



STATEMENT OF WORK

Gap Assessment

Optiv Opportunity Number: 1178331-2

Texas DIR Contract Number: DIR-TSO-4133

Issue Date: 6/21/2019

Optiv Security Inc. ("Optiv") has prepared this Statement of Work (SOW) for Williamson County, Texas ("Williamson County") for the consulting services ("Services") herein.

Service Overview

Background

Williamson County has identified a need to conduct a NIST SP 800-53 Risk Assessment. Optiv's NIST SP 800-53 Risk Assessment services assist clients with understanding the current state of risk to confidentiality, integrity, and availability of protected information in the enterprise, and provide guidance and recommendations for controls to reduce risk in the most cost-effective manner possible.

Overview

The NIST SP 800-53 Risk Assessment is an objective analysis of the effectiveness of current security controls that protect an organization's assets. The assessment also helps determine the threats and vulnerabilities to those assets. An effective security risk assessment allows an organization to make risk-based decisions (such as spending or additional analysis); to provide usable input into a security risk management program; and/or to provide necessary information for audit and compliance efforts.

The effectiveness of an organization's information security program depends on the ability to effectively measure and address the information security risks to the most critical systems and sensitive assets. The accurate assessment of risk allows for the effective and efficient selection and application of controls and countermeasures.

Optiv has developed an information security risk assessment method that is closely aligned with a number of risk management standards and risk assessment approaches developed by international and national standards bodies, including:

- ISO/IEC 27005: Information Security Risk Management
- ISO/IEC 27001: Information Security Management Systems - Requirements
- NIST SP 800-30: Guide for Conducting Risk Assessments
- NSA IAM/IEM
- RIIOT Data Gathering Approach¹
- Expected Elements Review²

¹ Landoll, Douglas J., *"The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments"*, Second Edition, May. 20, 2011, CRC Press.

² Ibid



Ultimately, an effective information security risk management program needs to be tailored to the needs of the organization. Optiv's experience enables this sort of tailoring in every project risk assessment project. The most effective information security risk management programs take specific business objectives and unique environments into account. This SOW details our approach to providing this assistance.

Service Activities and Approach

NIST SP 800-53 Risk Assessment

Pre-Engagement

Kick-Off Call

This Kick-Off Call consists of project planning and coordination and helps to identify the following items:

- Williamson County and Optiv resources and roles
- Agreement on project timeline and resource availability

Kick-Off Meeting

In this meeting, Optiv consultants and Williamson County will confirm and clarify the overall information security risk assessment structure and scope, including:

- Review business mission
- Confirm scope of controls to be assessed
- Confirm depth and breadth of data gathering activities
- Discuss/obtain any necessary permission and notification
- Define stakeholders and asset owners
- Define in-scope systems, controls, assets, and threats
- Review measurement approach:
 - Asset valuation
 - Threat determination
 - Vulnerability exploitation likelihood
 - Vulnerability impact
 - Safeguard effectiveness
 - Security risk determination

This structure and scope will guide all subsequent risk assessment activities.

Interview Planning

After the kick-off meeting, Optiv will provide communications content designed to inform intended interviewees of the planned activities, questions, and how they can prepare. Optiv recommends some level of internal project management support in organizing and distributing such communications appropriately.

Conduct Preliminary Interviews with Relevant Stakeholders

Optiv and Williamson County together will identify stakeholders across the organization for interviews. The goals of the interview sessions include:

- System and Data Identification:
 - Identify systems that are hosting, storing, processing, or transmitting protected data
- Controls Identification:
 - Map systems and identify controls
- Threat Identification:
 - Identify and confirm applicable threats to pre-defined assets
- Asset Valuation:
 - Interviews will be conducted with asset owners to determine the value of the assets, based on the value and criticality definitions developed during the initial Kick-Off phase of this engagement. Typically, protected assets are qualified by the volume and the accessibility of that data based on its network posture and business function (internal or external application, user base, etc.).
 - Assets will be grouped into categories (to cover such disparate assets as data, intellectual property, data center, applications, etc.), and ratings will be derived based upon value, criticality, and/or availability.
- Optiv will conduct interviews with individuals responsible for information security and IT governance, with Privacy and Compliance offices, with business units representing clinical, administrative, educational, and research areas, and with IT operations, HR, Legal, and physical facilities representatives. Interviews may be conducted in a workshop format or individually. Interviews typically are performed on-site at the employee's main office but may be conducted remotely as necessary. Optiv is flexible and is capable of accommodating schedules and activities within the scope of committed timelines of the overall project and within reason.

