STATEMENT OF WORK (SOW)

**Order Identification Number: [XX ###XXX#T5]**

# DNS Security Extensions (DNSSEC) Deployment Project

# Issued by:

**[Agency Logo, Name, and Address]**

# DATE: [DD MM YYYY]

**Table of Contents**

DNS Security Extensions (DNSSEC) Deployment Project i

Issued by: i

DATE: [DD MM YYYY] i

1 Project Description 1

1.1 Purpose 1

1.2 Background 4

1.2.1 Organization and Mission 4

1.3 Scope 4

1.3.1 General Description of Requirements 4

1.3.2 Existing Domain Name System (DNS) Infrastructure 4

1.3.3 Anticipated Limitations and Constraints 4

1.4 Acquisition Selected 4

1.5 Period of Performance 5

1.6 Place of Performance 5

1.7 Government Furnished Equipment 5

1.8 Fair Opportunity 6

1.9 Requirements and Guidelines 6

1.9.1 Requirements 6

1.9.2 Guidelines 7

2 Statement of Work 8

2.1 Task 1 – DNSSEC and Email Authentication Deployment Planning and System Analysis 10

2.1.1 Sub-task 1 – Project Management Plan 10

2.1.2 Sub-task 2 – DNSSEC and Email Authentication Training Plan 12

2.1.3 Sub-task 3 –DNSSEC Configuration / Architecture 13

2.1.4 Sub-task 4 –DNSSEC Servers’ Platform and Administration Rules 16

2.1.5 Sub-task 5 – DNSSEC Testing and Deployment Roll-out Plan 18

2.2 Task 2 – Set Up Test Lab 19

2.2.1 Sub-task 1 – Test Lab Installation 19

2.2.2 Sub-task 2 – Test Lab Connectivity to NIST/DHS/Sparta SNIP System 20

2.3 Task 3 – Convert, Test, and Archive DNSSEC Servers 21

2.3.1 Sub-task 1 – Implementation Checklists for DNS Security 21

2.3.2 Sub-task 2 – Test Plans for DNS Threats 23

2.3.3 Sub-task 3 – DNSSEC Key Generation and Management Procedures 24

2.3.4 Sub-task 4 – Conversion of Production Zone DNS Servers 25

2.3.5 Sub-task 5 – Test and Archive DNSSEC Servers in the Test Lab 26

2.3.6 Sub-task 6 – Convert, Test, and Archive DNSSEC Servers for Each Site 27

2.4 Task 4 – DNSSEC Deployment/Cutover of Agency Production Zones 27

2.5 Task 5 –Operational Procedures for Administration of DNSSEC 28

2.6 Task 6 – Authentication of Agency Email System with DKIM and SPF 28

2.6.1 Sub-task 1 – Email Authentication Planning and System Analysis 29

2.6.2 Sub-task 2 – Deployment/Cutover of Email Authentication System 30

2.6.3 Sub-task 3 –Administration of Email Authentication System 31

3 Labor Types 33

3.1 Personnel Requirements 33

3.2 Proposed Personnel 34

3.3 Special Qualifications and Certifications 35

4 Task 2 – Set UP Test Lab 36

5 Travel and Other Direct Costs (ODC / Un-priced Items) 39

5.1 Travel 39

5.2 Other Direct Cost (ODC / Un-priced Items) 39

6 Inventory and Warranty 40

7 Invoicing and Payment 40

7.1 Detail Billing Requirements 40

7.2 Invoice Address, Data Format and Delivery Method 40

7.2.1 Invoice Address 41

7.2.2 Invoice Submission 41

7.2.3 Billing Cycle and Data Elements 42

7.2.4 Electronic Funds Transfer (EFT) 43

7.3 Billing for Other Direct Costs (ODCs) or Unpriced Item 43

7.3.1 Invoice for Travel Expenses 44

8 Electronic and Information Technology Accessibility Standards (Section 508) 45

9 Proposal Instruction to Offerors 46

10 SOLICITATION CLOSING DATE AND TIME: 46

11 REQUIRED SUBMISSIONS: 46

11.1 General Instructions 46

11.2 Preparation of Technical Proposal 47

12 Past Performance Worksheets 50

13 PAST PERFORMANCE INSTRUCTIONS 50

13.1 Preparation of Price Proposal 51

15 Evaluation Factors and Basis for Award 52

15.1 Evaluation Methodology and Basis for Award 52

15.2 Evaluation Approach – Trade Off or LPTA 53

15.3 Technical Evaluation Criteria 55

15.4 Price Evaluation Criteria 58

16 Task Order Award 59

17 Organizational Conflicts of Interest 60

18 Nondisclosure Agreement 60

19 Attachments 61

19.1 Attachment A – Program Management Plan 61

19.2 Attachment B – Support Locations 61

19.3 Attachment C – Pricing Requirements 61

19.4 Attachment D – Pricing Template 61

19.5 Attachment E – Equipment, Support and Warranty Inventory 61

19.6 Attachment F – Past Performance Worksheet 61

19.7 Attachment G – Task Order Deliverables 62

19.8 Attachment H – Sample Existing DNS Security Architecture and Figures 62

19.9 Attachment I – DNS Security (DNSSEC) Reference Architecture 62

19.10 Attachment J – NIST Specified DNSSEC Implementation Checklists 62

# Project Description

**Domain Name System (DNS) Security Extensions (DNSSEC) Deployment Project**

Note: Text boxes contain informational material that should be deleted by the Agency when finalizing this document. All text in orange color need to be personalized for the Agency-specific SOW.

The Connections II DNSSEC Deployment Project Statement of Work (SOW) Template is provided by GSA to help customer Agencies contract for services to transition their network infrastructures and applications from (a) DNS to DNSSEC and (b) Email authentication based on the deployed DNSSEC. The SOW Template is designed as an example SOW that can be readily tailored to meet an Agency’s deployment needs.

Some Agencies may contract directly for DNSSEC Deployment services, while others may require advisory services to aid the Agency and/or existing IT contractors with the Deployment. The SOW Template assumes the DNSSEC offeror will implement the changes, but each Agency may modify the language as appropriate for its specific contractual environment.

The SOW Template is intended to accommodate Agency customers with enterprise DNS configurations of varying complexity and security policies. Client agencies with more basic DNS configuration environments may not need all of the detailed specifications it provides. Parts of the SOW Template may be tailored, replaced or omitted entirely, depending on the requirements of the Agency.

Note also that although the SOW Template implementation tasks are generally ordered in the sequence they will be executed, they may overlap in some cases and be performed in parallel (see **Section 2: Statement of Work**).

## Purpose

This Statement of Work supports the [Agency] DNS Security Extensions (DNSSEC) Deployment Project to help deployment of the [Agency’s] (a) DNS configurations from DNS to DNSSEC and (b) Email Authentication based on the deployed DNSSEC under the General Services Administration (GSA) Connections II contract.

Operational deployment and use of DNSSEC has been mandated by the Office of Management and Budget (OMB) by the OMB directive, *M-08-23 Securing the Federal Government’s Domain Name System Infrastructure*, for securing the Agency’s external DNS facing the Internet.

The intent of this SOW Template for the deployment of DNSSEC in Federal agencies is to enable agencies to leverage existing capabilities and technologies when implementing DNS in evolving Enterprise Architectures and to achieve compliance with the National Strategy for Trusted Identities in Cyberspace (NSTIC) in the context of their respective missions, programs, and initiatives. NSTIC calls for the development of interoperable technology standards and policies - an "Identity Ecosystem" - where individuals, organizations, and underlying infrastructure - such as routers and servers - can be authoritatively authenticated. DNSSEC is a critical enabling technology for NSTIC.

Domain Name System (DNS) services are critical to the operation of Agency networks and services, providing several types of key directory services. Malicious DNS exploits (e.g. redirection of Internet connections to Government Agency web sites to malicious web sites instead) can have very substantial negative consequences. It is important to ensure the integrity of DNS information for this reason. DNS Security Extensions (DNSSEC) provides DNS nameserver authentication and email authentication so that they can be trusted as authentic and unmodified. In addition, there is an OMB mandate for all Agencies to have implemented DNS security measures known as DNS Security Extensions (DNSSEC) by December 2009.

DNSSEC provides valuable benefits to agencies by improving cyber security. While not all expected benefits will be fully realized until the DNSSEC adoption is completed, incremental benefits will accrue as the deployment takes place. Examples of anticipated DNSSEC benefits include:

* *DNS information validation*: Due to the non-secure nature of DNS, there are many high profile instances where DNS servers have been hijacked (redirecting the resolution of DNS names to rogue DNS servers), DNS records spoofed, and DNS caches poisoned, leading users to believe they are connecting to legitimate sites when in fact they have been led to a web site that contains malicious content or collects their information by pharming. [Pharming is similar to phishing, except that instead of following a link in email, users visit the site on their own, using the correct URL of the legitimate site, so they think they’re safe. But the DNS records have been changed to redirect the legitimate URL to the fake, pharming site.] To help provide added security, the DNS Security Extensions (DNSSEC) were created to provide a method for validating DNS information. Thus DNSSEC addresses an identified security risk and helps prevent malicious activities like cache poisoning, pharming, and man-in-the-middle attacks. In addition, DNS is commonly used for purposes beyond looking up IP addresses, including uses as directory servers for black-lists and for Sender Policy Framework parameters.
* *Email authentication*: Email was not designed with any integrated requirements of trust or confidence. One consequence is that common email cannot be trusted to be authentic or unmodified due to the myriad vulnerabilities found across email systems. A number of known vulnerabilities enable malicious actors to alter information within an email message to fool an unsuspecting reader. These vulnerabilities enable well-known security challenges, such as spam and phishing. Email authentication can be achieved through the implementation of either DomainKeys Identified Mail (DKIM) or Sender Policy Framework (SPF), based on DNSSEC, which can be implemented separately or together. In brief, SPF validates MAIL FROM vs. its source server; DKIM validates the "From:" message header and a mail body by cryptographic means (public key).

The purpose of this SOW is to describe the requirements for contractor assistance needed to support a comprehensive and coherent deployment from DNS to DNSSEC and Email authentication based on the deployed DNSSEC, while ensuring compliance with OMB directives.

## Background

The Agency’s DNSSEC Deployment Office is responsible for developing the Master Deployment Plan and for all required activities related to its execution. Required support tasks include providing infrastructure and technical guidance, and ensuring the use of unified solutions across the Agency to minimize prices and maximize security.

In order to provide background information relevant to this SOW, this section should include at a minimum the following subsections.

### Organization and Mission

[Add Agency-specific information here]

## Scope

Scope information for this SOW should include at a minimum the following subsections.

### General Description of Requirements

[Add Agency-specific information here]

### Existing Domain Name System (DNS) Infrastructure

[Add Agency-specific information here]

See ***Attachment H – DNS Security Architecture and Figures*** for a sample diagram.

### Anticipated Limitations and Constraints

[Add Agency-specific information here]

## Acquisition Selected

The Agency will need to determine which type of task order to use (either FFP or T&M).

[Agency] has selected the Connections II Contract for the DNSSEC Deployment Project. Connections II allows Firm Fixed Price (FFP) or Time & Material (T&M) task orders. This requirement will be for a [Add Agency-specific information here] task order.

This solicitation includes requirements for all labor and equipment necessary to support DNSSEC planning, deployment and implementation.

The offeror shall adhere to the terms and conditions of the Connections II Contract, and shall meet and comply with the Agency-specific requirements described in this SOW.

## Period of Performance

The Tasks agreed upon by [Agency] and the offeror will remain in effect for the life of the Connections II Task Order. The offeror shall provide technical support, and shall procure and install [or recommend] equipment for these Tasks. The term of the order will be from the date of award through a base period plus [n] option periods. The overall period of performance is specified in the following table.

**Table 1.5-1: Date of Task Order Award**

|  |  |  |
| --- | --- | --- |
|  | **Start Date** | **End Date** |
| **Base Year** | <Performance\_Start\_Date> | <Performance\_End\_Date\_Base\_Period> |
| **Option Period 1** | <Performance\_Start\_Date\_Option\_Period\_1> | <Performance\_End\_Date\_Option\_Period\_1> |
| **Option Period 2** | <Performance\_Start\_Date\_Option\_Period\_2> | <Performance\_End\_Date\_Option\_Period\_2> |
| **Option Period 3** | <Performance\_Start\_Date\_Option\_Period\_3> | <Performance\_End\_Date\_Option\_Period\_3> |
| **Option Period n** | <Performance\_Start\_Date\_Option\_Period\_n> | <Performance\_End\_Date\_Option\_Period\_n> |

*Note: This table is for illustration purposes only. The Agency has the option to add or remove years in order to complete the DNSSEC Deployment. The Connections II contract was awarded in October 2011. It ends January 19, 2021. An order placed before January 19, 2021 can last up to January 19, 2026.*

## Place of Performance

The offeror shall comply with the geographic requirements specified in this solicitation to provide support. The Place of Performance will be specified in ***Attachment B – Support Locations***.

