



State of Oklahoma
Office of Management and Enterprise Services

**ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH TRUE DIGITAL SECURITY, INC.
RESULTING FROM STATEWIDE CONTRACT NO. 1042**

This Addendum 1 (“Addendum”) is an Amendment to the Contract awarded to True Digital Security, Inc. in connection with Statewide Contract No. 1042 (“Solicitation”) and is effective August 23, 2017.

Recitals

Whereas, the State issued a Solicitation for proposals to provide information technology risk, security and compliance products and services to state agencies and to ensure compliance with all industry and regulatory data security standards, as more particularly described in the Solicitation;

Whereas, True Digital Security, Inc. submitted a proposal which contained various other Contract Documents; and

Whereas, the State and True Digital Security, Inc. have negotiated the final terms under which True Digital Security, Inc. will perform the Services under the Contract.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. **Addendum Purpose.**

This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to True Digital Security, Inc. as of even date with execution of this Addendum. The parties agree that Supplier has not yet begun performance of work contemplated by the Solicitation.

2. **Negotiated Documents of the Contract.**

2.1. The parties have negotiated certain terms of the Contract as follows:

- i. revisions to True Digital Security, Inc's Pricing Proposal as contained in Attachment A to this Addendum titled, certain negotiations additional terms to the Solicitation as contained in Attachment A to this Addendum titled Negotiated Additional Terms;
- ii. revisions to True Digital Security, Inc.'s bidder agreement as contained in Attachment B to this Addendum titled, Bidder Agreement; and
- iii. revisions to True Digital Security, Inc.'s Sample Statement of Work Template as contained in Attachment C to this Addendum titled Sample Statement of Work Template; and
- iv. revisions to True Digital Security, Inc.'s Letter of Understanding as contained in Attachment D to this Addendum titled Letter of Understanding.

2.2. Accordingly, any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

State of Oklahoma

By: _____

Name: James L. Reese, II

Title: Chief Information Officer

Date: _____

9-6-17

True Digital Security, Inc.

By: _____

Name: _____

Title: _____

Date: _____

PRESIDENT & CFO

AUGUST 23, 2017



Attachment A to
Addendum 1 to
State of Oklahoma Contract with True Digital Security, Inc.
Resulting from Statewide Contract No. 1042

This Pricing Proposal is hereby amended as set forth below and supersedes all prior Documents submitted by True Digital Security, Inc. or discussed by the parties.

TRUE DIGITAL SECURITY PRICING

IT Risk, Security and Compliance Products and Services Bid Response to Solicitation #0900000255

Prepared for: The Office of Management and Enterprise Services
Central Purchasing (CP) and Information Services
Response Due Date: March 22, 2017; Time: 3:00 PM CST

Kayna Kelley, Business Development
918-770-7700 x110 business
918-633-0414 cell
kayna.kelley@truedigitalsecurity.com

True Digital Security, Inc.

P.O. Box 35623

Tulsa, OK 74153

p. 866.430.2595

f. 877.720.4030

truedigitalsecurity.com

TRUE will use the following fixed firm and hourly, not to exceed (NTE) pricing for agencies requiring security services from information security experts. When hourly NTE pricing is supplied, TRUE will collect necessary scoping details to calculate fixed firm engagement costs, inclusive of tool costs and/or materials, when applicable. Supplying pricing within an Hourly NTE format provides TRUE the greatest flexibility to provide the most competitive pricing for agencies based on the actual scope of each project, while also accounting for nonstandard testing requests.