Data Gathering and Review

RIIOT Method

During the data-gathering phase, the consultants will apply various techniques to gain insight on the existence and effectiveness of the security controls. In order to control and manage the vast amount of potential controls and data gathering activities in this phase, Optiv utilizes the "Review, Interview, Inspect, Observe, and Test (RIIOT) Method" of data gathering. The RIIOT Method organizes each of the data gathering activities into one of these five different approaches as described below.

Within each of the data gathering areas (e.g. Administrative, Technical and Physical), not all RIIOT Methods may be appropriate for each of the data gathering exercises. Please note that it is not necessary or advisable to always use all of the RIIOT activities for each control assessment. The activities will be tailored based on what is appropriate for the specific assessment.

Gather Administrative Data

In this phase, Optiv will gather and review data concerning administrative controls. Steps include:

- Policy and Procedures and Security Awareness Program Review:
 - **Review documents** – Optiv consultants will review information security policies and procedures using the following approach:
 - Catalog and Review – Collect and catalog all available and relevant documents

- Clarity, Content, Compliance – Review documents for clarity (understandability for intended audience), content (completeness of document, correctness of controls, consistency with other documents), and compliance (review against regulations and laws)
 - **Interview key staff** – Optiv consultants will interview key staff members to gain an understanding of currently implemented controls and their perceived effectiveness.
 - **Observe behavior** – While onsite, Optiv consultants will observe the security-relevant behavior of individuals to determine compliance with policies and procedures.
- Security Organization Review:
 - **Review documents** – Optiv consultants will review organization charts, job descriptions, and key policies to determine the reporting structure and relevant roles within the information security organization.
 - **Interview key staff** – Optiv consultants will interview the identified key staff members to gain an understanding of the job functions, perceived effectiveness, and hindrances.

Gather Technical Data

In this phase, Optiv will gather and review data concerning technical controls. Steps include:

- Architectural Design Review:
 - **Review documents** – Optiv consultants will review available system and network design documents for the following areas:
 - Identification of Systems, Controls, and Interfaces
 - Implementation of Security Principles:
- Network Segmentation – Effective segmentation of networks to reduce scope of sensitive data exposure and user access
- Defense in Depth – Use of multiple controls to decrease exposure to threats
- Separation of Duty – Limitation of administrative privileges to the minimum set required to perform the job function
 - **Interview key staff** – Optiv consultants will interview IT operations personnel to confirm (or fill in gaps) from the information above, and to gain an understanding of currently implemented controls and their perceived effectiveness.
- Configuration Review:
 - **Review documents** – Optiv consultants will review available system and device configuration documents for the following areas:
 - Compliance with documented policies and procedures
 - Consistency between devices
 - **Interview key staff** – Optiv consultants will interview IT operations personnel to confirm (or fill in gaps) from the information above, and to gain an understanding of current configuration issues and the perceived effectiveness of the current configurations.

Gather Physical Data

In this phase, data will be gathered and reviewed concerning physical controls. Steps include:

- Perimeter/Internal Controls Review:
 - **Review documents** – Optiv consultants will review available documents, maps, and schematics regarding physical controls protecting the perimeter of the physical locations.

- **Interview key staff** – Optiv consultants will interview key staff members to gain an understanding of currently implemented controls and their perceived effectiveness.
- **Inspect controls** – Optiv consultants will inspect the general condition and coverage of perimeter controls.
- **Observe behavior** – While onsite, Optiv consultants will observe the security-relevant behavior of individuals to determine compliance with policies and procedures and the effectiveness of perimeter controls.
- **Environmental Controls Review:**
 - **Review documents** – Optiv consultants will review available documents, maps, and schematics regarding environmental controls protecting the sensitive areas (e.g. data centers) at the physical locations.
 - **Interview key staff** – Optiv consultants will interview key staff members to gain an understanding of currently implemented environmental controls and their perceived effectiveness.
 - **Inspect controls** – Optiv consultants will inspect the general condition and coverage of environmental controls.

