



Statement of Work (SOW)
for
U.S. Customs and Border Protection
Office of Information and Technology (OIT)
Wickr Software Licenses

August 30, 2023

PR# 2013-5100

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

Contents

1.0 Background 3

2.0 Scope..... 3

3.0 Applicable Documents..... 4

4.0 Specific Tasks 4

5.0 Deliverables and Delivery Schedules 5

5.1 Licenses and Professional Services 5

5.2 Privacy..... 5

6.0 Government Furnished Equipment and Information 6

7.0 Period of Performance 6

8.0 Security..... 6

9.0 Special Considerations..... 6

9.1 Inspection and Acceptance..... 6

9.2 Task Order Administration 6

9.3 Invoice Instructions..... 7

9.4 Unique Standards 8

9.4.1 CBP Requirements..... 8

9.4.2 ISO Requirements..... 9

9.4.3 Section 508 Requirements 15

ADDENDUM A - Acronyms 17

ADDENDUM B – Acquisition Clauses..... 18

Wickr Software Licenses

PR # 2013-5100

1.0 Background

CBP is deploying a secure, multi-capability messaging capability that will enable CBP officers, agents, and staff to communicate in an ultra-secure, yet auditable manner. To support this requirement, CBP is engaging with Wickr Inc. to leverage their software capabilities.

2.0 Scope

This Statement of Work (SOW) describes delivery order for Wickr Software. Wickr is an instant messaging application which provides users with a secure messaging platform that enables voice and video chat, as well as file, video and photo transfers. For example, CBP requires a secure messaging application to meet multiple use-cases across all components. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

CBP-approved users of

Wickr will be able to access the application from mobile devices, laptops and workstations. This will allow for greater coordination at the operational and strategic planning level, as well as tactical coordination when needed.

The scope of this delivery order shall include several areas of capabilities:

1. The renewal of the existing Wickr user licenses and the ability to increase the number of CBP licenses available for users. The renewal period shall start at the end of the existing license period.
2. Professional Service Support hours to be provided by Wickr.
3. Licenses shall include the TAK plug-in (both Android and if applicable iOS)
4. Options for future development to support operational use cases such as:
 - a. Integrated Auth support for Macintosh OS X & Windows integrated AUTH clients using Azure as the Identity Provider (IDP).
5. Provide a solution to support High Availability (HA) and minimize the infrastructure downtime. The current environment is utilizing Docker Containers which does not allow for HA. The Docker Containers need to be migrated to Kubernetes Containers which would provide HA.
6. Create role base access controls (RBAC) with in the Wickr backend portal, Admin console, and replicated dashboard.
7. Currently both internal and external users are required to use a configuration file to onboard when launching Wickr. Develop a seamless workflow that does not require a configuration file to onboard both internal and external federation of agencies.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

The contractor shall have total program responsibility for ensuring that the requirements in this SOW are met.

This procurement will be competed through NASA SEWP contract holders. The contract will be firm fixed price.

3.0 Applicable Documents

- Executive Order -- Commission on Enhancing National Cybersecurity: <https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity>
- Section 508 of the Rehabilitation Act: <http://www.section508.gov/>
- DHS 4300A Policy Directive (Version 13.2, September 20, 2022)
- DHS 4300A Sensitive System Handbook: <https://www.dhs.gov/dhs-security-and-training-requirements-Contractors> <https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook>
- DHS IT Security Policies (National Institute of Standards and Technology (NIST) 800-47) & (CBP 1400-05C): <http://csrc.nist.gov/> (b)(7)(E) [/nistpubs/800-47/sp800-47.pdf](http://nistpubs/800-47/sp800-47.pdf)
- Department of Defense Information Assurance C&A Process (DIACAP): http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- U.S. Customs and Border Protection Information Systems Security Policies and Procedures Handbook, HB 1400-05D
- FEDRAMP Security Assessment Framework Resources <https://www.fedramp.gov/>

4.0 Specific Tasks

4.1 The contractor vendor shall provide (b)(7)(E)
(b)(7)(E)
(b)(7)(E) to procure within
the Base Period.

4.2 The contractor shall provide a Monthly Report due by the tenth (10th) business day of the month, supporting the hours utilized. The report should include the hours used and remaining along with a summary of what the hours were used for.

Wickr Software Licenses

PR # 2013-5100

5.0 Deliverables and Delivery Schedules

5.1 Licenses and Professional Services

The Contractor shall provide the WICKR licenses and professional services renewal without a lapse in coverage. The licenses and anything related shall be emailed to the Task Manager (TM) at their email address provided below in Section 11.0. The Period of Performance will be **9/16/2023 – 9/15/2024**.

Wickr Enterprise Package to include the following:

(b)(7)(E)

- 24/7/365 Help-desk support services

CDRL001	System Data: Messages, Files, Metadata, etc..	As Requested, At Contract Completion
CDRL002	Installation and Software Documentation	At Contract Award
CDRL003	Optional Platform Development	Contract Award
CDRL004	Training Documentation	At Contract Award

5.2 Privacy

Solution providers shall not display advertisements to end users of the Information System as part of its business model (i.e. not an advertising-based model).

Solution providers shall safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)” and in accordance with M-06-16: Protection of Sensitive Agency Information

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf> :

Safeguarding Against and Responding to the Breach of Personally Identifiable Information. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy. An Ordering Activity may request that PII be kept within U.S. Data Centers.

The solution must disclose privacy-impacting features that cannot be disabled.

6.0 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

No Government-furnished equipment and information is anticipated under this award.

7.0 PERIOD OF PERFORMANCE

The period of performance for the licenses will be **9/16/2023 – 9/15/2024**.