| Product Line/Product/Service | Verifiable List Price | % Off List Price | Cost (NTE) |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------|-------------|
| EVALUATION OF NETWORK SECURITY | | | |
| Security Architecture Review/Threat Model – Custom Quote Required | \$225/hour | ~6.67% | \$210/hour |
| System Hardening Configuration Review – Custom Quote Required | \$225/hour | ~6.67% | \$210/hour |
| Firewall Configuration Review – Custom Quote Required | \$225/hour | ~6.67% | \$210/hour |
| VULNERABILITY TESTING | | | |
| Network Vulnerability Assessment – Up to 25 IPs <ul style="list-style-type: none"> Performed remotely | \$5,475 | ~6.58% | \$5,115 |
| Network Vulnerability Assessment – Up to 50 IPs <ul style="list-style-type: none"> Performed remotely | \$7,350 | ~6.53% | \$6,870 |
| Network Vulnerability Assessment – Up to 75 IPs <ul style="list-style-type: none"> Performed remotely | \$8,325 | ~6.49% | \$7,785 |
| Network Vulnerability Assessment – Up to 100 IPs <ul style="list-style-type: none"> Performed remotely | \$9,300 | ~6.45% | \$8,700 |
| Network Vulnerability Assessment – Greater than 100 IPs or with Technical Controls Review – Custom Quote Required <ul style="list-style-type: none"> Performed remotely | \$225/hour | ~6.67% | \$210/hour |
| Quarterly External Network Vulnerability Scanning – Up to 200 IPs <ul style="list-style-type: none"> *Tool costs additional at \$10 per IP One (1) year term Reporting consists of technical scan results Performed remotely | \$2,150* | ~4.65% | \$2,050* |
| All Other External Network Vulnerability Scanning (One-Time, Monthly or Quarterly) – Custom Quote Required <ul style="list-style-type: none"> *Tool costs additional Reporting can consist of technical scan results or analyst summary along with technical scan results | \$215/hour | ~4.65% | \$205/hour* |
| Quarterly Internal Network Vulnerability Scanning – Up to 200 IPs <ul style="list-style-type: none"> Includes scanning from a single location | \$5,365 | ~2.05% | \$5,255 |

| | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|-------------|
| <ul style="list-style-type: none"> • Tool costs included • One (1) year term • Reporting consists of technical scan results • Performed remotely | | | |
| All Other Internal Network Vulnerability Scanning (One-Time, Monthly, or Quarterly) – Custom Quote Required <ul style="list-style-type: none"> • *Tool costs additional; will vary based on frequency • Reporting can consist of technical scan results or analyst summary with technical scan results | \$215/hour* | ~4.65% | \$205/hour* |
| PCI Quarterly External ASV Scanning – Up to 10 IPs <ul style="list-style-type: none"> • One (1) year term • Performed remotely | \$2,200 | ~4.55% | \$2,100 |
| PCI Quarterly External ASV Scanning – Up to 20 IPs <ul style="list-style-type: none"> • One (1) year term • Performed remotely | \$3,180 | ~4.40% | \$3,040 |
| PCI Quarterly External ASV Scanning – Up to 30 IPs <ul style="list-style-type: none"> • One (1) year term • Performed remotely | \$3,695 | ~4.33% | \$3,535 |
| PCI Quarterly External ASV Scanning – Greater than 30 IPs – Custom Quote Required <ul style="list-style-type: none"> • *Tool costs additional • One (1) year term • Performed remotely | \$215/hour* | ~4.65% | \$205/hour* |
| Application Security Assessment/Source Code Review – Custom Quote Required <ul style="list-style-type: none"> • *Tool costs additional, if applicable • Performed remotely | \$225/hour* | ~6.67% | \$210/hour* |
| PENETRATION TESTING | | | |
| Network Penetration Testing – Up to 5 IPs <ul style="list-style-type: none"> • Performed remotely | \$1,850 | ~6.49% | \$1,730 |
| Network Penetration Testing – Up to 15 IPs <ul style="list-style-type: none"> • Performed remotely | \$4,150 | ~6.51% | \$3,880 |
| Network Penetration Testing – Up to 30 IPs <ul style="list-style-type: none"> • Performed remotely | \$7,350 | ~6.53% | \$6,870 |
| Network Penetration Testing – Up to 50 IPs <ul style="list-style-type: none"> • Performed remotely | \$11,450 | ~6.55% | \$10,700 |
| Network Penetration Testing – Up to 75 IPs <ul style="list-style-type: none"> • Performed remotely | \$13,300 | ~6.54% | \$12,430 |
| Network Penetration Testing – Up to 100 IPs <ul style="list-style-type: none"> • Performed remotely | \$15,150 | ~6.53% | \$14,160 |

| | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|-------------|
| Network Penetration Testing – Greater than 100 IPs – <i>Custom Quote Required</i> <ul style="list-style-type: none"> *Tool costs additional | \$225/hour* | ~6.67% | \$210/hour* |
| Application Penetration Test – Small Application <ul style="list-style-type: none"> Small: Classified as a standard website with limited to no dynamic functionality. Typically, a CMS driven corporate or marketing site. Performed remotely | \$3,700 | ~6.49% | \$3,460 |
| Application Penetration Test – Medium Application <ul style="list-style-type: none"> Medium: Classified as a web application consisting of a single role or login developed using standard web technologies with up to five (5) functional areas. Performed remotely | \$9,100 | ~6.59% | \$8,500 |
| Application Penetration Test – Large Application <ul style="list-style-type: none"> Large: Classified as a web application encompassing multiple roles and logins with up to ten (10) functional areas and testing of up to three (3) roles. Performed remotely | \$14,500 | ~6.62% | \$13,540 |
| Application Penetration Test – Other – <i>Custom Quote Required</i> <ul style="list-style-type: none"> *Tool costs additional Performed remotely | \$225/hour* | ~6.67% | \$210/hour* |
| Wireless Security Assessment of a Single Wireless Network | \$2,700 | ~6.67% | \$2,520 |
| Wireless Security Assessment Including Optional Wireless Configuration Review, Wireless Physical Control Review, and/or Multiple Wireless Networks – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| Email Phishing Social Engineering Assessment <ul style="list-style-type: none"> Includes up to one hundred (100) users Performed remotely | \$5,050 | ~6.53% | \$4,720 |
| Phone/Physical Social Engineering Assessment – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| TECHNICAL TRAINING SERVICES | | | |
| Application Security Training for Software Developers – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| General and PCI Security Awareness Training – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| OTHER SERVICES | | | |
| Information Security Risk Assessment, Gap Analysis – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |

| | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------|------------|
| HIPAA Compliance Services – HIPAA Risk Analysis, HIPAA Gap Assessment – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| PCI Compliance Services – PCI Gap Assessment, PCI SAQ Assessment, PCI On-site Assessment/Audit, PCI Risk Assessment, PCI QSA-for-a-Day Guidance, (For PCI Pen Testing see Penetration Testing; For PCI ASV Scanning see Vulnerability Assessment sections) – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| Security Policy Gap Analysis & Development – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |
| Hourly Incident Response & Forensics | \$300/hour | ~16.67% | \$250/hour |
| SOC Audit Preparation – <i>Custom Quote Required</i> | \$225/hour | ~6.67% | \$210/hour |

**Attachment B to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH TRUE DIGITAL SECURITY, INC.
RESULTING FROM STATEWIDE CONTRACT NO. 1042**

The Bidder Agreement is hereby amended as set forth below and supersedes all prior documents submitted by True Digital Security, Inc. or discussed by the parties.