Determine Base Control Gaps

Optiv will create a baseline for controls analysis using the following sources:

- **NIST SP 800-53 v4 (2013)** which includes domains covering the following topics:
 - Access Control
 - Awareness and Training
 - Audit and Accountability
 - Certification, Accreditation, and Security Assessments
 - Configuration Management
 - Contingency Planning
 - Identification and Authentication
 - Incident Response
 - Maintenance
 - Media Protection
 - Physical and Environmental Protection
 - Planning
 - Program Management
 - Personnel Security
 - Risk Assessment
 - System and Services Acquisition
 - System and Communications Protection
 - System and Information Integrity

These domain areas will be used to discuss current and expected controls in the Williamson County environment.



Determine Vulnerabilities

Optiv consultants will assess the information gathered through the RIIOT Method to determine the effectiveness of controls and to compile a list of vulnerabilities in each of the controls areas (e.g. Administrative, Technical and Physical).

Information Security Risk Analysis

Threat and Vulnerability Mapping

Each of the vulnerabilities will be paired with one or more appropriate threats to create threat/vulnerability pairs. For each vulnerability that is identified through either logical analysis or technical testing, Optiv will identify the control weakness, the paired threat that exercises the vulnerability to breach system security, and the relevant evidence collected on that vulnerability.

Determine Vulnerability Impact

Optiv rates the severity of each vulnerability (regardless of the threat pairing) based on the impact to the business if the vulnerability were successfully exercised. The severity rating is based on exposure of sensitive information, damage to critical systems, access to/control of critical systems, and/or damage to physical buildings.

Determine Vulnerability Realization Probability

Each threat/vulnerability pair is rated based on the likelihood that there will be attempts to exercise the vulnerability by the threat class and whether the threat class is able to exercise the vulnerability. The “threat attempt likelihood” and “vulnerability exercise success” ratings are determined based on Optiv experience, historic data, and any known industry statistics.

Calculate and Summarize Information Security Risk

A risk is calculated for each threat/vulnerability pair based on the vulnerability probability and impact ratings. These risks are summarized by risk categories that specify the severity of the information security risk.

A qualitative risk rating is calculated for each threat/vulnerability pair based on the vulnerability realization probability and vulnerability impact ratings. These qualitative risks ratings are classified by risk categories that specify the severity of the information security risk and the attention required to reduce the security risk to the system.

Document Risk Remediation Recommendations

Optiv consultants will identify risk remediation options for the identified information security risks. Remediation options (e.g. safeguards/additional controls) will be described in sufficient detail to support Williamson County’s decision whether to pursue implementation. This detail includes high-level descriptions of the class of recommended controls.

Documentation Deliverables

Optiv will provide Williamson County with the following deliverable documents (“Deliverables”) electronically in standard Optiv format.

NIST SP 800-53 Risk Assessment

Project Report

Optiv will provide project reports that includes the following:

- Executive Summary:
 - Overview of project and methodology
 - Abstract of findings (including positive and constructive feedback about current risks and control state)
 - Prioritized risks and recommendations (Top 10 list)
- Technical Report:
 - Findings grouped by NIST SP 800-53 Risk Assessment control areas, including:
 - Findings
 - Gaps
 - Risks
 - Recommendations
- Risk Treatment Roadmap:
 - Projects and activities
 - Sequence and order

Appendices will include: Controls used in baseline, Interviewee list, documentation collection list, and evidence references.

Formal Presentation

Optiv consultants will deliver a presentation (in the standard Optiv presentation format) via web conference to an audience chosen by Williamson County. Traditionally focused on an executive level out-brief, this presentation describes the effort executed, provides an overview of the results, and describes the next steps outlined for the organization.

Deliverable Acceptance

Deliverables defined in this SOW are subject to inspection and acceptance by the designated Williamson County Point of Contact (POC).

- There will be one (1) round of Deliverable review.
- Williamson County is responsible for consolidating its stakeholder feedback into a single view for Optiv within ten (10) business days.
- If Williamson County does not accept or reject the draft within this period, the Deliverable(s) shall be considered acceptable by Williamson County and a final version will be provided.

- If the draft is rejected, Optiv will update the within a mutually agreeable timeframe. Optiv will then provide the updated, finalized Deliverable to Williamson County.

Service Scope

Scoping Considerations

Scoping details listed below were provided by Williamson County through documents and/or interviews; and some assumptions may have been made based upon industry best practices.

