TIPS VENDOR AGREEMENT

TIPS RFP 230504 Information Technology Equipment, Software, and Services

The following Vendor Agreement ("Agreement") creates a legal agreement between The Interlocal Purchasing System ("TIPS"), a government purchasing cooperative and Department of Texas Region 8 Education Service Center and (INSERT ENTITY NAME):

U.S. TelePacific Corp., dba TPx Communications

---

its owners, agents, subsidiaries, and affiliates (together, "Vendor") (individually, "Party", and collectively the "Parties") and this agreement shall exclusively govern the contractual relationship ("Agreement") between the Parties.

TIPS, a governmental entity and a national purchasing cooperative seeks to provide a valuable and necessary solution to public entities and qualifying non-profits by performing the public procurement solicitation process and awarding compliant contracts to qualified vendors. Then, where the law of a customer's jurisdiction allows, instead of public entities and qualifying non-profits expending time, money, and resources on the extensive public procurement process, the use of TIPS allows public entities to quickly select and purchase their preferred products or services from qualified, competitively evaluated vendors through cooperative purchasing.

1. **Purpose.** The purpose of this Agreement is to identify the terms and conditions of the relationship between TIPS and Vendor. Public entities and qualifying non-profits that properly join or utilize TIPS "(TIPS Members") may elect to "piggyback" off of TIPS' procurements and agreements where the laws of their jurisdiction allow. TIPS Members are not contractual parties to this Agreement although terms and conditions of this Agreement may ensure benefits to TIPS Members.

2. **Authority.** The Parties agree that the signatories below are individual authorized to enter into this Agreement on behalf of their entity and that they are acting under due and proper authority under applicable law.

3. **Definitions.**

    a. **TIPS Pricing:** The specific pricing, discounts, and other pricing terms and incentives which Vendor submitted and TIPS approved for each respective TIPS Contract awarded to Vendor and all permissible, subsequent pricing updates submitted by Vendor and accepted by TIPS, if any.

    b. **Authorized Reseller:** A reseller or dealer authorized and added by a Vendor through their online TIPS Vendor Portal to make TIPS sales according to the terms and conditions herein.

4. **Entire Agreement.** This Agreement resulted from TIPS posting a "TIPS Solicitation" (RFP, RCSP, RFQ, or other) and Vendor submitting a proposal in response to that posted TIPS Solicitation for evaluation and award. The Parties agree that this Agreement consists of the provisions set forth herein and: (1) The TIPS solicitation document resulting in this Agreement; (2) Any addenda or clarifications issued in relation to the TIPS solicitation; (3) All solicitation information provided to Vendor by TIPS through the TIPS eBid System; (3) Vendor's entire proposal response to the TIPS solicitation including all accepted required attachments, acknowledged notices and certifications, accepted negotiated terms, pricing, accepted responses to questions, and accepted written clarifications of Vendor's proposal, and; any properly included attachments to this Agreement. All documentation and information listed is hereby incorporated by reference as if set forth herein verbatim. In the event of conflict between the terms herein and one of the incorporated documents the terms and conditions herein shall control.

5. **Vendor's Specific Warranties, Terms, and License Agreements.** Because TIPS serves public entities and non-profits throughout the nation all of which are subject to specific laws and policies of their jurisdiction, as a matter of standard practice, TIPS does not typically accept a Vendor's specific "Sale Terms" (warranties, license agreements, master agreements, terms and conditions, etc.) on behalf of all TIPS Members. TIPS may permit Vendor to attach those to this Agreement to display to interested customers what terms may apply to their Supplemental Agreement with Vendor (if submitted by Vendor for that purpose). However, unless this term of the Agreement is negotiated and modified to state otherwise, those specific Sale Terms are not accepted by TIPS on behalf of all TIPS Members and each Member may choose whether to accept, negotiate, or reject those specific Sale Terms, which must be reflected in a separate agreement between Vendor and the Member in order to be effective.

6. **Vendor Identity and Contact Information.** It is Vendor's sole responsibility to ensure that all identifying vendor information (name, EIN, d/b/a's, etc.) and contact information is updated and current at all times within the TIPS eBid System and the TIPS Vendor Portal. It is Vendor's sole responsibility to confirm that all e-correspondence issued from tips-usa.com, ionwave.net, and tipsconstruction.com

to Vendor's contacts are received and are not blocked by firewall or other technology security. Failure to permit receipt of correspondence from these domains and failure to keep vendor identity and contact information current at all times during the life of the contract may cause loss of TIPS Sales, accumulating TIPS fees, missed rebid opportunities, lapse of TIPS Contract(s), and unnecessary collection or legal actions against Vendor. It is no defense to any of the foregoing or any breach of this Agreement that Vendor was not receiving TIPS' electronic communications issued by TIPS to Vendor's listed contacts.