## Government Furnished Equipment

Upon the award and placement of each task order, Government Furnished Equipment (GFE) may be made available by the Agency for use by the offeror to support the tasks. The offeror shall use GFE to provide support services as mutually agreed upon by the offeror and Agency. The offeror shall evaluate all equipment as the Agency directs.

## Fair Opportunity

This SOW will be governed by the requirements outlined in **FAR Part 16.505** as it relates to Fair Opportunity.

## Requirements and Guidelines

The offeror should review the following requirements and guidelines:

### Requirements

* + - 1. Internet Engineering Task Force (IETF) Domain Name System Security Extensions (DNSSEC) specifications, covered by Request for Comments (RFC) 4033, 4034, 4035, and 3833 [RFC4033], [RFC4034], [RFC4035], [RFC3833]. These are also individually listed below.
      2. IETF Transaction Signature (TSIG) specifications, covered by RFCs 2845 and 3007 [RFC2845], [RFC3007].
      3. NIST SP 800-81 - Security Domain Name System (DNS) Deployment Guide
      4. NIST SP 800-57 - Recommendation for Key Management, Part 1 – General and Part 3 – for Application-Specific Key Management
      5. IETF RFC 4033 - Domain Name System Introduction and Requirements
      6. IETF RFC 4034 - Resource Records for DNS Security Extensions (DNSSEC), revision 3
      7. IETF RFC 4035 - Protocol Modifications for DNS Security Extensions (DNSSEC)
      8. IETF RFC 3833 – Threat Analysis of the Domain Name System (DNS)
      9. IETF RFC 4408 - Sender Policy Framework (SPF) - for verifying Email sender IP addresses
      10. IETF RFC 4641 – DNSSEC Operational Practices - for Signature Generation, Key Rollover, and Related Policies
      11. IETF RFC 6376 - DomainKeys Identified Mail (DKIM) - for the signed domain to take responsibility of an email
      12. IETF RFC 2845 - Secret Key Transaction Authentication - for DNS Transaction Signature
      13. OMB Memo M-08-23 - Securing the Federal Government’s Doman Name System Infrastructure
      14. FIPS Pub 200 - Minimum Security Requirements for Federal Information and Information Systems
      15. FIPS Pub 140-2 - Security Requirements for Cryptographic Module
      16. FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems
      17. NIST SP 800-53 - Recommended Security Controls for Federal Information Systems

### Guidelines

* + - 1. NIST: Special Publication (SP) 800-81: Secure DNS Deployment Guide, Version 1.0, November 2009
      2. DHS: Domain Name System (DNS) Security Reference Architecture [published by: Federal Network Security - Federal Interagency Technical Reference Architectures]
      3. DHS: Electronic Mail Gateway Security Reference Architecture, [published by: Federal Network Security - Federal Interagency Technical Reference Architectures]
      4. Federal CIO Council: DNSSEC and Email Authentication Considerations [Considerations and Lessons Learned for Federal Agency Implementation of DNS Security Extensions and Email Authentication]
      5. DHS: DNSSEC Roadmap [DNSSEC deployment Initiative for developing required critical tools, technologies, and partnerships]

# Statement of Work

This Statement of Work will address the full deployment of DNSSEC, as specified by NIST, DHS, and Inter-Agency CIO Council, for the external DNS security and the Email authentication based on the deployed DNSSEC.

|  |
| --- |
| For an understanding of the total scope of the DNSSEC deployment for external DNS security and Email authentication, a brief overview of DNS, DNSSEC, and Email authentication is presented below:  Overview of DNS  Internet network resources are identified by numeric IP addresses, but these IP addresses are difficult for network users to remember. The DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. The DNS database contains records that map user-friendly alphanumeric names (e.g., gsa.gov) for network resources to the IP address used by those resources for communication. In this way, DNS acts as a mnemonic device (like a telephone or email directory), making network resources easier to remember for network users. DNS is a globally distributed database to store this name and address information for all public hosts on the Internet. An Agency’s DNS is a key component of its network infrastructure. Therefore it is vital that the DNS infrastructure is responsive, robust, and secure so that it can meet its two primary business purposes: (a) allow Agency personnel to reach the Internet; and (b) allow the general public to reach the Agency’s public-facing web services.  Overview of DNSSEC  DNSSEC is a set of modifications to the DNS protocol intended to provide DNS data integrity, authenticated denial of existence, and a trusted path of authentication of DNS data. DNSSEC is designed to protect an ISP’s DNS resolvers (clients) from forged DNS data, which occurs as the result of a DNS attack. DNSSEC secures DNS by signing all records hosted on the authoritative name server using a cryptographic key to produce a digital signature. When a DNS resolver requests a DNS record, it also receives a digital signature of the record that was created by the cryptographic key. The resolver decrypts the signature using the associated public key to verify that the record it received is identical to the record on the authoritative server. DNSSEC uses the digital signature to create a chain of authority. Then, it uses the chain to verify that the source domain name, which the DNS resolver returns, matches the DNS record stored at the authoritative DNS. If it cannot validate the source, it discards the response. Thereby, a chain of trust for a domain-name is ensured. Thus, DNSSEC provides a means to authenticate DNS responses and ensures (a) origin authentication of DNS data, (b) data integrity, and (c) authenticated denial of existence.  DNSSEC depends not only on the zone (the database of DNS records for a domain) being signed, but on the local resolver (usually that of your ISP) being enabled for DNSSEC (or 'security aware'). If a resolver is not security-aware, then DNSSEC is not relevant. When a zone is DNSSEC signed, the creator of the zone generates what are called key-pairs. These form the basis of what is usually called Public Key (PK) encryption, or asymmetrical encryption. In PK, the private key is used to encrypt a message, and it can only be decrypted by the public key. This is performed in such a way that the private key cannot be derived from the public key. The public key is listed in the zone file under the DNSKEY record. The private key is stored securely on the authoritative nameserver. The fact that the zone has been signed is registered at the root for that zone. All root servers are currently DNSSEC enabled and the major top level domains (.gov, .com, .org) have been signed.  When a security-aware DNS resolver queries the root servers for a domain's authoritative nameservers, it also receives the information of whether or not a domain is signed. If it is, then it will only accept digitally signed responses for it, and refuse any others. It will also receive a digest copy of the key for the next servers down the line. Now, as the resolver works its way down the chain, it will receive the information for the next set of authorized servers with a digital signature, as well as the key to validate the next piece of information it get; and, thereby creates a “chain of trust”.  Overview of Email Authentication by DKIM and SPF based on DNSSEC  Email was not designed with any integrated requirements of trust or confidence. One consequence is that common email cannot be trusted to be authentic or unmodified due to the myriad vulnerabilities found across email systems. A number of known vulnerabilities enable malicious actors to alter information within an email message to fool an unsuspecting reader. These vulnerabilities enable well-known security challenges, such as spam and phishing. Email authentication can be achieved through the implementation of either DomainKeys Identified Mail (DKIM) or Sender Policy Framework (SPF) based on DNSSEC, which can be implemented separately or together. In brief, SPF validates MAIL FROM vs. its source server; DKIM validates the "From:" message header and a mail body by cryptographic means (public key). Most major commercial Email systems, such as Yahoo mail, Google mail, MS Windows/Exchange, and Lotus Notes Mail support DKIM and/or SPF either directly or through plug-ins.  DKIM and DNSSEC rely on the security of the public–private key pairs used to sign and validate messages. DKIM is a method for associating a domain name to an email message, thereby allowing a person, role, or organization to claim some responsibility for the message. The association is set up by means of a digital signature which can be validated by recipients. Responsibility is claimed by a signer - independently of the message's actual authors or recipients - by adding a DKIM-Signature field to the message's header. The verifier recovers the signer's public key using the DNS, and then verifies that the signature matches the actual message's content. A DKIM signature can cover other fields of a message's header, such as, the “From:” and “Subject:” fields and the message body (or its initial part).  SPF is an email validation system designed to prevent email spam by detecting email spoofing, a common vulnerability, by verifying sender IP addresses. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or TXT record) in the Domain Name System (DNS). Mail exchangers use the DNS to check that mail from a given domain is being sent by a host sanctioned by that domain's administrators. |

This Statement of Work is in support of the [Agency] DNSSEC Deployment Project for the required deployment of the Agency’s external DNS configurations/ network, systems and operations support from DNS to DNSSEC and Email authentication based on the deployed DNSSEC under the General Services Administration (GSA) Connections II contract.

This section describes the full range of contractor support services, equipment, and equipment services that may be needed, including the performance measures to be used to assess the quality and timely delivery of the following required Tasks:

* + - * Task 1 – DNSSEC and Email Authentication Deployment Planning and System Analysis
      * Task 2 – Test Lab
      * Task 3 – Convert, Test, and Archive DNSSEC Servers
      * Task 4 – DNSSEC Deployment/Cutover of Agency Production Zones
      * Task 5 – Operational Procedures for Administration of DNSSEC
      * Task 6 – Authentication of Agency Email System with DKIM and SPF

Some Agencies may choose to authorize and execute the above tasks one at a time, basing the requirements for later tasks on the results obtained from the previous task or tasks.

## Task 1 – DNSSEC and Email Authentication Deployment Planning and System Analysis

DNSSEC Deployment planning and system analysis includes the following activities:

* + - * Create an DNSSEC and Email Authentication Project Management Plan
      * Create an DNSSEC and Email Authentication Training Plan
      * Define DNSSEC configuration /architecture
      * Develop DNSSEC servers’ platform and administration rules
      * Develop DNSSEC Testing and Deployment roll-out plan

### Sub-task 1 – Project Management Plan

The contractor shall establish and execute [or recommend] DNSSEC Project Management Plan (PMP) to ensure that all activities from the kick-off meeting to the final DNS infrastructure deployment to DNSSEC are executed properly; as planned and on schedule.

* + - 1. The contractor shall establish a Project Management (PM) function to provide management and operations support to the Agency and serve as a single point of contact for the Agency to manage and administer the DNSSEC Deployment order, which includes both DNS transition to DNSSEC and Email authentication based on deployed DNSSEC.
      2. The contractor shall provide project management support that includes management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work. The contractor shall identify a Project Manager (PM) by name, to provide management, direction, administration, quality assurance, and leadership for the execution of this task order. The PM will be the primary point of contact for all program activities
      3. The contractor shall describe in the PMP proposed Labor Types for professional and technical expertise that fully meet the requirements in Tasks 1 through 6 to support DNSSEC Deployment solutions, including as applicable: life cycle management, analysis, planning, design, specification, implementation, integration and management of network services and equipment before and after deployment.
      4. The PMP shall include development of a DNSSEC and Email Authentication Deployment Strategy document to ensure that network, computing, application, and service components are enabled in a sequence that maximizes the benefit to the Agency’s business mission through meaningful DNSSEC activity. The DNSSEC Deployment Strategy document shall address the following:
  1. Identification of Deployment activities
  2. Identification of Deployment priorities and possible phases
  3. Deployment milestones, to include the enterprise DNSSEC configurations/architecture and risk mitigation
  4. Deployment criteria for legacy, upgraded, and new capabilities
  5. Dependencies (for example, among the enterprise architecture, network management, and network and operation security)
  6. Risks and mitigation strategies
  7. Strategies for ensuring interoperability and security during deployment
  8. Deployment governance that includes but is not limited to: policy, roles and responsibilities, management structure, management controls, management actions, performance measurement, and reporting
  9. Testing
     + 1. The PMP shall delineate the activities required to prepare and support the DNSSEC deployment, such as inventory management of DNS, training, and the methodology for acquiring DNSSEC testing with the DHS/NIST/Sparta SNIP system, as described in this Statement of Work. The potential impact of the lead time required to obtain testing with the DHS/NIST/Sparta SNIP system shall be included.
       2. The PMP shall capture and establish the SOW goals, identify a critical path, create general timelines to provision required hardware and software, and implement appropriate operational procedures. The PMP shall contain at a minimum:
  10. Project management approach for Tasks 1, 2, 3, 4, 5, and 6.
  11. Project Team Organization (Roles & Responsibilities)
  12. Project Tracking and Communication Plan
  13. Project Schedules & Milestones
  14. Earned value reporting
      + 1. The PMP shall describe how the Deployment activities will be integrated with third-party services provided by other Government Agencies or by commercial vendors.
        2. The PMP shall serve as a repository documenting the processes and methodology for meeting the requirements of each task described in this Statement of Work.
        3. The PMP shall be updated periodically for any changes to the program plans, activities, schedules, and any other related issues that may potentially impact the timely completion of the DNSSEC Deployment.
        4. An initial draft PMP shall be provided to the Government with the proposal. Upon award the Government will provide comments, which shall be incorporated in the final PMP. The contractor shall provide to the Agency both the draft and final document deliverables in MS Word format, and any required briefings/presentations in MS PowerPoint format.