NIST SP 800-53 Risk Assessment Scope

| Activity | Details |
|-------------------------------------|--|
| Onsite Visits (Physical reviews) | <ul style="list-style-type: none"> • One (1) |
| Interviews | <ul style="list-style-type: none"> • Interviews aligned to the domains of the framework chosen • Interviews aligned to the Applications or Processes in scope • Interviews aligned to the site visits • Specific interviewees will be defined during the kickoff process |
| Policies, Standards, and Procedures | <ul style="list-style-type: none"> • Up to 250 pages • Organization has central security policies and a single information security department and IT department |
| Applications and Environments | <ul style="list-style-type: none"> • One (1) |
| Additional Notes | <ul style="list-style-type: none"> • Optiv will map to HIPAA with the NIST 800-53 framework |

Project Scoping Assumptions

- "Business Hours" are Monday through Friday 8:00 A.M. to 5:00 P.M. (local US time). "Non-Standard Hours" include hours/testing windows/maintenance windows outside of Business Hours ("After Hours") or any hours that fall on Optiv-recognized holidays ("Holiday Hours").
- All work to be performed by Optiv under this SOW will be completed during Business Hours unless Non-Standard Hours are otherwise noted.
- Optiv assumes that all project phases will be conducted from the geographical location(s) or number of location(s) specified herein.
- Work described herein will be performed over continuous business days, unless specific breaks are otherwise noted.



- Significant variance from the scope stated herein or to the terms and conditions of this SOW will result in a written, mutually executed Change Order.

Risk Assessment Scoping Assumptions

- Williamson County is required to own its own copy of the standard(s)/framework(s) utilized in this assessment.

Professional Considerations

Rescheduling or Cancellation

In accordance with the Agreement, two (2) weeks' written notice is required for cancelling or rescheduling any services. If cancellation or rescheduling of on-site work occurs with less than two (2) weeks' advance notice, nonrefundable and/or nontransferable travel expenses will be billed to and paid by Williamson County at actual cost.

Optiv Responsibilities

The following list details Optiv's responsibilities for this project, in addition to performance of Services as described in the Approach section:

- Optiv will provide project facilitation, budget reporting, and Change Order management.
- Optiv consultants consider all Williamson County information and documentation as sensitive and confidential and will handle appropriately.
- Optiv shall have responsibility only for consultants employed or subcontracted by Optiv for performance of Services.

Williamson County Responsibilities

The following list details Williamson County's responsibilities for this project. Failure to meet these responsibilities may result in delay of the project or the need for a Change Order.

- Williamson County will provide access to items necessary for the success of this project in a commercially reasonable response time, including but not limited to:
 - One (1) primary POC for the project responsible for required meetings, coordination of other key personnel, data gathering, and project-related issues
 - Applicable proprietary information, applications, systems, and/or network diagrams
 - Facility and/or remote access
 - Operational Internet connection



Pricing, Payment, and Expenses

Fixed-Price Services

The Services shall be performed on a fixed-price basis.

| Description of Service | Price |
|---|-----------------|
| NIST 800-53 v4 Moderate Risk Assessment | \$57,300 |
| DIR Discount | (\$7,440) |
| Total | \$49,860 |

Note: Price is in accordance with the DIR-TSO-4133 Pricing Index.

Invoicing Terms

- Invoice 50% upon kick-off call and remaining 50% upon project completion.

Optiv reserves the right to invalidate and re-issue this SOW if not signed and returned in its entirety within 30 days of SOW Issue Date.

Additional Payment Terms

- All pricing is in U.S. Dollars (USD).
- For any un-scoped client-requested project holds greater than 30 days, Optiv will invoice for fees and charges accrued (using a pro-rated amount for fixed price services) for work performed up to the time of hold request.
- Any project remaining on un-scoped hold for 90 days will terminate and will be bound to any applicable termination provisions, unless otherwise mutually agreed to in writing.
- Termination of this SOW for any reason does not release either party from any liability, which, at the time of termination, has already accrued to the other party. Upon termination, Optiv will invoice for fees and charges accrued but unpaid as of the termination date.

Expenses

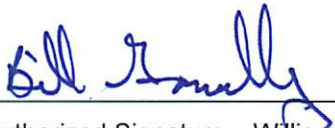
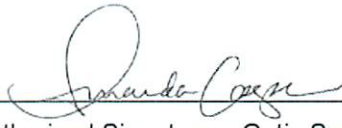

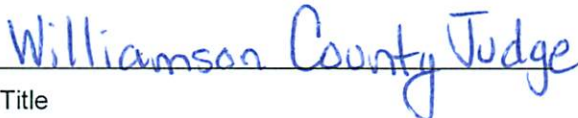

- Travel and expenses are not included in the price and will be invoiced monthly as incurred.
- Travel expenses will pre-approved by Williamson County.
- Travel and living expenses will be reimbursed at cost in accordance with applicable portions of the Williamson County Vendor Reimbursement Policy”.