Bidder Agreement

1. MUTUAL CONFIDENTIALITY AND PROTECTION OF PROPRIETARY INFORMATION AND TRADE SECRETS

- a. True Digital Security, Inc. ("TRUE") acknowledges that by providing its services to the State of Oklahoma ("Customer") under this Bidder Agreement ("Agreement"), TRUE will have access to information of a private nature and may include, but is not limited to, Customer's trade secrets, proprietary and confidential business information. Additionally the services provided by TRUE may reveal weaknesses in Customer's network and data systems that could be exploited by unauthorized third parties, including (i) information relating to the Customer's Network Configuration, (ii) information regarding Customer's network or physical security, (iii) information regarding Customer's network traffic, (iv) and data created, stored, or transmitted by Customer's internal network. Therefore TRUE:
 1. will limit access to Customer's sensitive or proprietary information to those employees or agents of TRUE who, at TRUE's sole discretion, are necessary to the performance of the services contracted by Customer;
 2. will ensure that any service(s) performed by TRUE's employees will be performed pursuant to non-disclosure agreements maintained by TRUE;
 3. will maintain all analysis, results, or reported vulnerabilities revealed or compiled by TRUE, as confidential and will release that information only to those individuals designated by the Customer.
- b. Customer similarly acknowledges that TRUE has developed and acquired sensitive trade secrets including, but not limited to, tools, processes, software, hardware, and methodologies ("proprietary tools"). These proprietary tools are unique to TRUE and are not known, or enjoyed, by TRUE's competitors. Customer therefore agrees for any proprietary tools identified by TRUE as a proprietary tool:
 1. to promptly return to TRUE any proprietary tool in Customer's possession upon request by TRUE; without regard to any claim, demand, or pending action Customer may have against TRUE or its agents;
 2. not to reveal, copy, decompile, de-engineer, sell, transfer, or in any way compromise the security of any proprietary tool employed by TRUE;
 3. not to assert any claim of ownership, directly or indirectly, to TRUE's proprietary tools;
 4. any proprietary tools specially created or enhanced by TRUE, as a result of, or in order to perform under this Agreement are the exclusive property of TRUE or its agents.
- c. If TRUE receives any demands or requests for information or data under the Oklahoma Open Records Act, or any similar state, federal, or foreign law, TRUE will not disclose the requested information or data. TRUE will, instead, immediately forward the request or demand to the Customer. TRUE acknowledges that the Customer is considered a governmental entity, and as such is subject to statutes and other laws governing public information. TRUE agrees to hold Customer harmless from the terms of this Agreement in the event that withholding the information would violate public information laws.
- d. With regard to PCI (Payment Card Industry) Security Standards Council (SSC): QSA may disclose such information as necessary to comply with its obligations and requirements
 1. Customer acknowledges that TRUE may be required to disclose Record of Compliance (ROC), Attestation of Compliance and other related information to PCI SSC and/or PCI SSC Member.
 2. To the extent any PCI SSC Member obtains such information in accordance with the preceding clause d.1, such Member may disclose
 - a. such information on an as needed basis to other PCI SSC Members and to such PCI SSC Members' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and
 - b. that such PCI SSC Member has received a ROC and other related information with respect to Customer and whether the ROC was satisfactory
- e. Accordingly, notwithstanding anything to the contrary in Section 1, TRUE may disclose Confidential Information relating to

such Customer and obtained by TRUE in connection with this Agreement to PCI SSC in accordance with this Section 1, and PCI SSC may in turn disclose such information to their respective Financial Institutions and PCI SSC Members. Customer hereby consents to such disclosure by TRUE, PCI SSC and PCI SSC Members.

- f. In the event TRUE is required by the PCI SSC to disclose Customer's information, TRUE has no obligation to resist requests to produce and disclose information about such matters and Customer shall not seek to hold TRUE liable for such compliance.

2. LIMITATION OF LIABILITY

TRUE's liability to Customer for any damages arising from the performance of this Agreement shall be limited to the sum-total cost of all services contracted for under the affected Invoice Schedule and accompanying Statement of Work, provided that:

- a. Neither party shall be liable to the other for incidental, indirect, special, or consequential costs or damages including, but not limited to, downtime costs; lost business, revenues, or profits; failure to realize expected savings; loss of data; damage to systems, machines, or networks; or software restoration;
- b. Unless caused by TRUE's gross negligence, TRUE shall not be liable for any damages arising directly or indirectly from failures caused by improperly installed or configured network devices, systems, or failures caused by hardware, software, or firmware that has not been updated to all publicly released patches, drivers, and updates.
- c. Any limitation of liability submitted by TRUE does not apply to the extent a court of competent jurisdiction (including any appellate court of final review) determines such limitation of liability violates Oklahoma law, in which case the specific limitation that the court determines is in violation of Oklahoma law shall be void.
- d. For the avoidance of doubt, this limitation of liability set forth in this Section 3 shall not apply to (a) any claims or actions arising from or related to TRUE's breach of confidentiality or (b) infringement of third party intellectual rights by TRUE. Any damages associated with such a claim will be limited to five (5) times the Sum Total included in the specific Invoice Schedule of the applicable Statement of Work.