### Sub-task 2 – DNSSEC and Email Authentication Training Plan

The contractor shall establish and maintain [or recommend] a DNSSEC and Email Authentication Training Plan for appropriate Agency personnel involved with the Agency DNS infrastructure:

* + - 1. Identify initial and ongoing DNSSEC and email authentication training requirements for Agency review, comment, and approval. The training shall include both DNS transition to DNSSEC and Email authentication based on deployed DNSSEC. The Training Plan shall at a minimum describe the training schedule, curriculum, materials, and the resources required to ensure that the training meets the Agency’s needs.
      2. The contractor shall provide the following types of training as required by the Agency:
  1. The contractor shall train Agency security architects to understand and mitigate the risks of DNSSEC and Email Authentication Deployment.
  2. The contractor shall train Agency network security architects on how to take full advantage of DNSSEC and Email Authentication capabilities.
  3. The contractor shall train Agency IT employees who are involved with the network security management, including employees on operations teams, to understand how DNSSEC and Email Authentication affect their areas of responsibility.
     + 1. Deliverables for the Agency to verify successful performance of the task:
  4. The contractor shall produce a Training Plan that describes the training schedule and curriculum, and the required materials, resources, and evaluation forms for Agency review, comment, approval, and signoff.
  5. The contractor shall provide training as per the approved Training Plan. Each unit of training shall conclude with a written evaluation that shall be made available to the Agency upon request.
  6. An initial draft Training Plan shall be provided to the Government with the proposal. Upon award, the Government will provide comments, which shall be incorporated in the final Training Plan. The Training Plan shall be updated upon request. The contractor shall provide to the Agency both the draft and final document deliverables in MS Word format, and any required briefings/presentations in MS PowerPoint format.

### Sub-task 3 –DNSSEC Configuration / Architecture

|  |
| --- |
| For an understanding of DNSSEC configuration/architecture, an overview of various external DNS server types (Authoritative Name Servers, Recursive Caching Name Server, and different classes of sub-servers for each type; see Figure 1 in Attachment I), based on different Agency security policies, is presented below:   1. Authoritative Name Servers    1. Authoritative servers maintain a portion of the global DNS database for an enterprise (referred to as its zone, as an example, ‘agency.gov’). The authoritative servers for the respective zones are able to provide any resolution within its portion of the name space (e.g. \*.agency.gov) or issue an error message such as NXDOMAIN (not able to resolve the requested name to an IP address).    2. Authoritative servers are further divided into two categories: primary (or “master”) and secondary (or “slave”).       1. A primary name server loads its information from a locally maintained file or database.       2. A secondary name server is an authoritative name server which obtains the zone information that it serves from a primary name server by DNS protocol (*zone transfer)* or by some other data replication services from a locally maintained database.    3. Name Server Exposure       1. Public-Facing Name Server - An Authoritative name server is “public-facing” if it responds to DNS queries from an external network. It is usually located in an Agency’s DMZ but may reside elsewhere.       2. Private Name Server - A name server is private if it does not respond to DNS queries from an external network. Private name servers (internal mail servers, application servers, etc) are positioned inside firewalls as close to internal users as is practical. [Note: internal DNS is out of scope of this SOW, but is included to show how it differs from external DNS.] 2. Recursive Caching Name Server 3. A recursive caching server (or “caching resolver server”) performs DNS resolution on behalf of clients (“stub” clients without the ability to do a full DNS query). It then stores the responses in a cache for the benefit of all the stub clients it services. |

The contractor shall customize [or recommend] the following DNSSEC configuration (DNSSEC servers types) for each Agency HQ and Office sites as per Agency CIO security policy (see Figure 1 in the Attachment I for a Reference DNSSEC configuration / architecture diagram):

* + - 1. The contractor shall define [or recommend] the DNSSEC Configuration (Server Types as applicable) for Agency HQ:
  1. In the DMZ

1. External Authoritative DNS (recursion disabled) for “Query” from the Internet users for host name resolution
2. *Recursive Caching DNS* for “Query” from internal Agency users for Internet host name resolution
   1. In the Internal Network (related to external DNS)
3. *Hidden Primary DNS*, as main database, to load *Internal Authoritative DNS* (via Zone Transfer)
4. *Internal Authoritative DNS* for “Forward” any updates to *Recursive Caching DNS* in the DMZ
5. *Internal Recursive Caching DNS* for
   * + 1. Query” from internal users for Internet host name resolution
       2. “VPN Tunneled Query” from Remote VPN clients (teleworkers) for Internet host name resolution
       3. “Recursion Request” to *Recursive Caching DNS* in the DMZ for Internet host name resolution, if unable to resolve “Query” from Agency users
       4. The contractor shall define [or recommend] the DNSSEC Configuration (Server Types as applicable) for each Agency Office site(s)
   1. In the DMZ
6. *Recursive Caching DNS* for “Query” to other DNSs (Root, other) in the Internet for host name resolution
   1. In the Internal Network (related to external DNS)
   2. *Internal Authoritative DNS* (geographical diversity for fault tolerance) for
      1. “Zone Transfer” (Load) from *Hidden Primary* in the Agency HQ
      2. “Forward” any updates to *Recursive Caching DNS* in the DMZ
7. *Internal Recursive Caching DNS* for
   * + 1. “Query” from internal users for Internet host name resolution
       2. “VPN Tunneled Query” from Remote VPN clients (teleworkers) for Internet host name resolution
       3. “Recursion Request” to *Recursive Caching DNS* in the DMZ for Internet host name resolution, if unable to resolve “Query” from Agency users

The contractor shall use the following consideration guidelines for defining [or recommending] DNS configurations (DNSSEC server types):

* + - 1. Considerations for Agency Size and Complexity
  1. For small agencies, one or two recursive servers may be enough. Larger agencies may need several recursive servers and may want to consider having a larger Agency-wide aggregate cache (i.e. forwarder) to provide faster response time for users and provide a single gateway for any monitoring by intrusion detection systems (IDS) or similar systems.
  2. Separate departments within an Agency would have their own recursive server that would forward its queries to the aggregate cache, which would then build an Agency-wide cache of responses.
  3. Most stub clients (i.e., desktop and laptop systems) do not perform DNSSEC validation, and will/must rely on a validating recursive server.
     + 1. Considerations for External Authoritative Servers
  4. Use dedicated external name servers to eliminate cache poisoning
  5. Disperse name servers to increase availability and site resiliency
  6. Use hidden primary to minimize configuration errors leading to Denial of Service (DoS) and to eliminate DoS targeting primary servers for zones
     + 1. Considerations for Recursive Caching Servers
  7. Use dedicated external name servers to eliminate cache poisoning
  8. Disperse name servers to increase availability and site resiliency
  9. Use hidden primary to minimize configuration errors leading to DoS and to eliminate DoS targeting primary servers for zones
     + 1. Considerations for Internal Authoritative Servers
  10. Set up DNS forwarding to isolate name server functions and to maintain tighter security boundary
  11. Disperse name servers to increase availability and site resiliency
  12. Use “hidden” primary name server to minimize configuration errors leading to DoS
  13. Evaluate DNSSEC to eliminate cache poisoning and to maintain DNS integrity
      + 1. Deliverables for the Agency to verify successful performance of the task:
  14. The contractor shall produce DNSSEC configurations, depicted as modified Figure 1 in the Attachment I, for each Agency HQ and Office sites, for Agency comments, approval, and signoff.

### Sub-task 4 –DNSSEC Servers’ Platform and Administration Rules

The contractor shall develop [or recommend] DNSSEC servers’ platforms for each Agency HQ and Office sites and DNSSEC administration rules for the proposed new Agency DNSSEC configurations/ architecture. More specifically, the contractor shall develop [or recommend] the following:

* + - 1. The contractor shall develop [or recommend] DNSSEC Server platforms
  1. Hardware and operating system

1. Hardware platform (e.g., HP server)
2. OS types (e.g., Windows, Linux)
   1. DNSSEC-aware software (nameserver, resolver)
3. DNSSEC capable nameserver (e.g., open source BIND 9 from Internet Systems Consortium)
4. DNSSEC capable resolver
   1. DNSSEC database
5. Zone file
6. Configuration file
   * + 1. The contractor shall develop [or recommend] DNSSEC administration policy/rules, addressing the following, at a minimum:
   1. Choice of algorithms and key sizes (TSIG and DNSSEC)
   2. Key management (generation, storage, and usage)
   3. Public key publishing and setting up trust anchors
   4. Key rollover frequency (scheduled and emergency) for key-signing keys (KSKs) and zone-signing keys (ZSKs), including a grace period, during which both the old and new keys are to be considered valid to allow for messages in transit during a key rotation, otherwise it might be rejected as invalid.
   5. DNS parameters, including times-to-live (TTLs) for records
   6. Zone re-signing frequency
   7. Signature expiration date
   8. Validity times for a zone and its signing keys
   9. Use of Next Secure (NSEC) vs. NSEC3 records
   10. Synchronization of authoritative nameserver and caching resolver when DNSSEK keys are changed or updated to prevent DKIM, DNSSEC, and SPF transaction failure.
   11. Methods to secure the private key in a secure place with access control list. Note: once the key is compromised, all records must be unsigned and resigned with a different key.
       * 1. The contractor shall develop [or recommend] DNS Registration rules/policy
   12. Decommissioning and retiring of old Agency domain names
   13. Must be reflected at the .gov root level (repository: Verisign); otherwise, unreachable or not responding servers will create an attack vector that cannot be prevented by DNSSEC.
   14. GSA registration of valid Agency domain names for record keeping (email: [registrar@dotgov.gov](mailto:registrar@dotgov.gov))
   15. Top Level Domain (TLD) nameserver registration for DNS operation for Root Trust-Anchor
7. Verisign for .gov
8. Internet Assigned Numbers Authority (IANA) for others (<https://www.iana.org/dnssec/>)
   * + 1. Deliverables for the Agency to verify successful performance of the task:
   1. DNSSEC Server Platform types, for each Agency HQ and Office sites, for Agency comments, approval, and signoff
   2. DNSSEC Servers administration policy/rules, for Agency comments, approval, and signoff
   3. DNS Registration rules/policy, for Agency comments, approval, and signoff

### Sub-task 5 – DNSSEC Testing and Deployment Roll-out Plan

The contractor shall develop [or recommend] a DNSSEC Testing and Deployment roll-out plan that lists DNSSEC hardware and software to be purchased and describes how it will be upgraded to DNSSEC and made operational in the production network. More specifically, the contractor shall:

* + - 1. The contractor shall develop [or recommend] DNSSEC Testing sequences and schedules for each site (Agency HQ and Office sites)
      2. The contractor shall develop [or recommend] DNSSEC Roll-out and Deployment sequence
  1. Flash cut or roll-out in the same sequence as being tested
     + 1. The lists of DNSSEC hardware and software that needs to be purchased for each Agency HQ and Office site(s).
       2. The contractor shall develop [or recommend] Deliverables for the Agency to verify successful performance of the task:
  2. Testing and roll-out plan for Agency comments, approval, and signoff.
  3. Spreadsheet of hardware and software to be purchased for each Agency HQ and Office site(s) for Agency comments, approval, and signoff.

## Task 2 – Set Up Test Lab

Lab testing minimizes the risk of running tests that could potentially cause disruptions or introduce a security risk if deployed on the production network. Many unexpected results during DNSSEC deployment are due to the misconfiguration of DNS servers and key generation required to support DNSSEC. This underscores the importance of testing, training and providing hands-on experience before DNSSEC is deployed in an operational environment. The test environment in the DNSSEC Test Lab (henceforth referred to as *Agency Test Pilot Zone*) should resemble the target DNSSEC environment (for Agency HQ and Office sites, henceforth referred to as *Agency Production Zones*) as closely as possible.

The contractor may provide suggestions and options to the Agency for using a virtualized (software-based) Test Lab and environment if doing so is more cost-effective.