Authorization/Signatures

All Services will be performed subject to the Statement of Work Terms and Conditions listed at the following URL: "<https://www.optiv.com/agreements>".

IN WITNESS WHEREOF, this SOW is agreed to and executed by duly authorized representatives of each party and shall be binding as of the date of last signature below ("SOW Effective Date").

| | |
|--|--|
|  |  |
| Authorized Signature – Williamson County, Texas | Authorized Signature – Optiv Security Inc. |
|  | Amanda Cooper |
| Name Printed | Name Printed |
|  | Senior Director, SOW Development |
| Title | Title |
|  | 6/21/2019 |
| Date | Date |

Opportunity #: 1178331-2

The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination or other use of or taking of any action upon this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability.

Handwritten or typewritten text (or any other unauthorized modification or file export/conversion) intended to alter the original content of this SOW will have no effect and will not modify the terms of this SOW.



Appendix A - Key Points of Contact

Optiv Sales Contacts

Michael Spess

Account Manager

512.203.7288

mike.spess@optiv.com

Jim Chefan

Solutions Architect

832.280.7655

jim.chefan@optiv.com

Michael Scott

Sr. Advisor – Risk Management

michael.scott@optiv.com

Christy Anders

SOW Development Manager

christy.anders@optiv.com

Williamson County Contacts

Project Lead – Lead resource that the Optiv PMO will make initial contact with to discuss project details and scheduling.

Technical Lead – Lead resource that the Optiv consultant(s) will be interacting with through the course of the project for technical information.

Billing Contact – Lead resource that will receive all project-related Optiv invoices.

Project & Technical Lead

Minnie Beteille

Technology Services Project Manager

512.943.1448

mbeteille@wilco.org

Billing Contact

Minnie Beteille

405 Martin Luther King Street

Georgetown, TX 78626

512.943.1448

mbeteille@wilco.org

Appendix B - Statement of Work Terms and Conditions

The following Statement of Work Terms and Conditions govern the statement of work or other work order ("SOW") between Optiv Security Inc. or one of its Affiliates (the applicable entity identified in the SOW as providing Services is defined as "Contractor") and the client described in the SOW ("Client") and apply to all Services and Deliverables (both defined below) provided by Contractor. "Affiliate" or "Affiliates" means any entity that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with OPTIV Security Inc., and its successors and assigns.