3. PAYMENT TERMS AND CONDITIONS

Except as otherwise set forth in Oklahoma Statewide Contract 1042 with TRUE, in exchange for the services provided by TRUE, Customer shall be obligated to pay the Sum Total of all services set forth in a Statement of Work. This Agreement is non-divisible unless agreed to in writing by both parties in advance. TRUE shall be obligated to perform in accordance with the Statement of Work, executed by both parties, and except as otherwise provided in the contract resulting from Statewide Contract No. 1042 with TRUE, Customer shall become obligated for the entire sum total upon Customer's receipt of a proper invoice. Customer agrees to pay the invoice in accordance with applicable Oklahoma law. Following execution of a Statement of Work, any changes to scope of work or sum total payment(s) due must be clearly defined and agreed to in writing in advance by both Parties via Change Order (CO).

4. WARRANTY

Customer acknowledges that while TRUE uses technology, constantly evolving strategies, and qualified professionals to counter a growing and constantly changing worldwide threat, TRUE makes no guarantee that its services and/or products will completely eliminate the risks or vulnerabilities of Customer's network, data systems, or information. In providing services under this Agreement, TRUE will endeavor to perform in a manner consistent with that degree of care and skill exercised by members of the same profession currently providing similar services under similar conditions and circumstances. Customer acknowledges that TRUE makes NO WARRANTIES OR GUARANTEES that its products, services, or recommendations will prevent all unauthorized access, compromise of data or systems, or malicious attacks, including, but not limited to, viruses, worms, Trojans, Denial-of-Service attacks, defacements, or eavesdropping.

5. CANCELLATION

Except as otherwise set forth in SW1042 Contract Customer will provide TRUE with not less than five (5) day notice in the event that Customer needs to cancel or reschedule onsite meetings.

6. OTHER APPLICABLE TERMS

- a. No term or provision of this Agreement may be amended, waived, released, discharged or modified in any respect except by in writings signed by both parties.

7. SURVIVAL

Notwithstanding the termination of this Agreement, it is acknowledged and agreed that the following rights and obligations shall survive such expiration or earlier termination: Sections 1, 2, 3, 5 and 6

**Attachment C to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH TRUE DIGITAL SECURITY, INC.
RESULTING FROM STATEWIDE CONTRACT NO. 1042**

The Sample Statement of Work Template is hereby amended as set forth below and supersedes all prior documents submitted by True Digital Security, Inc. or discussed by the parties. The parties agree to use this Sample Statement of Work Template or a document substantially in the form of this Sample Statement of Work Template.

Sample Statement of Work Template

Prepared for: <Agency Name>
Submitted: <Date>

Kayna Kelley, Business Development
True Digital Security, Inc.
1350 S. Boulder Ave., Suite 1100
Tulsa, OK 74119
918-770-7700 x110 business
918-633-0414 cell
kayna.kelley@truedigitalsecurity.com

NETWORK SECURITY SERVICES ADDENDUM (NSSA)

This Statement of Work is entered in between True Digital Security, Inc. and <Agency Name> and hereby fully incorporates the Oklahoma Statewide Contract SW1042 with True Digital Security, Inc., including any addendums or amendments.

True Digital Security, Inc.

P.O. Box 35623

Tulsa, OK 74153

p. 866.430.2595

f. 877.720.4030

truedigitalsecurity.com

Contents

| | |
|--------------------------------------------------------------|---|
| 1. Introduction | 3 |
| 2. Project Overview & Scope | 3 |
| <Service Name>..... | 3 |
| Scope & Assumptions | 3 |
| Methodology..... | 3 |
| Benefits | 3 |
| 3. Project Deliverables | 3 |
| 4. Customer Responsibilities..... | 3 |
| 5. Dedicated Team of Certified Security Experts | 4 |
| 6. Company Background | 4 |
| 7. Proposed Pricing | 5 |
| 8. Invoice Schedule | 6 |
| 9. Signatures | 6 |
| Appendix A: Security Testing Risk Disclosure Statement | 8 |

1. Introduction

True Digital Security, Inc. (TRUE) is pleased to submit this <Service Name> proposed Statement of Work to <Agency Name>. This document contains a comprehensive view of TRUE's winning qualifications, project methodology, technical approach, deliverables and pricing, outlining all the information you need to make a well-informed decision.