### Sub-task 1 – Test Lab Installation

The contractor shall develop and install [or recommend] a Test Lab, as per the following:

* + - 1. The contractor shall develop [or recommend] DNSSEC Configurations (as developed in Task 1 Sub-task 3) in the DMZ and in the Internal Network for
  1. Agency HQ
  2. Agency Office sites
     + 1. The contractor shall ensure that it is able to test each Agency HQ and Office site (*Agency Production Zones*) as the *Agency Test Pilot Zone*
       2. During testing, the contractor shall ensure [or recommend] protection of the DNS host platform, DNS software, and DNS data for integrity and availability, using the following approaches:
  3. Host Platform Protection Approaches
     1. Running a secured OS (Unix, Windows)
     2. Securing OS configuration
  4. DNS Software Protection Approaches

1. Running the latest version of nameserver software, or an earlier version with appropriate patches
2. Running nameserver software with restricted privileges
3. Isolating name server software
4. Setting up a dedicated nameserver instance for each function
5. Removing name server software from non-designated hosts
6. Creating a topological and geographical dispersion of authoritative nameservers for fault tolerance
7. Limiting IT resource information exposure through two different zone files in the same physical nameserver (termed as split DNS) or through separate nameservers for different client classes
8. Review, evaluate, and incorporate, as applicable, additional NIST specified checklists for Guidelines for Securing DNS Hosting Environment
   * + 1. Checklist items 1 through 6 (see Attachment J, Section J.1)
   1. The contractor shall develop [or recommend] DNS Zone file Protection approaches
9. Develop the zone file integrity checker for database of necessary constraints for desirable field values (ranges or lists) in the various RRs of zone file for RRs in an unsigned zone but also for additional RRs in a signed zone (zones that have implemented the DNSSEC specification) for the content control of Zone file.
   * + 1. Deliverables for the Agency to verify successful performance of the task:
   1. Fully functional Test Lab, with documentation, to test DNSSEC configurations for each Agency HQ and Office sites (*Agency Production Zones*), for Agency comments, approval, and signoff.

### Sub-task 2 – Test Lab Connectivity to NIST/DHS/Sparta SNIP System

The contractor shall develop [or recommend] connectivity to NIST/DHS/Sparta SNIP infrastructure for testing *Agency Test Pilot Zone* for DNSSEC, as per the following steps.

* + - 1. The contractor shall coordinate, on behalf of the Agency, to participate in the NIST/DHS/Sparta Secure Naming Infrastructure Pilot (SNIP) system for testing DNSSEC deployment [http://www.dnsops.gov/ to participate in the pilot program]. Note: In addition to standard network connectivity, the SNIP servers also have an additional IPv6 enabled Internet2 connection. This allows the dnsops.gov zone to be reachable through both IPv4 and IPv6 (for those with an Internet2 connection).
      2. Note: NIST/DHS/Sparta SNIP system provides signed dnsops.gov root and act as a registrar for signed subzones and participating Agency will act as delegated subzones from the dnsops.gov parent zone. This will allow DNSSEC testing without obtaining new .gov delegations for testing purposes and without affecting the *Agency Production Zone* by the following procedures:
  1. First, use basic SNIP delegation from the SNIP domain (dnsops.gov) and attempt to mirror the current operational procedures they currently do with their .gov domain (i.e., incrementally from current operation to targeted DNSSEC operation, if required)
  2. Second, sign this new zone with DNSSEC, and develop and test new procedures required to maintain a digitally signed DNS zone.
     + 1. Deliverables for the Agency to verify successful performance of the task:
  3. Demonstrate, with documentation, that the test lab is successfully integrated with the NIST/DHS/Sparta SNIP infrastructure and able to perform DNSSEC testing.

## Task 3 – Convert, Test, and Archive DNSSEC Servers

The overall task for converting, testing, and archiving of DNSSEC servers for each Agency HQ and Office sites (*Agency Production Zones*) includes the following steps:

* + - 1. Upgrade existing DNS facilities to a level that includes DNSSEC functionality and establish key generation and management facilities and procedures; and, provide associated testing, validation, documentation, archiving DNS server(s) images/database to allow for flush-cutover or cutover as being tested, and training as needed. In addition, it will also entail real-time proactive security monitoring, rapid troubleshooting, and service restoration.
      2. Converting, testing, and archiving DNSSEC Servers for each Agency HQ and Office sites (*Agency Production Zones*) will be done one site at a time, as per the testing/implantation schedule developed in Task 1 Sub-task 5
      3. Taking a phased approach to DNSSEC Deployment will allow the Agency to prioritize aspects of the deployment as the project progresses. This minimizes the need to install and maintain deployment technologies that will eventually be removed.

### Sub-task 1 – Implementation Checklists for DNS Security

The contractor shall develop [or recommend] Implementation Checklist to secure DNS, as per the following steps.

* + - 1. The contractor shall develop [or recommend] DNSSEC Implementation checklists
  1. For overall, the contractor shall
  2. Ensure recursive and authoritative DNS servers are not the same machines
  3. Eliminate split-DNS in the DNS configuration from the environment by limiting IT resource information exposure through two different zone files in the same physical name server (termed as split DNS) or through separate name servers for different client classes (see also Task 2 Sub-task 1).
  4. When implementing DNSSEC, stand up new DNS servers rather than upgrading or modifying existing servers. This facilitates rapid back-out and restoration to the previous state in the event something goes wrong
  5. Identify the correct points of contact for technical and managerial authority over DNS
  6. Use dotgov.gov capabilities to enable an Agency-wide view of the domain name inventory.
  7. Develop how to handle increased DNSSEC packet sizes above the original UDP packet limit of 512 bytes. When this occurs, a DNS client could attempt to use TCP port 53 instead. Some organizations may still have packet filtering rules to block DNS over TCP
  8. For External Authoritative Servers, the contractor shall
     1. Utilize DNS resolution blocking and logging to tighten security control
     2. Turn off all services except for DNS to minimize Denial of Service (DoS) and impact of security vulnerabilities of other services
     3. Restrict access to DNS ports to outside users to minimize DoS and increase defense depth
     4. Use authenticated zone transfers to prevent compromised Zone transfer data
     5. Disable Dynamic DNS Updates (DDNS) to eliminate unauthorized DNS updates
     6. Enable DNSSEC to sign zones to minimize cache
  9. For Recursive Caching Servers, the contractor shall

1. Utilize DNS resolution blocking and logging to tighten security control
2. Turn off all services except for DNS to minimize DoS and impact of security vulnerabilities of other services
3. Restrict access to DNS ports to outside users to minimize DoS and to increase defense depth
4. Use authenticated zone transfers to prevent compromised Zone transfer data
5. Disable DDNS to eliminate Unauthorized DNS updates
6. Enable DNSSEC to sign zones to minimize cache
   1. For Internal Authoritative Servers, the contractor shall
7. Define query-list to tighten control and to minimize DoS
8. Block access from outside to minimize DoS
   1. The contractor shall review, evaluate, and incorporate, as applicable, the following NIST specified DNSSEC implementation checklists to guard against DNS Threats:
9. The contractor shall use the following guidelines, as applicable, for Securing DNS Transactions
   * + 1. Checklist items 7 through 14 (see Attachment J, Section J.2)
10. The contractor shall use the following guidelines, as applicable, for Securing DNS Query/Response
    * + 1. Checklist items 15 through 17 (see Attachment J, Section J.3)
11. The contractor shall use the following guidelines, as applicable, for Minimizing Information Exposure through DNS Data Content Control
    * + 1. Checklist items 18 through 27 (see Attachment J, Section J.4)
        2. Deliverables for the Agency to verify successful performance of the task:
    1. The contractor shall produce fully documented Implementation Checklists for DNS Security for Agency comments, approval, and signoff.

### Sub-task 2 – Test Plans for DNS Threats

The contractor shall develop [or recommend] Test Plans for the following DNS Threats:

* + - 1. Denial of Service (DoS)
  1. DoS can be initiated intentionally either by malicious attacker or unintentionally by a valid user/system. The effect is that the DNS services are overloaded with requests and not able to handle valid requests. DoS can also result when DNS data is incorrectly modified (either maliciously or unintentionally) thus not allowing connectivity to those services
     + 1. Cache Poisoning
  2. DNS client is redirected to different set of IP addresses for valid names. The user is not aware that the traffic isn’t being directed to the “correct” servers.
     + 1. Compromised Zone transfer data
  3. DNS client is redirected to different set of IP addresses for valid names. The user is not aware that the traffic isn’t being directed to the “correct” servers.
     + 1. Unauthorized Updates
  4. For DNS servers supporting Dynamic DNS Updates (DDNS), the client can issue DDNS update to automatically update the particular zone with data.
     + 1. Deliverables for the Agency to verify successful performance of the task:
  5. The contractor shall produce documentation for the above test plans for Agency comments, approval, and signoff.

### Sub-task 3 – DNSSEC Key Generation and Management Procedures

The contractor shall develop [or recommend] DNSSEC Key Generation and Management Procedures as follows:

* + - 1. For Asymmetric Key Requirements, the contractor shall
  1. Separate cryptographic keys (referred to as "Key Signing Keys" or KSKs) shall be used to sign the DNSKEY and DS RRSets then are used to sign all the other RRSets (including providing an additional signature for the DNSKEY RRSets as well) in any DNS Query/Response transaction (the keys that are used to sign all the RRSets in a DNS Query/Response transaction are referred to as "Zone Signing Keys" or ZSKs).
  2. Public cryptographic keys for Agency domains delegated from the ".gov" top level domain must be provided to the ".gov" repository (Verisign) to upload KSKs directly when authorized or via Agency staff in a secured manner.
  3. Public cryptographic keys for Agency domains delegated from top level domains other than the ".gov" top level domain (if any) must be provided to the IANA trust anchor repository to upload KSKs directly when authorized or via Agency staff in a secured manner.
  4. Asymmetric public/private key pairs shall be generated for use as Key Signing Keys or Zone Signing Keys as RSA asymmetric key pairs suitable for use with the RSA-SHA 256 digital signature algorithm
  5. At a minimum, the hosts used for storage of private copies of KSK keys must meet or exceed the requirements listed for Security Level 3 within the FIPS 140-2 and for the ZSKs in read-only storage only.
  6. All Key Signing Keys must be changed (rolled over) once per year or Agency-specific interval as identified in Task 1 Sub-task 4 above.
     + 1. For Symmetric Key Requirements, the contractor shall
  7. All DNS zone file transfers and Dynamic update transactions shall be digitally signed in accordance with the Transaction Signature (TSIG) standard, IETF RFC 2845
     + 1. The contractor shall develop automated scripts or automated tools to streamline the signing of the records as well as zone/key singing key roll-over process.
       2. For Performance metrics, the contractor shall ensure
  8. Time Synchronized to NTP shall be within 5 Seconds (Primary/Secondary Nameserver) for 99% of the cases
  9. Configuration/Key Change
  10. Shall be within 5 hours for a Normal priority change (e.g. ZSK or Trust Anchor key)
  11. Shall be within 2 hours for an Urgent priority change (e.g., KSK)
      + 1. Deliverables for the Agency to verify successful performance of the task:
  12. The contractor shall produce fully documented DNSSEC Key Generation and Management Procedures for Asymmetric Keys and Symmetric Keys for Agency HQ and Office sites (as applicable) for Agency comments, approval, and signoff.
  13. The contractor shall develop fully documented automated scripts or automated tools for DNSSEC Key Generation to streamline the signing of the records as well as zone/key singing key roll-over process for Agency comments, approval, and signoff.

### Sub-task 4 – Conversion of Production Zone DNS Servers

For each selected *Agency Production Zone*, as per testing/implantation schedule developed in Task 1 Sub-task 5, the contractor shall convert and archive the existing *Agency Production Zone* DNS server(s) in the Internal Network and/or in the DMZ to be tested in the Test lab as *Agency Test Pilot Zone*, as follows:

* + - 1. The contractor shall populate appropriate DNSSEC server(s) in the Test Lab with Production zone data as per DNSSEC server configuration rules as developed in Task 1 Sub-task 3 above and per implementation checklist and DNSSEC key generation procedure as developed in Task 3 Sub-tasks 1 and 3 above.
  1. For *Authoritative Nameserver*, the contractor shall
     1. Check zone file(s) for any possible integrity errors
        + 1. Develop [or recommend] the zone file integrity checker for database of necessary constraints for desirable field values (ranges or lists) in the various RRs of zone file for RRs in an unsigned zone but also for additional RRs in a signed zone (zones that have implemented the DNSSEC specification) for the content control of Zone file.
     2. Generate asymmetric key pair for each zone and include them in the zone file
     3. Sign the zone
     4. Load the signed zone onto the server
     5. Configure name server to turn on DNSSEC processing
  2. For *Caching Nameserver*, the contractor shall

1. Obtain one or more trust anchors for zones Agency DNS administrator wants validated
2. Configure resolver to turn on DNSSEC processing
   * + 1. The contractor shall archive each converted *Agency Production Zone* DNS server(s) for later testing in the Test lab as *Agency Test Pilot Zone*
       2. Deliverables for the Agency to verify successful performance of the task:
   1. Fully documented and archived database containing converted DNS servers for each Agency HQ and Office sites for Agency comments, approval, and signoff.