1. **Services and Deliverables.** The services to be performed by Contractor ("Services") and any deliverables to be provided by Contractor ("Deliverables") are set forth in the SOW.
2. **Fees.** Client agrees to pay Contractor the fees set forth in the SOW. Client further agrees to reimburse Contractor for actual, third party, reasonable travel and living expenses incurred by Contractor in connection with the performance of Services. Unless otherwise specified in the SOW, expenses are subject to the Contractor Travel Policy, available upon request. Client will pay or reimburse to Contractor all sales, service, value added and other taxes on the Services (other than tax imposed upon the income of Contractor). Unless otherwise set forth in the SOW, Contractor's invoices are due and payable by Client in full within thirty (30) days from the invoice date. Undisputed invoices not paid within thirty (30) days from the invoice date will bear interest from the due date until paid at a rate of one and one-half percent (1.5%) per month or the maximum rate permitted by law, whichever is less. Client shall also be responsible for all collection costs incurred by Contractor in connection with past due undisputed invoices.
3. **Warranties and Covenants.** Contractor covenants that it and its employees ("Contractor Personnel") will provide the Services in accordance with: (i) the prevailing standard of care exercised by consultants in the information security industry, and (ii) applicable laws and governmental regulations. If any material portion of the Services or Deliverables does not conform to the forgoing covenants, and Client notifies Contractor within fifteen (15) days of completion of the Services and delivery of Deliverables, then Contractor will work diligently to re-perform the nonconforming portion of the Services and/or Deliverables. Contractor will not be responsible for nonconformities arising from inaccurate or incomplete data or information provided by Client, for failures or delays caused by Client's failure to perform its obligations under the SOW or these Terms and Conditions, or for failures, damages or delays caused by third party hardware, software or other products. Contractor hereby waives and disclaims all other warranties, express or implied, including without limitation implied warranties of merchantability and fitness for a particular purpose. Client agrees to reasonably cooperate with Contractor in the performance of Services. Unless otherwise expressly stated in the SOW, the Services may be rendered at Client's, Contractor's or subcontractor's facilities or at other suitable locations.
4. **Ownership of Deliverables.** The parties agree that, except as specifically provided herein or the SOW, all Deliverables are the property of Client. Notwithstanding the foregoing, the parties agree that any know-how, processes, techniques, concepts, methodologies, tools, ideas, designs, inventions, patents, copyrights, improvements, processes, computer programs, software, source code, object code, graphics, intellectual property, information and/or pictorial representations that (i) Contractor developed prior to entering into the SOW with Client; (ii) is or are developed separate and apart from the SOW and Services at any time by Contractor, or (iii) led to or produced the results of the Services or that were otherwise used by Contractor to provide the Services (collectively, "Contractor Intellectual Property") shall not be considered work for hire and shall remain the exclusive property of Contractor. In the event Contractor Intellectual Property is incorporated into any Deliverables, Contractor grants Client an irrevocable, nonexclusive, royalty-free, limited license for Client to use Contractor Intellectual Property to the extent necessary to use such Deliverable for its internal purposes only.
5. **Confidential Information.**
 - 5.1. **Defined.** "Confidential Information," as used herein, means all information proprietary to a party or its affiliates any of its customers or suppliers that is marked as confidential or that due to its nature is known or in good faith should be known to be confidential. Confidential Information of Client will be deemed to include, without limitation, all confidential Client data to which Contractor obtains access by performing the Services and any Deliverable containing such data. Confidential Information of Contractor will be deemed to include, without limitation, all Contractor Intellectual Property. The obligations of the party ("Receiving Party") that receives Confidential Information of the other party ("Disclosing Party") shall not apply to Confidential Information: (i) generally available to the public at any time at no fault of the Receiving Party, (ii) furnished at any time to the Receiving Party by a third party having the right to furnish it with no obligation of confidentiality to the Disclosing Party, (iii) independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party, (iv) approved for use or disclosure by written authorization from the Disclosing Party or (v) required to be disclosed pursuant to a valid order by a court or other governmental entity with jurisdiction, provided that the Receiving Party provides the Disclosing Party with prompt written notice of such order in order to permit the Disclosing Party to challenge such disclosure.
 - 5.2. **Obligations.** The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation hereof and to use Confidential Information of the Disclosing Party solely for the purposes hereof. Upon demand by the Disclosing Party, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information; provided that the Receiving Party may retain one archival copy solely for the purpose of administering its obligations under the SOW; and provided further that Client may retain any Deliverables subject to any license set forth herein. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party. The Receiving Party may disclose Confidential Information of the Disclosing Party to



its employees, officers, directors and representatives who have a reasonable need to know such Confidential Information in connection with the Services.

5.3. **Injunction.** Both parties agree that violation of any provision of this Section 5 would cause the Disclosing Party irreparable injury for which it would have no adequate remedy at law, and that the Disclosing Party will be entitled to immediate injunctive relief prohibiting such violation, in addition to any other rights and remedies available to it.