8.0 SECURITY

There are no specific security classification level requirements associated with this procurement action. Information is deemed unclassified.

9.0 Special Considerations

9.1 Inspection and Acceptance

The Government reserves the right to reject any deliverable based on defects with respect to completeness correctness, clarity, and consistencies. In the event of a rejection of any deliverable, the Contracting Officer will notify the contractor in writing within five (5) business days of the receipt of the deliverable of any deficiencies to be corrected. The contractor shall have five (5) business days to correct the deficiencies.

9.2 Task Order Administration

COR

(b)(6) (b)(7)(C)

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

The COR will provide no supervision to contractor personnel. The COR is not empowered to make any commitments or changes which affect the task order price or other items and conditions. Any such proposed changes must be brought to the immediate attention of the CO for action. The acceptance of any changes by the contractor without specific approval and written consent of the CO shall be at the contractor's risk.

Technical POCs:

(b)(6) (b)(7)(C)

National Finance Center:
CBPINVOICES@cbp.dhs.gov

9.3 Invoice Instructions

The Contractor shall submit an invoice (s) for the licenses. Invoice (s) shall be electronically transmitted to the COR as listed in section 9.2, and the Contractor shall invoice CBP in accordance with CBP invoicing clause, "Electronic Invoicing and Payment Requirements – Invoice Processing Platform (IPP) (JAN 2016)".

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer.

The Contractor shall submit an invoice for the cost. The invoice shall be simultaneously transmitted electronically to the COR and Task Monitor at the e-mail address provided in Section 9.2, the submittal e-mail must include the following information:

- Purchase Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

- Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

Payment requests should be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process". The IPP website address is <https://www.ipp.gov>.

The contractor must send a courtesy e-mail to the COR once an invoice is submitted. Only the CO has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

9.4 Unique Standards

9.4.1 CBP Requirements

CBP Enterprise Architecture Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Personal Identifiable Information (PII)

When a contractor, on behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredited (ATO) this information system to the (HHM) FIPS level.

9.4.2 ISO Requirements

DHS Security Policy Requirement

All hardware, software, and services provided under this task order must be compliant with DHS 4300A Policy Directive (Version 13.3, February 13, 2023).

Wickr Software Licenses

PR # 2013-5100

Encryption Compliance Requirement

- 1) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
- 2) National Security Agency (NSA) Type 2 or Type 1 encryption.
- 3) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS), DHS 4300A Policy Directive (Version 13.3, February 13, 2023).

Security Review Requirement

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

Supply Chain Risk Management Requirement

The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNS number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

1. How risks from the supply chain will be identified,
2. What processes and security measures will be adopted to manage these risks to the system or system components, and
3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COTR) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractor's Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the "end of life."). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

Cyber-Supply Chain Risk Management (C-SCRM)

a. Definitions

- i. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
- ii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
- iii. information and communications technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards,

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

- iv. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.
- b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product
 - i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new OEM.
 - ii. The contractor may provide previously-used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.
- c. List of Components in ICT Products
 - i. Contractors shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.
 - ii. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
 - iii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.
 - iv. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract, and replaced when End of Support (EoS) is reached.
- d. Supply-Chain Transport

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

- i. The contractor shall use formal and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.
- ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance, and make available for inspection upon request of the Government.
- iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.
- iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.
- v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Foreign Equities

The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any changes to corporate ownership or control from contract award through final delivery or the end of the period of performance.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility or information system access shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

Procurements for software products or software development shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

9.4.3 Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at <https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication

Section 508 Requirements for Technology Products

Section 508 applicability to Information and Communications Technology (ICT): WICKR Software Licenses

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results substantially equivalent or

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components: Does not apply

Applicable 508 requirements for software features and components (including but not limited to Web, desktop, server, mobile client applications): All requirements in Chapter 5 apply, including all WCAG 2.0 Level A and AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including but not limited to Mobile phones): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Section 508 Deliverables

Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at <https://www.itic.org/policy/accessibility/vpat>. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

ADDENDUM A - Acronyms

AES	Advanced Encryption Standard
CBP	Customs and Border Protection
CFR	Code of Federal Regulations
CISO	Chief Information Security Officer
CLIN	Contract Line Item Numbers
CO	Contracting Officer
COR	Contracting Officer's Representative
DIACAP	Department of Defense Information Assurance C&A Process
DHS	Department of Homeland Security
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
OIT	Office of Information and Technology
PII	Personally Identifiable Information
PIV	Personal Identification Verification
SOW	Statement of Work
TM	Task Manager

ADDENDUM B – Acquisition Clauses

HSAR 3052.204-71: CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) “Information Technology Resources” include, but are not limited Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, in-subordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
- (2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

Wickr Software Licenses

PR # 2013-5100

Safeguarding of Sensitive Information (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions.* As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO*. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review*. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations,

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and*

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- (i) Inspections,
- (ii) Investigations,
- (iii) Forensic reviews, and
- (iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements.*

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

address verification and/or address location services. At a minimum, the notification shall include:

- (i) A brief description of the incident;
- (ii) A description of the types of PII and SPII involved;
- (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
- (iv) Steps individuals may take to protect themselves;
- (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

- (1) Provide notification to affected individuals as described above; and/or

- (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

- (i) Triple credit bureau monitoring;
- (ii) Daily customer service;
- (iii) Alerts provided to the individual for changes and fraud; and
- (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
- (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization.*

**HSAR Class Deviation 15-01 Information Technology Security and Privacy Training
(MAR 2015)**

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs->

Statement of Work (SOW)

Wickr Software Licenses

PR # 2013-5100

security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements*. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.