### Sub-task 5 – Test and Archive DNSSEC Servers in the Test Lab

The contractor shall test selected *Agency Production Zone,* as per testing/implantation schedule developed in Task 1 Sub-task 5, in the Test Lab as *Agency Test Pilot Zone* with the NIST/DHS/Sparta SNIP infrastructure and Archive DNSEC servers’ images/databases for later cutover of Agency DNS infrastructure. The contractor shall perform the following steps, at a minimum:

* + - 1. The contractor shall ensure *Agency Test Pilot Zone* is working operationally the same as the *Agency Production Zone* being tested
      2. The contractor shall execute Test Plans for verifications, as developed in Task 3 Sub-tasks 2, for DNS threats (Denial of Service, Cache Poisoning, Compromised Zone Transfer data, and Unauthorized Updates) for testing DNSSEC
      3. The contractor shall archive tested *Agency Test Pilot Zone* servers’ images (database) to be used during *Agency Production Zone* cutover to DNSSEC per Task 4
      4. Deliverables for the Agency to verify successful performance of the task:
  1. The selected (Agency HQ or Office sites) *Agency Production Zone* is successfully tested for DNSSEC and databases achieved for later cutover of Agency DNS infrastructure in accordance with Task 4.

### Sub-task 6 – Convert, Test, and Archive DNSSEC Servers for Each Site

The contractor shall test all *Agency Production Zones* (i.e., Agency HQ and Office sites) as *Agency Test Pilot Zones,* one site/zone at a time, with the NIST/DHS/Sparta SNIP infrastructure and Archive DNSEC servers’ images/databases for later cutover of Agency DNS infrastructure, as per Task 3 Sub-Tasks 4 and 5 above.

* + - 1. The contractor shall repeat Task 3 Sub-task 4 and Sub-task 5, for each *Agency Production Zone* (i.e., each Agency HQ and Office sites) for successful conversion and testing of DNS infrastructure.
      2. Deliverables for the Agency to verify successful performance of the task:
  1. All *Agency Production Zones* (Agency HQ or Office sites) are successfully converted and tested for DNSSEC, and databases achieved for later cutover of Agency DNS infrastructure in accordance with Task 4.

## Task 4 – DNSSEC Deployment/Cutover of Agency Production Zones

The contractor shall develop the following for the DNSSEC deployment/cutover of Agency Production Zones at Agency HQ and Office sites:

* + - 1. The contractor shall develop [or recommend] DNS Outsourcing Options
  1. Agencies may choose to outsource all or part of their DNS infrastructure. The reasons for doing so are that trusted third parties may be better able to provide the security, geographical dispersion and high-availability safeguards than an internal network data center.
  2. Develop the costs and benefit of DNS outsourcing for Agency considerations.
     + 1. The contractor shall install/replace DNSSEC servers in the DMZ and in the Internal Network with the tested DNSSEC servers with the archived databases for each Agency Production Zone to be cutover (HQ and sites)
  3. As a Flash cut or roll-out in the same sequence as being tested as developed in Task 1 and Sub-task 4.
  4. Cutover to be done in the business off-hours or in the weekend to allow for roll-back in case of problem encountered
  5. Send copy of public key to the parent (VeriSign for .gov and IANA for non .gov) for secure delegation
     + 1. The contractor shall test each *Agency Production Zone* (HQ and sites) DNSSEC to ensure there is no problem to the operational traffic
       2. Deliverables for the Agency to verify successful performance of the task:
  6. DNSSEC Outsourcing options (all or part of their DNS infrastructure) for Agency comments, approval, and signoff.
  7. Completed the cutover from DNS to DNSSEC in the Agency DNS infrastructure

## Task 5 –Operational Procedures for Administration of DNSSEC

The contractor shall develop Operational Procedures for ongoing Administration of DNSSEC, as follows:

* + - 1. The contractor shall address the following key areas, at a minimum, to develop the ongoing administration of DNSSEC
  1. DNS parameters, including times-to-live (TTLs) for records
  2. Key length and algorithm
  3. Zone re-signing frequency
  4. Key rollover frequency (scheduled and emergency) for key-signing keys (KSKs) and zone-signing keys (ZSKs)
  5. Signature expiration date
  6. Validity times for a zone and its signing keys
  7. Use of Next Secure (NSEC) vs. NSEC3 records
  8. Monitoring of DNS server logs for developing incidence response
     + 1. The contractor shall review, evaluate, and incorporate, as applicable, the following NIST specified DNSSEC guidelines for DNS Security Administration Operations
  9. Checklist items 28 through 34 (see Attachment J, Section J.5)
     + 1. Deliverables for the Agency to verify successful performance of the task:
  10. Provide *Operational Procedures for ongoing Administration of DNSSEC* document for Agency comments, approval, and signoff.

## Task 6 – Authentication of Agency Email System with DKIM and SPF

DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF), with extensions to the Domain Name System Security Extensions (DNSSEC) DNS-records, can be used to validate domains and correlate them with IP addresses. If none of these technologies are implemented, a domain validating message transfer agent (MTA) may “fall back” to a simple “white list” or “black list.” In either case, domain validation is critical to making policy decisions regarding the delivery of mail

The process of signing outbound messages and verifying the signature is typically done by the e-mail servers at each end - not by end-users client software. DKIM uses DNS TXT-records to define policy and public encryption keys for a domain name. There are basically two types of DNS records used by DKIM - policy records and public key records.

SPF domains have to publish at least two directives: a version identifier and a default mechanism as an SPF record (e.g., when an agency.gov never sends mail, it is defined as: agency.gov. TXT "v=spf1 -all").

### Sub-task 1 – Email Authentication Planning and System Analysis

The contractor shall perform [or recommend] the following steps for the Email Authentication of the Agency Email system:

* + - 1. The contractor shall define Email Authentication for the Agency Email system in accordance with the Agency CIO security policy
  1. Define authentication System
     1. DKIM or SPF or both DKIM and SPF
  2. Develop deployment/roll-out sequences and schedules for Agency HQ and Agency sites (if different)
     + 1. The contractor shall develop inventory of Agency Email services and platforms at HQ and Agency sites (if different) with capabilities to support DKIM, SPF, or both DKIM and SPF:
  3. Agency Email system

1. Google Mail or MS Windows/Exchange or Lotus Notes mail or other Email system
   1. Capabilities to support DKIM, SPF, or both DKIM and SPF
2. Already built-in but not-enabled, or
3. Need new plug-in inserts, or
4. Need new upgrade
   * + 1. The contractor shall develop implementation checklists for
   1. Use of SPF and DKIM in combination to ensure the sending message server is permitted to send (by SPF) and to ensure the authenticity of the digital signature (by DKIM)
   2. Coordinate DKIM and SPF adoptions across all current mail relays
   3. Use SPF for domains that will never send e-mail
   4. Test all DKIM and SPF rule sets for correctness in a simulated environment before deployment
      * 1. Deliverables for the Agency to verify successful performance of the task:
   5. The contractor shall provide documentation of the following for Agency comments, approval, and signoff:
5. Spreadsheet of Agency Emails that support DKIM, SPF, or both DKIM and SPF as already built-in but not-enabled or need new plug-in inserts or need new upgrade
6. Transition roll-out plans and schedules
7. Implementation checklists

### Sub-task 2 – Deployment/Cutover of Email Authentication System

The contractor shall transition existing Agency Email server to DNSSEC-aware DKIM/SPF Email server as follows:

* + - 1. The contractor shall upgrade Agency Email software/platform with DKIM/SPF/both for email authentication using DNSSEC database
  1. Email system
  2. Enable or upgrade Email system with new version or plug-in for DKIM and/or SPF
  3. Convert existing Agency Email server (database) to the DNSSEC-aware DKIM/SPF Email server (database)
     + 1. The contractor shall configure DNS (DNSSEC) database by adding
  4. SPF TXT records to check for allowed (sender) hosts
  5. DKIM digital signatures records for required email fields (From, Subject, and message body or its initial part) to check for domain-level sender authentication
     + 1. The contractor shall develop Test Plans for
  6. Normal email operation
  7. DKIM Threats of spoofed/hijacked emails (From, Subject, and message body or its initial part)
  8. SPF Threats of unauthorized senders
     + 1. The contractor shall execute Test Plans for verification as follows
  9. In the Test Lab
     1. The contractor shall set up a Test Email Authentication system with few users for testing and verification, by installing
        1. DKIM/SPF Email system
        2. DNSSEC-aware DKIM/SPF Email server (database)
        3. DNS (DNSSEC) database with DKIM/SPF records
     2. The contractor shall execute Test Plans for verification
  10. In the production live environment

1. The contractor shall test Email Authentication in the production live environment, by upgrading/installing
   * + 1. DKIM/SPF Email system
       2. DNSSEC-aware DKIM/SPF Email server (database)
       3. DNS (DNSSEC) database with DKIM/SPF records
2. The contractor shall execute Test Plans for verification only during non-business hours for roll-back in case of failure
   * + 1. Deliverables for the Agency to verify successful performance of the task:
   1. The contractor shall provide documentation of the following for Agency comments, approval, and signoff:
      1. Updated spreadsheet (see Task 6 Sub-task 1) of Agency Emails for supporting DKIM, SPF, or both DKIM and SPF with actual implementation dates for
         1. Upgraded/enabled Email system for DKIM and/or SPF
         2. Converted Email server database for DNSSEC
      2. Test Plans to test Email system for DKIM and/or SPF
      3. Email Transition results

### Sub-task 3 –Administration of Email Authentication System

The contractor shall develop [or recommend] Operational Procedures for ongoing Administration of Email system for DKIM and SPF:

* + - 1. Operational Procedures
  1. Additional Email administration procedures that synchronize with the Agency DNSSEC administration procedures (see Task 5)
     + 1. Deliverables for the Agency to verify successful performance of the task:
  2. Fully documented Operational Procedures for ongoing Administration of Email system for DKIM and SPF for Agency comments, approval, and signoff.

# Labor Types

The offeror shall propose Labor Types for both professional and technical expertise that fully meet the requirements in Tasks 1-6 to support DNSSEC Deployment solutions, including full life cycle management as applicable, and the analysis, planning, design, specification, implementation, integration and management of network services and equipment before and after the Deployment.

Over the life of the Task Order, the offeror may propose any new labor and equipment that emerges in the telecommunications market.

The offeror shall provide:

* + - 1. Technical support and equipment to Government-site support locations and Support Delivery Points (SDPs), as identified in ***Attachment B – Support Locations***
      2. Daily network and security operations support and monitoring (NOC and SOC functions) performed at the Agency site or offeror site as identified in ***Attachment B – Support Locations***
      3. Proposed Labor Types for each Task as specified in ***Attachment D – Pricing Template***

Work locations are defined as Government or offeror sites:

* + - 1. **Government site**: The Contractor shall provide technical support and equipment when required to the locations identified in ***Attachment B – Support Locations***.
      2. **Contractor site:** The Contractor shall provide network and security operations support and monitoring when required, and this work may be performed at the Contractor’s NOC and SOC, respectively.

Proposed Labor Types for each Task shall include the Labor Type description, work location type, business day type, clearance status, and minimum qualifications. The Labor Types shall be provided using ***Attachment D – Pricing Template.***

## Personnel Requirements

The offeror has ultimate responsibility for managing the order, for achieving the performance results in each of the task areas, and for determining the appropriate staffing pattern in support of its technical approach.

* + - 1. The offeror shall provide experienced personnel to perform the required services. The Government and the offeror understand and agree that the services to be delivered are non-personal services and both parties recognize and agree that no employer-employee or master-servant relationships exist between the Government and the offeror and/or between the Government and the offeror’s employees.
      2. Offeror personnel shall conform to standards of conduct and code of ethics, which are consistent with those applicable to Government employees. Offeror personnel shall obtain authorization to have access to Agency support sites and Government facilities, and shall obtain Common Access Cards (CAC) for computer access.
      3. All offeror employees must be fluent in spoken and written English.
      4. Background Checks: All DNSSEC offeror employees must submit a Questionnaire for National Security Positions (SF-86) to the [Agency] Personnel Security Manager. A favorable SF-86 is required before gaining access to a U.S. Government LAN. The offeror, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the order.
      5. The contracting officer may require the offeror to remove from the job site any offeror employee who is identified as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population.
      6. In order to ensure a smooth and orderly startup of work, it is essential that the key personnel specified in the offeror's proposal be available [within xxx business days of the task order award or on the effective date of the order]. If these personnel are not made available at that time, the offeror must notify the contracting officer and show cause. If the offeror does not show cause, the offeror may be subject to action for default.
      7. The offeror-supplied personnel are employees of the offeror and under the administrative control and supervision of the offeror. The offeror, through its personnel, shall perform the tasks prescribed herein. The offeror must select, supervise, and exercise control and direction over its employees (including subcontractors) under this order. The Government shall not exercise any supervision or control over the offeror in its performance of contractual services under this order. The offeror is accountable to the Government for the action of its personnel.