2. Project Overview & Scope

The following section provides an overview of TRUE's <Service Name> offering with the scope and assumptions, followed by the methodology and benefits for the proposed engagement.

<Service Name>

<Service Description>

Scope & Assumptions

<Service Name>

Scope:

- Service to be performed: <Service Name>
- <Applicable scoping details>

Assumptions:

- <Applicable assumptions>

Methodology

<Service Methodology>

Benefits

<Service Benefits>

3. Project Deliverables

<Service Deliverables>

4. Customer Responsibilities

<Agency Name> will assign a project owner for TRUE who will serve as our primary point of contact and be responsible for acquiring any information required on behalf of TRUE. Your point person will manage <Agency Name> resources for this engagement, which may include scheduling testing activities, on-site activities and information requests with the appropriate <Agency Name> parties.

<Service Customer Responsibilities>

In most cases, TRUE cannot begin project execution until all required information is received from <Agency Name>. Therefore, the requested information should be provided as soon as possible following contract signature to avoid delays.

5. Dedicated Team of Certified Security Experts

Companies hire TRUE certified security experts to work alongside them in order to reach their security goals. In contrast to your standard vendor, TRUE works very hard to be an integral part of your team, helping you make informed decisions while enabling your business to operate more securely. When you select TRUE as your information assurance provider, you can be confident our staff and firm have the security credentials and know-how to deliver.

Key highlights of our accolades include:

- Expert consulting and services staff, including analysts, consultants, project managers, and management with:
 - CISSP (Certified Information Systems Security Professional) credentials
 - United States Department of Defense CNSS (Committee on National Security Systems) credentials
 - United States Department of Defense Cyber Corps program credentials
 - Service in information assurance within United States Department of Defense agencies
 - Advanced degrees, Masters or Ph.D., in Computer Science with emphasis in information assurance
- Payment Card Industry (PCI) certified Qualified Security Assessor (QSA)
- Payment Card Industry (PCI) certified Approved Scanning Vendor (ASV)

Bios for the certified security professionals TRUE proposes to assign to your project are available upon request as well as a list of references.

6. Company Background

True Digital Security is a premier information security services firm committed to delivering best-in-class, real-world security and compliance solutions. Established in 2004 in Tulsa, OK as an information security research and development shop, TRUE quickly expanded its focus to meet the increasing demand for information assurance services provided by accredited security experts. As an information security services and managed solutions company, TRUE has formulated procedures for identifying the weaknesses that exist in an organization's security posture. After exposing these deficiencies, we then supply the processes, supporting technologies, and expert guidance to enable our customers to make necessary adjustments and better manage controls going forward. Operating as an extension of our customers' in-house IT/infrastructure team, we provide highly specialized strategy and expert consultation that enables companies to remain focused on moving their business forward, with TRUE peace of mind that their security and related risk assessment needs are adequately addressed.

TRUE provides several consulting and testing services offered under State Contract No. 1042 to assist State agencies with IT Risk, Security and Compliance initiatives including the following categories:

Evaluation of Network Security

- Security Architecture Review/Threat Model
- System Hardening Configuration Review
- Firewall Configuration Review

Vulnerability Testing

- Network Vulnerability Assessment

- Quarterly External Network Vulnerability Assessment
- One-Time/Monthly/Quarterly External/Internal Network Vulnerability Scanning
- Quarterly PCI External ASV Scanning
- Application Security Assessment/Source Code Review

Penetration Testing

- Network Penetration Testing
- Application Penetration Testing
- Wireless Security Assessment
- Email Phishing Social Engineering Assessment
- Phone/Physical Social Engineering Assessment