6. **Indemnification.** To the extent authorized under Texas law, except to the extent caused by the acts, errors or omissions of the indemnified party, each party shall indemnify, defend and hold harmless the other party and its affiliates and their respective officers, directors, employees and agents from and against third party claims made against the indemnified party for death, bodily injury or physical damage to or loss or destruction of any real or tangible personal property to the extent caused by the indemnifying party's gross negligence or willful misconduct, but only to the extent permitted by Texas law.
7. **Limitation of Liability.** To the extent authorized under Texas law, in no event will either party or its affiliates (including, without limitation, Contractor's Affiliates) or suppliers, or any of their respective officers, directors, employees, or agents, be liable to the other party or its affiliates, whether in contract or in tort or under any other legal theory (including, without limitation, strict liability and negligence), for lost profits or revenues, loss of use or loss or corruption of data, for equipment or systems outages or downtime, or for any indirect, special, exemplary, punitive, multiple, incidental, consequential or similar damages, arising out of or in connection with the SOW or otherwise, even if advised of the possibility of such damages. In no event will Contractor's, Contractor's Affiliates', their supplier's, or their respective officers', directors', employees' or agents' aggregate liability for all claims arising out of or in connection with the Services, Deliverables, the SOW and otherwise exceed the amount of fees actually paid by Client to Contractor under the SOW. No action regarding the Services or Deliverables, other than with respect to payments hereunder, may be brought more than one (1) year after the first to occur of either (a) the conclusion of Services and delivery of any Deliverables under the SOW, or (b) the claimant party's knowledge of the event giving rise to such cause of action.
8. **Non-Solicitation.** Client agrees that it and its affiliates, and their employees, will not, either during or for a period of twelve (12) months after termination or expiration of the SOW, solicit to hire as an employee or contractor any of Contractor's and/or Contractor's Affiliates' employees. Publication of open positions in media of general circulation (e.g., Internet website job postings) will not constitute solicitation of employees. If Client or one of its affiliates hires any employee(s) of Contractor and/or Contractor's Affiliates prior to expiration of the twelve (12) month period, as an employee or contractor, Client agrees to pay to Contractor or Contractor's Affiliates, as applicable, within thirty (30) days of the hiring date, an amount equal to the person's annual compensation (including bonuses) at Contractor and/or Contractor's Affiliates at the time of his or her departure from Contractor and/or Contractor's Affiliates.
9. **Contractor's Affiliates.** Contractor's Affiliates, and/or employees of Contractor's Affiliates, may provide Services under the SOW. Such Affiliates and/or their employees that provide Services will be subject to these Terms and Conditions. Only the entity that is defined as Contractor and/or provides Services will be liable under these Terms and Conditions with respect to such Services. There shall be no joint and several liability with respect to entities that do not provide Services under these Terms and Conditions.
10. **Assignment.** Except as otherwise set forth in these Terms and Conditions, neither party may assign the SOW or these Terms and Conditions without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign the SOW or these Terms and Conditions without consent to any parent, subsidiary or other affiliate, in connection with a merger involving any of its affiliates or in connection with an acquisition of all or substantially all of such party's assets or equity interests. In addition, Contractor may assign the SOW or these Terms and Conditions to an Affiliate.
11. **Notices.** All notices and other communications hereunder will be in writing and deemed delivered one (1) day after being sent by a nationally recognized overnight courier service or three (3) days after being sent certified U.S. mail, return receipt requested, postage prepaid. All notices and other communications hereunder will be given to the party at the address indicated in the SOW.
12. **Governing Law.** The SOW and these Terms and Conditions will be governed by, and construed and enforced in accordance with, the laws of the State of Texas, excluding conflicts of law principles. Exclusive jurisdiction for any lawsuit or claim in connection with the SOW and these Terms and Conditions shall be in the state or federal courts of the State of Texas.
13. **Execution in Counterparts.** The SOW may be executed in any number of counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same agreement. Delivery of an executed counterpart of the SOW by electronic transmission or any other reliable means shall be effective for all purposes as delivery of a manually executed original counterpart. Either party may maintain a copy of the SOW in electronic form.

Miscellaneous. These Terms and Conditions are made a part of and incorporated into the SOW. The SOW, Texas DIR Contract Number: DIR-TSO-4133 and these Terms and Conditions constitute the entire agreement between the parties with respect to its subject matter. The parties agree that as of the Effective Date, these Terms and Conditions will supersede, terminate and replace in its entirety all prior services agreements, product purchase agreements, and confidentiality agreements between the parties or their predecessors in interest. These Terms and Conditions shall govern in the event of a direct conflict with the SOW and Texas DIR Contract Number: DIR-TSO-4133, unless the SOW expressly specifies that the SOW shall control in the event of a direct conflict. During the term of the SOW, a purchase order, acknowledgment form or similar routine document may be used. The parties agree that any provisions of such routine documents, which purport to add to or change, or which conflict with the provisions of the SOW or these Terms and Conditions shall be deemed deleted and have no force or effect. No forbearance, failure or delay in exercising any right, power or privilege is waiver thereof. In the event a court of competent jurisdiction holds any provision of the SOW or these Terms and Conditions invalid or unenforceable, the remainder of the SOW and these Terms and Conditions will continue in effect. Each party agrees that it will not, without prior written consent of the other party, use in advertising or other publicity the name of the other party. Neither party is liable for non-performance under the SOW and these Terms and Conditions to the extent to which the non-performance



is caused by events or conditions beyond that party's control; provided, however, this shall not apply to either party's obligations with respect to payments pursuant to the terms of the SOW and these Terms and Conditions.