## Proposed Personnel

The offeror must assemble a DNSSEC project team with the required knowledge and experience described in **Section 3.3: Special Qualifications & Certifications**.

The core project team should be a composed of qualified professionals with strong technical backgrounds and experience in designing large, complex DNSSEC configurations.

The offeror shall identify, by name, the proposed Key Personnel (i.e., the key management and technical personnel who will work under this order).

The proposed DNSSEC project team structure and an organizational chart must be included in the proposal, with the names, positions and resumes of proposed personnel.

## Special Qualifications and Certifications

The offeror shall ensure that its employees have all required professional certifications and licenses (current and valid) for each applicable task and labor type category before commencement of work. The offeror’s proposed personnel shall be proficient in the following technical and professional services skills:

**Task 1 – DNSSEC and Email Authentication Deployment Planning and System Analysis**

The Contractor shall propose appropriate Connections II Labor Type(s) and personnel experience levels (senior level or a mix of senior, mid, and entry levels) that meet the minimum required qualifications, based on the complexity and scale of the Agency’s current DNS production network.

**Sub-task 1 – Program Management Plan**

The Project Manager (PM) should possess the intellectual and leadership qualities necessary to manage, develop, articulate and carry out a vision for the DNSSEC Deployment project. The proposed personnel may be required to have a Program Management Plan (PMP) certification, and shall have experience developing a PMP for a large, complex DNSSEC configurations Deployment, and hands-on experience with all aspects of DNSSEC Deployment and security issues.

**Sub-task 2 – DNSSEC and Email Authentication Training Plan**

Personnel shall have experience providing DNSSEC configuration training at all levels of management.

**Sub-task 3 – DNSSEC Configuration /Architecture**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or Certified Information Systems Security Professional (CISSP) or equivalent, and hands-on experience with large, complex DNSSEC configurations.

**Sub-task 4 – DNSSEC Servers’ Platform and Administration Rules**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on administration experience with large, complex DNSSEC configurations.

**Sub-task 5 – DNSSEC Testing and Deployment Roll-out Plan**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in deploying large, complex DNSSEC configurations.

# Task 2 – Set UP Test Lab

**Sub-task 1 – Test Lab Installation**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in setting up a DNSSEC Test Lab.

**Sub-task 2 – Test Lab Connectivity to NIST/DHS/Sparta SNIP System**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integrating and testing DNSSEC in a lab, including security.

**Task 3 – Convert, Test, and Archive DNSSEC Servers**

**Sub-task 1 – Implementation Checklists for DNS Security**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in implementation and integration of large DNS configuration.

**Sub-task 2 – Test Plans for DNS Threats**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in DNS threats and testing in a live environment.

**Sub-task 3 – DNSSEC Key Generation and Management Procedures**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in developing DNSSEC key generation and management procedures.

**Sub-task 4 – Conversion of Production Zone DNS Servers**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration and testing in a live environment.

**Sub-task 5 – Test and Archive DNSSEC Servers in the Test Lab**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration and testing in a live environment.

**Sub-task 6 – Convert, Test, and Archive DNSSEC Servers for Each Site**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in IT database management, integration, and testing in a live environment.

**Task 4 – DNSSEC Deployment/Cutover of Agency Production Zones**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration, testing, and deployment/cutover of a large DNSSEC production configuration.

**Task 5 – Operational Procedures for Administration of DNSSEC**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level), and/or CISSP or equivalent, and hands-on experience in integration, testing, and administration of a large DNSSEC production configuration.

**Task 6 – Authentication of Agency Email System with DKIM and SPF**

**Sub-task 1 – Email Authentication Planning and System Analysis**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration and testing of Email system in a live environment.

**Sub-task 2 – Deployment/Cutover of Email Authentication System**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration and testing, and deployment/cutover of a large Email production environment.

**Sub-task 3 – Administration of Email Authentication System**

Personnel shall have minimum experience equivalent to Cisco certified network engineer (e.g., CCIE for senior level, CCNP for mid-level, and CCNA for entry-level) and/or CISSP or equivalent, and hands-on experience in integration and testing, and administration of a large Email production environment.

# Travel and Other Direct Costs (ODC / Un-priced Items)

## Travel

Travel under this task order is governed by Section G.5.1.2 of the Connections II contract and the instructions given in this section.

**Local Vicinity**: If travel within the local vicinity is required, travel reimbursements for local travel are not authorized; neither is the use of a Government vehicle.

**Distance Travel**: If travel outside the local vicinity is required, costs incurred by offeror personnel for travel, including costs of lodging, other subsistence, and incidental expenses, shall be considered reasonable and allowable only to the extent that they do not exceed the rates and amounts set by the Federal Travel Regulations. Refer to **FAR 31.205-46 (a)(2)(i)**.

As part of the Price Proposal, the Contractor shall provide any anticipated travel costs, to include origination, destination, and the number of trips, number of persons, and a breakdown of lodging, meals, transportation and related costs.

Prior written approval by the [Agency] contracting officer is required for all travel directly and identifiably funded by the [Agency] under this order. The Contractor shall therefore present to the contracting officer an itinerary for each planned trip, showing the name of the traveler, purpose of the trip, origin/destination (and intervening stops), and dates of travel, as far in advance of the proposed travel as possible, but in no event less than three weeks before travel is planned to commence.

For cost effectiveness, economy class travel must be used on all official travel funded under this Task Order. Business class travel should only be used under exceptional circumstances, and in compliance with the Federal Travel Regulations.

## Other Direct Cost (ODC / Un-priced Items)

The Contractor shall:

* + - 1. Provide a breakdown for un-priced items of any Other Direct Costs (ODCs) in the Price Proposal. The breakdown shall identify any “open market” items.
      2. Use ***Attachment E – Equipment, Support and Warranty Inventory*** to store and track equipment records by the task order number. The [Agency] may also task the Contractor to store additional information in this file.

# Inventory and Warranty

The Contractor shall:

* + - 1. Comply with **Section C.2.1.9: Warranty Service** of the Connections II contract to provide, at no additional cost to the Government, a minimum one-year system warranty, or the warranty provided by the Original Equipment Manufacturer (OEM) whichever is longer, for all hardware and software purchased under this order.
      2. Comply with **Section C.3.6:** Inventory **Management** of the Connections II contract to establish and maintain an Inventory File of equipment, equipment warranty, and maintenance services purchased under each of the Tasks. Each record of this file shall include the OEM’s name and contact number, the maintenance contractor’s name and local repair number, the date of acceptance, the date maintenance was performed (if available), a description of the maintenance action (if available), and the date that the warranty ends.

# Invoicing and Payment

The contractor shall meet and comply with the Billing and Invoice requirements as described in Sections C.3.4 Billing, G.5.1 General Billing Requirements, and G.6 Payment of Bills of the Connections II contract. The baseline requirements for Connections II contract for Invoicing and Billing including the handling of Associated Government Fee, approval for payment of supplies/services, resolution of billing disputes, and the option for Agency to pay by electronic funds transfer shall apply.

## Detail Billing Requirements

The offeror shall comply with the detail billing requirements defined in **Section C.3.4** and the general billing requirements in **Section G.5** of the Connections II contract when submitting a proper bill for each order.

## Invoice Address, Data Format and Delivery Method

The offeror shall be capable of directly billing each customer at the address given by the Agency in the order and shall also have the capability to centrally bill designated customers through GSA. The baseline requirements for direct and centralized billing as defined **Section C.3.4** of the Connections II contract shall apply.

### Invoice Address

The offeror shall send invoices directly to the address (electronic mail or postal/physical address) designated by the Agency’s authorized Ordering Entity. This address will be determined at the time the order is placed.

|  |
| --- |
| An Agency can receive invoices by electronic (email method), hard copy, or both. Suggested Requirements:  The offeror shall provide the signed original invoice via email:  [Agency provide email address here]  The offeror shall also provide via postal/physical address an additional copy of the invoice to the Contracting Officer and COR or provide [n] copies of the signed original to:  Name of Agency Department  POC Name/Position and Title  Email  Mailing Address  Street, City, Zip  Inquiries regarding payment of invoices should be directed to [Agency provide email address here] |

### Invoice Submission

The offeror shall comply with the detail billing requirements defined in Section C.3.4 and the general billing requirements in Section G.5 of the Connections II contract when submitting a proper bill for each order.

A proper invoice must include the following items:

1. Contractor name and address

2. Contractor representative

3. Contract number

4. Order number(s)

5. Accounting Control Transaction (ACT) number (assigned by the OCO on the order)

6. Period of performance (month services performed for work request orders, month

deliverable completed for fixed price orders)

7. Bill number

8. Customer’s name and address

9. For Fixed Price Orders, products delivered and accepted, listed by deliverable number;

for Time and Materials orders, labor charges accepted during the period of performance

10. Travel and per diem charges

11. Total billed amount

12. Prompt payment discount offered (if applicable)

### Billing Cycle and Data Elements

The offeror shall invoice on a monthly basis. The invoice shall include the period of performance covered by the invoice. All labor, equipment, equipment services and unpriced items (other direct costs) shall be reported, and shall be provided for the current billing month and in total from project inception to date. If subcontracting is proposed, one consolidated invoice from the prime contractor shall be submitted in accordance with other terms and conditions of the RFQ.​

|  |
| --- |
| The Agency has option to specify the format and agency-specific data elements for invoice content.  Suggested Requirements:  The offeror shall provide the invoice data in spreadsheet form with the following detailed information.  The listing shall include separate columns and totals for the current invoice period and the project to date. The following data elements shall be provided on the Invoice, at a minimum:   1. Labor Type (Employee) 2. CONNECTIONS II labor category 3. Monthly and total cumulative hours worked 4. Burdened hourly labor rate 5. Cost incurred not billed |

### Electronic Funds Transfer (EFT)

|  |
| --- |
| Agency has option to specify the method of delivery for invoice and payments.  Insert additional agency-specific requirements here.    Below is a standard ‘boilerplate” requirements for EFT. |

The offeror shall cooperate with the government to allow payment of bills via Electronic Funds Transfer (EFT) to the extent feasible in accordance with **Section G.6.3 Use of Electronic Funds Transfer** of the Connections II contract.

## Billing for Other Direct Costs (ODCs) or Unpriced Item

The offeror may invoice monthly on the basis of cost incurred for ODC or unpriced item.  The invoice shall include the period of performance covered by the invoice and the item number and title.

|  |
| --- |
| Agency has option to specify the format and agency-specific data elements for ODC and unpriced items.  Suggested Requirements:  The offeror shall provide the following detailed information for each invoice submitted, as applicable.  Spreadsheet submissions, in MS Excel format, are required.   1. ODCs or unpriced items purchased 2. Date delivery accepted by the Government 3. ODC or unpriced item number 4. Project to date totals 5. Cost incurred not billed 6. Remaining balance of each item |

### Invoice for Travel Expenses

The offeror may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulations/Federal Travel Regulation (JTR/FTR).  Long distance travel is defined as travel over 50 miles.  The invoice shall include the period of performance covered by the invoice, and the CLIN number and title.  Separate worksheets, in MS Excel format, shall be submitted for travel.

|  |
| --- |
| Agency has option to specify the format and agency-specific data elements for submitting Travel charges. Suggested Requirements:  The offeror shall provide the following detailed information for each invoice submitted for travel expenses. The Total Cost for Travel shall identify all current travel on the project and their total CLIN/Task costs billed.  The listing shall include separate columns and totals for the current invoice period and the project to date:   1. Travel Authorization Request identifier, approver name, and approval date 2. Current invoice period 3. Names of persons traveling 4. Number of travel days 5. Dates of travel 6. Number of days per diem charged 7. Per diem rate used 8. Total per diem charged 9. Transportation costs (rental car, air fare, etc.) 10. Total charges 11. Explanation of variances exceeding 10% of the approved versus actual costs 12. Indirect Handling Rate. |

[Agency may add Agency-specific billing and invoice payment processing requirements here]

# Electronic and Information Technology Accessibility Standards (Section 508)

All Electronic and Information Technology (EIT) procured through this task order must meet the applicable accessibility standards at 36 CFR 1194, unless an Agency exception to this requirement exists. **Section 508 Compliance Summary** is viewable at: <https://www.section508.gov/index.cfm?fuseAction=stdsSum#technical>

The offeror shall indicate for each line item in the schedule whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the proposal must indicate where full details of compliance can be found (e.g., the offeror's website or other exact location).