Technical Training Services

- Application Security Training for Software Developers
- General and PCI Security Awareness Training

Other Services

- Information Security Risk Assessment, Gap Analysis
- HIPAA Compliance Services (HIPAA Risk Analysis, HIPAA Gap Assessment)
- Other PCI Compliance Services (PCI Gap Assessment, PCI SAQ Assessment, PCI On-site Assessment/Audit, PCI Risk Assessment, PCI QSA-for-a Day Guidance)
- Security Policy Gap Analysis & Development
- Hourly Incident Response & Forensics
- SOC Audit Preparation

Beyond having the right solution set that your organization needs to mitigate risk, TRUE has the skills and experience to tailor our solutions to meet agency demands. Our expanding industry portfolio includes State Agencies, Government, Energy, Financial, Healthcare, Academic, Legal, Technology and E-commerce customers. As any of our customers will testify, TRUE can execute the highest quality security services at an affordable cost for organizations of all sizes. Furthermore, TRUE takes a personal approach to every project and regards each customer relationship as a partnership.

7. Proposed Pricing

The scoping details provided by <Agency Name> and included within the Scope & Assumptions section of this Statement of Work were used to determine the following engagement pricing.

| Services Delivered | Total |
|---------------------------------|----------|
| <Service Name> | |
| Documentation & Reporting | Included |
| TOTAL PROJECT INVESTMENT | |

Note:

While TRUE will attempt to uncover as many threats as possible, it is impossible to guarantee the disclosure of all threats.

8. Invoice Schedule

| Service | Payment Due |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fixed Firm Services | Invoiced Net45 upon contract signature, with payment due the later of 45 days from receipt of invoice or upon submission of final deliverable. Contractor shall be paid upon submission of proper invoice(s) to the agency at the prices stipulated on the contract. Invoices shall contain the purchase order number. Failure to provide proper invoices may result in delay of processing invoices for payment. Pursuant to 74 O.S. §85.44(B), invoices will be paid in arrears after products have been delivered or services provided. Interest on late payments made by the State of Oklahoma is governed by 62 O.S. §34.71 and 62 O.S. §34.72. |
| Subscription Services | Invoiced Net45 upon project commencement |
| Hourly Services | Invoiced Net45 monthly as incurred |

9. Signatures

The parties hereby agree to the terms of this Statement of Work, including all terms outlined in the Oklahoma Statewide Contract No. 1042 with TRUE, including any addendums or amendments. The effective date of this Statement of Work is the date <Agency Name> executes below:

<Agency Name>

Signature: _____

Date: _____

Name: _____

Title: _____

Billing Contact

(Note: Failure to include Billing Contact Information may delay project commencement.)

Name: _____ Address: _____

Email: _____ Address: _____

Phone: _____ City, State, Zip: _____

True Digital Security, Inc.

Signature: _____

Date: _____

Name: Jeff Harris

Title: President & CFO

SAMPLE

Appendix A: Security Testing Risk Disclosure Statement

TRUE has created this disclosure statement to inform its clients of the risks involved in conducting security testing procedures and ensure all parties understand and acknowledge their roles in reducing this risk.

Acknowledgement of Risk

TRUE's staff works diligently to avoid the risks of security testing; however, this risk can never be fully eliminated. The purpose of this Appendix is to inform all resources and parties associated with this engagement within <Agency Name> that these risks exist in the performance of the testing associated with this engagement. Such risks may include data destruction/modification, system crashes, or network interruptions, among other issues. <Agency Name> acknowledges these risks, and agrees that they are responsible for mitigating any risks they deem necessary prior to approving TRUE's testing windows.

Steps TRUE Takes to Minimize Risk

TRUE takes the following steps to minimize risk:

- TRUE does not use brute forcing or explicit denial of service testing.
- TRUE employs prompt communication strategies. Planning and coordination between <Agency Name> and TRUE will play a significant role in reducing the risk of impact to <Agency Name> information systems.
- Per client requirements, TRUE is available to perform testing during non-business hours.
- "Dangerous" tests (e.g., penetration testing) are to be performed only with client approval.

