sub-contractors. I/we understand that a user agency may ask me/ my firm to sign a separate agreement relating to the privacy and security of the information that a user agency administers, such as for HIPAA, PCI, PII, and/or other Data Privacy Cyber Security laws.

I/ our firm will use vendor provided software and/or utilities only in accordance with that vendor's license, and such provisions as may have been agreed to between such vendor and Fairfax County. I/we will not deliberately violate any copyright laws or agreements states or implied in my/our use of the software. I/we recognize that to do so makes me/my company liable for any applicable penalties and may lead to my/our firm's immediate dismissal from the County's engagement.

I/our firm further understands that the deliberate misuse of Fairfax County technology, data, and/or software which results in the change, damage or destruction of County systems, programs, and/or data is considered destruction of County property and may be considered a breach of contract and/or a criminal offense. I/we understand that our firm may be liable to include immediate release from the engagement for breach of the Fairfax County IT Security Policy, and possible prosecution for the actions of my/this firms actions in the destruction of County property, misuse or theft of classified (sensitive) data. I/we further understand and recognize that there are criminal penalties for deliberate misuse of government information.

I/we have completely read and fully understand the terms of this agreement and accept these terms.

_____
Name of Firm

_____ _____
Firm's Consultant/Representative Signature Date

_____ _____
Firm Authorized Representative Date

I acknowledging receipt of this agreement on behalf of Fairfax County, Virginia.

_____ _____
Fairfax County IT Security Officer Date