# Proposal Instruction to Offerors

**NOTE TO OFFERORS**: This section provides instructions to prospective offerors on preparing and submitting a proposal in response to this solicitation.

# SOLICITATION CLOSING DATE AND TIME:

**ALL OFFERS MUST BE RECEIVED ON OR BEFORE 3:00 PM** [Time Zone] **ON:** [DD MM YYYY].

# REQUIRED SUBMISSIONS:

Proposal shall be submitted to the attention of: [Agency Point of Contact]

**HARD COPY ADDRESS:** **ELECTRONIC COPY:**

* + - * Agency Name and Email Address
      * POC Name
      * Mailing Address
      * Telephone
      * Email

No offer received after the due date and time will be considered.

## General Instructions

**MATERIALS SUBMITTED:** The Offeror is advised that all submissions and related material become the property of the U.S. Government and will not be returned. The technical and price proposals, if accepted by the Government, will form binding parts of the Task Order that results from this solicitation. Therefore, care must be taken to properly address the requirements set forth in each of the Tasks. In the event of any conflict between the Connections II Contract and the proposal in any resulting Task Order, the Connections II Contract shall govern.

**FORMAT:** All materials shall be in typeface Times New Roman 11 point (or Arial 11 point), double-spaced on 8½” x 11” white paper with one inch margins all around. Tables and illustrations may use a reduced font style, but not less than 8 point, and may be single-spaced. **Each page must identify the submitting Offeror in the header or footer.**

The offeror’s proposal shall consist of physically separate volumes that are individually titled and numbered on the exterior of the top covers as stated below. **DO NOT INCLUDE PRICING IN THE TECHNICAL AND PAST PERFORMANCE VOLUMES:** THE CONTRACTOR IS ADVISED THAT COMBINING TECHNICAL AND PRICING VOLUMES IN THE OFFEROR’S PROPOSAL IS NOT RESPONSIVE TO THE SOW.

The required number of each type of proposal volume is shown below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VOLUME | VOLUME TITLE | COPIES | FORMAT | PAGE LIMITATIONS |
| Vol. I | TECHNICAL PROPOSAL   * Technical approach * Management approach | 1 Hard Original +  [n] Hard Copies +  [n] Electronic Copies | PDF | 1 page Executive Summary  [n] pages per Task Order |
| Vol. II | PRICE PROPOSAL | 1 Hard Original +  [n] Electronic Copies | EXCEL – Pricing Template | No page limit |
| Vol. III | APPENDICES  PAST PERFORMANCE  RESUME OF KEY PERSONNEL  PROJECT MANAGEMENT PLAN (PMP  TRAINING PLAN (TP) |  | PDF  PDF  PDF  PDF | [n] pages  [n] pages maximum per Resume  No page limit  No page limit |

**PROPRIETARY DATA:** Each page of the offeror’s proposals must be reviewed and marked as to proprietary data content by the Offeror in accordance with **FAR 52.215-1 Instruction to Offerors**. Additionally, refer to **FAR 3.104-4 Disclosure, Protection and Marking of Contractor Bid,** to ensure compliance. A single blanket statement at the front of the proposal is not acceptable. Failure to mark every page will subject the proposal to public release through Freedom of Information Act (FOIA) requests.

## Preparation of Technical Proposal

The Technical Proposal in response to this solicitation should address how the offeror intends to carry out the Statement of Work contained in **Section C**. The offeror’s Technical Proposal must demonstrate a clear understanding of the requirements, the adequacy of the solution approach in meeting the goals and objectives of the DNSSEC Deployment project, and fulfill the offeror’s program implementation responsibilities.

Technical Proposals are limited to [n] pages in length and shall be written in English. Each page must be numbered consecutively. Pages that exceed the page number limitation will not be evaluated.

Any page in the Technical Proposal that contains a table, chart, graph, etc., not otherwise specifically excluded below, is included within the above page limitation for the Technical Proposal. All critical information from appendices should be identified and summarized in the Technical Proposal. Not included in the page limitation are the following:

* Cover/title page
* Table of contents
* Executive summary
* Dividers
* Table summarizing qualifications of proposed personnel

The Technical Proposal will be organized by the technical evaluation criteria listed in **Section 7.3**, as clarified further below:

1. Technical Approach and Project Management
   * + Task 1
     + Task 2
     + Task 3
     + Task 4
     + Task 5
     + Task 6
2. Deliverables
   * + Project Management Plan (PMP)
     + Training Plan (TP)
3. Proposed Personnel Qualifications and Certifications
   * + Resumes
4. Past Performance
   * + Past Performance Worksheet

The Technical Proposal shall include a detailed description of the offeror’s technical solution for each task including the associated equipment, equipment services, labor, and installation. At a minimum, the offeror must organize its response in the Technical Proposal to contain and follow the information set forth herein.

**Executive Summary** (5-page size limit; does not count against Volume I [n] page limit)

This section is to summarize the key elements of the offeror’s strategy, approach, methodologies, personnel and implementation plan. The Executive Summary will not count towards the page limitation and must not exceed 5 pages in length.

**Technical Approach and Implementation** (See **Section 2.1 – 2.6**) (Volume I [n] page size limit)

The offeror’s Technical Approach and Implementation must demonstrate a clear understanding of the requirements. The Technical Approach and Implementation must include a description of the conceptual approach and the general strategy (i.e., implementation plan, testing methodology and risk mitigation strategy) being proposed for the implementation and Deployment of the Agency’s network, systems and operations support from DNS to DNSSEC. The Technical Approach and Implementation shall be specific, complete, presented concisely, responsive to the instructions contained herein and should address how the offeror intends to fulfill the statement of work. Marketing literature is not acceptable.

**Management Approach** - The offeror’s Management Approach shall provide a summary of the Project Management Plan and the rationale behind the selected organization and staff chosen, including qualifications of the selected staff. The plan shall also demonstrate that the offeror has the corporate capabilities to execute the submitted PMP.

**Deliverables**

* 1. **Project Management Plan** (See **Section 2.1.1**) (no size limit; submit as an Attachment)

The offeror shall submit a draft Project Management Plan (PMP) based on its proposed technical approach using ***Attachment A - PMP Template***. The offeror’s PMP will be evaluated as part of Technical Approach and Project Management. The PMP shall be submitted as an Attachment with no size limit.

* 1. **Training Plan** (See **Section 2.1.2**) (no size limit; submit as an Attachment)

The offeror’s Training Plan (TP) and training delivery methods must include a clear description and understanding of the training requirements as described in the SOW (i.e., training delivery methods, scheduling and curriculum). The offeror shall demonstrate its capability to provide DNSSEC training in support of the implementation of the DNSSEC Deployment.

**Qualifications of Proposed Personnel**

The offeror shall describe the skills, qualities and capacities of its proposed Project Manager and other key personnel to meet both the minimal qualifications described in **Section 2.0** as well as their ability to meet the technical and implementation challenges of the proposed implementation approach.

1. **Resumes** (See **Section 3.1 – 3.3**) (n-page size limit; submit as an Attachment)

The offeror shall include, in an annex, the resumes for all the proposed key personnel candidates and other long-term technical experts, up to a total number of [n]. Key personnel resumes may not exceed [n] pages in length and shall be in chronological order starting with most recent experience.

Each resume shall be accompanied by a signed letter of commitment from each candidate indicating his/her: (a) availability to work in the stated position, in terms of months; after award; and (b) intention to support and work for a stated term of the service. The offeror's proposed personnel shall also submit a minimum of three (3) references of professional contacts within the last three years. The offeror should provide a current phone, fax address, and email address for each reference contact.

**Past Performance** (See **Section 7.1**) (no size limit; submit as an Attachment)

# Past Performance Worksheets

The offeror shall use the past performance template provided in ***Attachment F – Past Performance Worksheet****.* The offeror shall provide [n] past performance references for projects of a similar type, size and scope to that described in the solicitation.

# PAST PERFORMANCE INSTRUCTIONS

Offerors shall submit the following information as part of their proposal:

1. The offeror shall describe its past performance directly related to contracts it has held within the last 3 years that are similar in scope, magnitude and complexity. Offerors shall provide a minimum of three (3) relevant examples of Deployment from a DNS to a DNSSEC environment.
2. Offerors shall provide relevant past performance documentation and references for services comparable to those described in the SOW. Past performances listed may include those entered into by the Federal Government, state and local government agencies, and commercial customers.
3. Offerors should notify each of their private-sector (commercial) references that they may be contacted by the [Agency] and authorize them to provide the past performance information requested. References other than those identified by the offeror may be contacted by the Government, and the information received from them may be used in the evaluation of the offeror’s past performance.

The offeror shall provide with the proposal a summary of the required past performance information as shown in ***Attachment F - Past Performance Worksheet***.

## Preparation of Price Proposal

The offeror shall submit its Price Proposal in the form of an MS Excel Workbook. The Price Model is used to facilitate the delivery of prices in the required format. A sample MS Excel workbook, “Pricing Template.xls” is included as ***Attachment D – Pricing Template***. In populating all Excel worksheets, the offeror shall present the data (e.g., item number, unit prices, quantities, and summarized prices) in a manner where all computations can be traced to the maximum extent possible. The offeror may add rows, columns, or worksheets to accommodate the required pricing information. See also: ***Attachment C –******Pricing Requirements***.

Failure by the offeror to use the prescribed pricing template may result in non-compliance. The Price Proposal must be submitted under separate cover from the Technical Proposal. While there is no page limit for the Price Proposal, the offeror must provide the necessary detail and supporting information to address the solicitation requirements and to allow a complete analysis of each line item price.

# Evaluation Factors and Basis for Award

The Government will evaluateeach of the offeror’s proposals to determine if the support services offerings satisfy the specific requirements under each task. The evaluations will be based on the evaluation factors defined in this section.

## Evaluation Methodology and Basis for Award

|  |
| --- |
| **SUGGESTED EVALUATION LANGUAGE**  **(Agency may remove or modify the narratives below)**   1. The Government may award a contract based on the initial proposal without discussions or negotiations with offerors, in accordance with **FAR 52.215-1**. Therefore, it is important that each proposal be fully compliant, without exception to any requirement, clause or provision. Offerors should submit initial proposals which respond most favorably to the SOW’s requirements. 2. The Government intends to evaluate offerors’ proposals in accordance with **Section 7.0** of this SOW and make a contract award to the responsible offeror whose proposal is most advantageous to the U.S. Government. 3. The Technical Proposal will be evaluated by a technical evaluation committee using the technical criteria shown below. 4. Price has not been assigned a numerical weight. Offerors are reminded that the Government is not obligated to award a negotiated contract on the basis of lowest proposed price, or to the offeror with the highest technical evaluation score. Agencies must state the following when using tradeoff process: ‘The solicitation shall state whether all evaluation factors other than cost or price, when combined, are significantly more important than, approximately equal to, or significantly less important than cost or price.’ 5. As technical scores converge, price may become a deciding factor in the award. Therefore, after the final evaluation of proposals, the contracting officer will make the award to the offeror whose proposal offers the best value to the Government considering both technical and price factors. |

## Evaluation Approach – Trade Off or LPTA

Note: The Agency is required to select either Trade off or LPTA Approach. Once a method has been selected, delete all information in this SOW relevant to the method that was NOT selected.

|  |
| --- |
| **SUGGESTED EVALUATION LANGUAGE**  **IF TRADE OFF APPROACH**  **IS SELECTED BY THE AGENCY**  **(Agency may remove or modify the narratives below)**  The Government anticipates awarding a task order to the offeror whose quote represents the best value, price and other factors considered.   1. The Government intends to evaluate proposals and may award a contract without discussions. However, the Government reserves the right to conduct discussions if determined by the contracting officer to be necessary. Therefore, each initial offer should contain the offeror’s best proposal from both a price and a technical standpoint. 2. Proposals received in response to this solicitation will be evaluated by the [Agency] in accordance with **FAR 52.215-1**, and as set forth in **Section 7.0: Proposal Instructions**, one award will be made by the contracting officer to the responsible offeror whose proposal, conforming to the solicitation, is determined most advantageous to the Government, all technical and price factors considered. 3. The formula set forth herein will be used by the contracting officer as a guide in determining which proposals will be most advantageous to the Government. |

|  |
| --- |
| **SUGGESTED EVALUATION LANGUAGE**  **IF LOWEST PRICE TECHNICALLY ACCEPTABLE (LPTA) APPROACH**  **IS SELECTED BY THE AGENCY**  **(Agency may remove or modify the narratives below)**  Award will be made to the offeror whose proposal represents the lowest price technically acceptable as defined in **FAR 15, Subpart 15.101-1**. The offeror’s proposal will be evaluated with regard to its ability to meet the tasks set forth in the SOW. To result in an award, the offeror’s proposal must demonstrate the ability to satisfy all technical requirements as set forth in the attached Statement of Work, and must conform to all required terms and conditions.  Lowest price technically-acceptable source selection process.   * + 1. The lowest price technically-acceptable source selection process is appropriate when best value is expected to result from selection of the technically-acceptable proposal with the lowest evaluated price.     2. When using the lowest price technically-acceptable process, the following apply:        1. The evaluation factors and significant sub-factors that establish the requirements of acceptability shall be set forth in the solicitation.        2. Solicitations shall specify that the award will be made on the basis of the lowest-evaluated price of proposals meeting or exceeding the acceptability standards for non-price factors.        3. If the contracting officer documents the file pursuant to 15.304(c)(3)(iii), past performance need not be an evaluation factor in lowest price technically-acceptable source selections.        4. If the contracting officer elects to consider past performance as an evaluation factor, it shall be evaluated in accordance with 15.305. However, the comparative assessment in 15.305(a)(2)(i) does not apply.        5. If the contracting officer determines that the past performance of a small business is not acceptable, the matter shall be referred to the Small Business Administration for a Certificate of Competency determination, in accordance with the procedures contained in subpart and U.S.C. 637(b)(7).     3. Proposals are evaluated for acceptability but not ranked using non-price factors. |

## 

## Technical Evaluation Criteria

The Government will review the responses to this solicitation to ensure that offerors have addressed the requirements for Tasks 1-6 and are sufficient in detail and clarity to allow the Government to determine whether the proposed support services, equipment, and equipment services are acceptable, or if the Government desires to enable the Agency contracting officer to identify items for discussions.