Steps <Agency Name> Should Take to Minimize Risk

TRUE recommends <Agency Name> take the following steps to minimize the risk associated with security testing:

- <Agency Name> should communicate testing procedures to all impacted internal and third parties, subject to the guidelines of the engagement.
- <Agency Name> should maintain current backups of all data and systems.
- <Agency Name> should closely monitor availability and performance during testing.
- <Agency Name> should have an incident response plan in place and be immediately accessible by a phone that does not rely on <Agency Name>'s network infrastructure.

**Attachment D to
 Addendum 1 to
 STATE OF OKLAHOMA CONTRACT WITH TRUE DIGITAL SECURITY, INC.
 RESULTING FROM STATEWIDE CONTRACT NO. 1042**

The Letter of Understanding is hereby amended as set forth below and supersedes all prior documents submitted by True Digital Security, Inc. or discussed by the parties. The parties agree to use this Letter of Understanding or a document substantially in the form of this Letter of Understanding.

<Date>

<Name>

<Title>

<Address Line 1>

<Address Line 2>

<City, State Zip>

RE: LETTER OF UNDERSTANDING CONCERNING <SERVICES> PROVIDED BY TRUE DIGITAL SECURITY TO <AGENCY NAME> THROUGH STATEWIDE CONTRACT NO. 1042 WITH TRUE

Dear <Name>:

This Letter of Understanding (“LoU”) is made and entered into on _____, 2017 by and between True Digital Security, Inc. (TRUE), of Tulsa, OK, and <Agency Name> of <City>, OK.

This LoU fully incorporates the Oklahoma Statewide Contract No. 1042 with TRUE, including any addendums or amendments.

Description: TRUE will perform ...

Assumptions:

- ...

Rate: TRUE will perform <Services> for <Agency Name>, as described above, billed at <Price>, totaling <Total Price>.

| Services Delivered | Total |
|---------------------------------|----------|
| <Service Name> | |
| Documentation and Reporting | Included |
| TOTAL PROJECT INVESTMENT | |

True Digital Security, Inc.

P.O. Box 35623

Tulsa, OK 74153

p. 866.430.2595

f. 877.720.4030

truedigitalsecurity.com

**Invoice
 Schedule:**

| Service | Payment Due |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fixed Firm Services | Invoiced Net45 upon contract signature, with payment due the later of 45 days from receipt of invoice or upon submission of final deliverable. Contractor shall be paid upon submission of proper invoice(s) to the agency at the prices stipulated on the contract. Invoices shall contain the purchase order number. Failure to provide proper invoices may result in delay of processing invoices for payment. Pursuant to 74 O.S. §85.44(B), invoices will be paid in arrears after products have been delivered or services provided. Interest on late payments made by the State of Oklahoma is governed by 62 O.S. §34.71 and 62 O.S. §34.72. |
| Subscription Services | Invoiced Net45 upon project commencement |
| Hourly Services | Invoiced Net45 monthly as incurred |

Note: While TRUE will attempt to uncover as many threats as possible, it is impossible to guarantee the disclosure of all threats.

Please sign, date and submit this letter of understanding to True Digital Security within thirty (30) days of the stated LoU date so that the described services herein may commence as agreed upon.

Thank you for your time and consideration.

Sincerely,

Kayna Kelley, Business Development
 918-770-7700 x110 business
 918-633-0414 cell
 877-720-4030 fax
 kayna.kelley@truedigitalsecurity.com

The parties hereby agree to the terms of this LoU, including all terms of Oklahoma Statewide Contract No. 1042, including any addendums or amendments. The effective date of this LoU is the date <Agency Name> executes below:

<Agency Name>

Signature: _____ Date: _____

Name: _____

Title: _____

Billing Contact

(Note: Failure to include Billing Contact Information may delay project commencement.)

Name: _____ Address: _____

Email: _____ Address: _____

Phone: _____ City, State, Zip: _____

True Digital Security, Inc.

Signature: _____ Date: _____

Name: Jeff Harris

Title: President & CFO