The Government will evaluate the [offerors] contractor’s proposal based upon the following four factors: technical approach, project management, proposed personnel, and past performance*.* Within these factors, the Government will evaluate the [11] sub-factors identified below. To achieve an acceptable rating, the contractor’s Technical Proposal must achieve a pass rating on all [11] sub-factors.

The Agency is required to develop a source selection / technical evaluation plan to describe how each of these factors will be rated. Depending on the approach used, the SSP/TEP may select an adjectival rating system, a points system, or any other approved system.

The Government will evaluate offerors’ Technical Proposals as described below:

|  |
| --- |
| **TECHNICAL EVALUATION CRITERIA** |
| **Factor 1: Technical Approach and Project Management** |
| Sub-factor 1: Task 1 |
| Sub-factor 2: Task 2 |
| Sub-factor 3: Task 3 |
| Sub-factor 4: Task 4 |
| Sub-factor 5: Task 5 |
| Sub-factor 6: Task 6 |
| **Factor 2: Deliverables** |
| Sub-factor 7: Project Management Plan |
| Sub-factor 8: Training Plan |
| **Factor 3: Proposed Personnel** |
| Sub-factor 9: Program/Project Manager Qualifications/Certifications |
| Sub-factor 10: Technical Personnel Qualifications/Certifications |
| **Factor 4: Past Performance** |
| Sub-factor 11: Past Performance History/Track Record |
|  |

|  |
| --- |
| **SUGGESTED EVALUATION LANGUAGE**  **FOR TECHNICAL EVALUATION OF TECHNICAL CRITERIA**  **PLEASE NOTE: The standard for evaluation is usually reserved for the SSP/TEP, however an Agency may choose to disclose this information in the RFQ/RFP**  **(Agency may remove or modify the narratives below)**  The following evaluation criteria will serve as the standard against which all proposals will be evaluated and will serve to identify the significant discussion items that offerors should address in their proposals.  The factors and sub-factors are presented below. Sub-factors are listed in descending order of importance, showing the evaluation weighting for each.   1. **Factor 1: Technical Approach and Project Management**   The extent to which the proposal demonstrates a clear understanding of the statement of work and the degree to which the proposed implementation approach is technically and managerially sound and likely to meet the objectives of the DNSSEC Deployment project as described in this solicitation. The technical approach must be realistic, directly relevant to the achievement of results and must seek to maximize results within budget resources.   * **Sub-Factor 1: Task 1 – DNSSEC and Email Authentication Deployment Planning and System Analysis** - The proposed solution shall effectively address creation of a DNS and Email infrastructure inventory, DNSSEC impact analysis, DNSSEC configuration/architecture, and DNSSEC and Email Authentication deployment strategy. * **Sub-Factor 2: Task 2 – Set Up Test Lab** - The proposed solution shall demonstrate the technical sufficiency of the test environment and the hardware and software equipment required to set up DNSSEC and Email authentication test lab. The offeror shall demonstrate understanding of the test environment requirements that resemble the production environment as closely as possible, including the network hardware and software features targeted for DNSSEC and Email Authentication integration. * **Sub-Factor 3: Task 3 – Convert, Test, and Archive DNSSEC Servers** - The proposed solution shall demonstrate the process and the technical sufficiency required to perform a pilot production deployment for one or more Agency office sites (Agency HQ and Office sites) and moving DNSSEC to production. The contractor shall demonstrate understanding of the requirements to test the DNSSEC integration with the DHS/NIST/Sparta SNIP infrastructure. * **Sub-Factor 4: Task 4 – DNSSEC Deployment/Cutover of Agency Production Zones** - The proposed solution shall demonstrate the offeror’s clear understanding of the Agency's requirements to DNSSEC deployment in the remaining Agency DNS infrastructure to a production environment. The proposal will be evaluated regarding the extent to which it demonstrates understanding of the requirements and the measures to be performed after the infrastructure changes are completed to ensure that the production network is ready for full DNSSEC deployment. * **Sub-Factor 5: Task 5 – Operational Procedures for Administration of DNSSEC** - The proposed solution shall demonstrate the offeror’s clear understanding of the Agency's requirements to develop Operational Procedures for Administration of DNSSEC in operational environment. The proposal will be evaluated regarding the extent to which it demonstrates understanding of the requirements and the administration procedures to be performed after the DNS infrastructure changes are completed to ensure that the production network is ready for full DNSSEC operation. * **Sub-Factor 6: Task 6 – Authentication of Agency Email System with DKIM and SPF** - The proposed solution shall demonstrate the offeror’s clear understanding of the Agency's requirements to deployment of the Authentication of Agency Email System with DKIM and SPF. The proposal will be evaluated regarding the extent to which it demonstrates understanding of the requirements and the measures to be performed after the Email infrastructure changes are completed to ensure that the production Email is ready for full DKIM and/or SPF deployment.  1. **Deliverables**  * **Sub-Factor 7: Program Management** - The proposed solution shall describe the extent to which it uses a creative and innovative program management approach, and clearly demonstrate how the proposed technical solution for each task will achieve expected results. The offeror’s Program Management Plan will be evaluated against these criteria. * **Sub-Factor 8: Training Plan and Delivery Methods** - The proposed solution shall demonstrate the quality of support and responsiveness of the proposed training plan and training delivery methods.  1. **Qualifications of Proposed Personnel**  * **Sub-Factor 9: Qualifications and Demonstrated Ability of the Project Manager/Program Manager** – The proposed Project Manager/Program Manager shall demonstrate the qualifications and ability to successfully lead this project, including the ability to work constructively at multiple levels of organizations, including senior levels of Government and business. * **Sub-Factor 10: Qualifications and Demonstrated Ability of the Proposed Technical Staff and Key Personnel** – The members of the proposed project team, including subject-matter experts (SMEs), shall demonstrate the experience and ability to successfully meet the project milestones, targets, and goals.  1. **Past Performance**  * **Sub-Factor 11: Past Performance** information will be used for both the responsibility determination and best value decision. The offeror and major subcontractor(s) past performance will be evaluated. A major subcontractor (if applicable) is defined as a subcontractor named in the proposal whose total price exceeds 15% of the offer’s bottom line total price, including fixed fee. The contracting officer will utilize existing database of contractor performance information (i.e. PPIRS) and solicit additional information from the references provided in this SOW and from other sources if and when the contracting officer finds the existing databases to be insufficient for evaluating an offeror’s performance. The [Agency] may use performance information obtained from other than the sources identified by the offeror/subcontractor. |

## Price Evaluation Criteria

|  |
| --- |
| **SUGGESTED EVALUATION LANGUAGE**  **FOR PRICE EVALUATION CRITERIA**  **(Agency may remove or modify the narratives below)**   1. No points are assigned to the price proposal evaluation. While the technical evaluation criteria are significantly more important than price, price remains important. 2. Price will primarily be evaluated for realism, allow-ability, and reasonableness. 3. This evaluation will consist of a review of the price portion of an offeror’s proposal to determine if the overall price proposed is realistic for the work to be performed, if the price reflects an accurate understanding of the requirements, and if the price is consistent with the Technical Proposal. 4. Evaluation of the price proposal will consider but not be limited to the following:  * Price reasonableness, price realism and completeness of the price proposal and supporting documentation * Overall price control/price savings evidenced in the proposal (avoidance of prices that exceed reasonable requirements) * The amount of the proposed fee, if any  1. Price realism is an assessment of the accuracy with which proposed prices represent the most probable cost of performance, within each Offeror’s technical and management approach. A price realism evaluation shall be performed as part of the evaluation process as follows:  * Verify the offeror’s understanding of the requirements * Assess the degree to which the price proposal accurately reflects the technical approach * Assess the degree to which the prices included in the Price Proposals accurately represent the work effort included in the respective Technical Proposals  1. The results of the price realism analysis will be used as part of the Agency’s best value/tradeoff analysis. 2. Although technical evaluation criteria are significantly more important than price, the closer the technical evaluation scores of the various proposals are to one another, the more important price considerations will become. The evaluation of proposed prices may therefore become a determining factor in the award as technical scores converge. |

# Task Order Award

The Task Order Award will be made to the responsible Offeror whose proposal is in the best interest of the [Agency], given the outcome of the [Agency]’s evaluation of each Offeror’s technical excellence, management and business risk factors, and proposed price. In selecting the Task Order Award, the [Agency] will consider the quality offered for the evaluated price. The relative quality of offers will be based upon the [Agency]’s assessment of the tradeoffs between the technical excellence offered in the Offeror’s proposal and whether it provides added value, added capability, and/or reduced management and business risk.

# Organizational Conflicts of Interest

In accordance with Section H.8 of the Connections II contract, the guidelines and procedures of **FAR Subpart 9.5** will be used in identifying and resolving any issues of organizational conflicts of interest at the task order level.

In the event that a task order requires activity that would create or has created an actual or potential conflict of interest, the offeror shall:

* + - * Notify the task order contracting officer (CO) of the actual or potential conflict, and not commence or continue work on any task order that involves a potential or actual conflict of interest until specifically notified by the task order CO to proceed.
      * Identify the conflict and recommend to the task order CO an alternate tasking approach which would avoid the conflict.

If the task order CO determines that it is in the best interest of the Government to issue or continue the task order, notwithstanding a conflict of interest, a request for waiver shall be submitted in accordance with **FAR 9.503**.  In the event that the offeror was aware of facts required to be disclosed or the existence of an actual or potential organizational conflict of interest and did not disclose, when known, such facts or such conflict of interest to the task order CO, the Government may terminate this contract for default.

In the event that a task order issued under this contract requires the offeror to gain access to proprietary information of other companies, the offeror shall be required to execute agreements with those companies to protect the information from unauthorized use and to refrain from using it for any purpose other than for which it was furnished.

# Nondisclosure Agreement

The Contractor shall comply with the requirements given at Section H.9 of the Connections II contract (Disclosure of Information).

Individual staff members performing work under this task order shall be required to execute [the Agency’s] nondisclosure agreement. One copy of each signed agreement shall be forwarded to [the Agency’s] designated representative prior to work commencing.

# Attachments

|  |
| --- |
| Double-clicking the attachments may produce the error "Word cannot start the converter mswrd632.wpc," which is a known Microsoft issue (http://support.microsoft.com/kb/973904). Microsoft provides the following workaround: right-click on the embedded attachment (instead of double-clicking) and then select "Document Object" and then use "Open" (instead of "Convert") from the pop-up menu. |

## Attachment A – Program Management Plan



## Attachment B – Support Locations



## Attachment C – Pricing Requirements



## Attachment D – Pricing Template



## Attachment E – Equipment, Support and Warranty Inventory



## Attachment F – Past Performance Worksheet



## Attachment G – Task Order Deliverables



## Attachment H – Sample Existing DNS Security Architecture and Figures



## Attachment I – DNS Security (DNSSEC) Reference Architecture



## Attachment J – NIST Specified DNSSEC Implementation Checklists