7. **Initiation of TIPS Sales.** When a public entity initiates a purchase with Vendor, if the Member inquires verbally or in writing whether Vendor holds a TIPS Contract, it is the duty of the Vendor to verify whether the Member is seeking a TIPS purchase. Once verified, Vendor must include the TIPS Contract Number on all purchase communications and sales documents exchanged with the TIPS Member.

8. **TIPS Sales and Supplemental Agreements.** The terms of the specific TIPS order, including but not limited to: shipping, freight, insurance, delivery, fees, bonding, cost, delivery expectations and location, returns, refunds, terms, conditions, cancellations, order assistance, etc., shall be controlled by the purchase agreement (Purchase Order, Contract, Invoice, etc.) (hereinafter "Supplemental Agreement") entered into between the TIPS Member Customer and Vendor only. TIPS is not a party to any Supplemental Agreement. All Supplemental Agreements shall include Vendor's Name, as known to TIPS, and TIPS Contract Name and Number. Vendor accepts and understands that TIPS is not a legal party to TIPS Sales and Vendor is solely responsible for identifying fraud, mistakes, unacceptable terms, or misrepresentations for the specific order prior to accepting. Vendor agrees that any order issued from a customer to Vendor, even when processed through TIPS, constitutes a legal contract between the customer and Vendor only. When Vendor accepts or fulfills an order, even when processed through TIPS, Vendor is representing that Vendor has carefully reviewed the order for legality, authenticity, and accuracy and TIPS shall not be liable or responsible for the same. In the event of a conflict between the terms of this TIPS Vendor Agreement and those contained in any Supplemental Agreement, the provisions set forth herein shall control unless otherwise agreed to and authorized by the Parties in writing within the Supplemental Agreement.

9. **Right of Refusal.** Vendor has the right not to sell to a TIPS Member under the awarded agreement at Vendor's discretion unless otherwise required by law.

10. **Reporting TIPS Sales**. Vendor must report all TIPS Sales to TIPS. If a TIPS sale is initiated by Vendor receiving a TIPS Member's purchase order from TIPS directly, Vendor may consider that specific TIPS Sale reported. Otherwise, with the exception of TIPS Automated Vendors, who have signed an exclusive agreement with TIPS regarding reporting, all TIPS Sales must be reported to TIPS by either: (1) Emailing the purchase order or similar purchase document (with Vendor's Name, as known to TIPS, and the TIPS Contract Name and Number included) to TIPS at tipspo@tips-usa.com with "Confirmation Only" in the subject line of the email within three business days of Vendor's acceptance of the order, or; (2) Within 3 business days of the order being accepted by Vendor, Vendor must login to the TIPS Vendor Portal and successfully self-report all necessary sale information within the Vendor Portal and confirm that it shows up accurately on your current Vendor Portal statement. No other method of reporting is acceptable unless agreed to by the Parties in writing. Failure to report all sales pursuant to this provision may result in immediate cancellation of Vendor's TIPS Contract(s) for cause at TIPS' sole discretion. Please refer to the TIPS Accounting FAQ's for more information about reporting sales and if you have further questions, contact the Accounting Team at accounting@tips-usa.com.

11. **TIPS Administration Fees.** The collection of administrative fees by TIPS, a government entity, for performance of these procurement services is required pursuant to Texas Government Code Section 791.011 et. seq. The administration fee ("TIPS Administration Fee") is the amount legally owed by Vendor to TIPS for TIPS Sales made by Vendor. The TIPS Administration Fee amount is typically a set percentage of the amount paid by the TIPS Member for each TIPS Sale, less shipping cost, bond cost, and taxes if applicable and identifiable, which is legally due to TIPS, but the exact TIPS Administration Fee for this Contract is published in the corresponding solicitation and is incorporated herein by reference. TIPS Administration Fees are due to TIPS promptly upon Vendor's receipt of payment, including partial payment, for a TIPS Sale. The TIPS Administration Fee is assessed on the amount paid by the TIPS Member, not on the Vendor's cost or on the amount for which the Vendor sold the item to a dealer or Authorized Reseller. Upon receipt of payment for a TIPS Sale, including partial payment (which renders TIPS Administration Fees promptly due), Vendor shall issue to TIPS the corresponding TIPS Administration Fee payment as soon as possible but not later than thirty-one calendar days following Vendor's receipt of payment. Vendor shall pay TIPS via check unless otherwise agreed to by the Parties in writing. Vendor shall include clear documentation with the issued payment dictating to which sale(s) the amount should be applied. Vendor may create a payment report within their TIPS Vendor Portal which is the preferred documentation dictating to which TIPS Sale(s) the amount should be applied. Failure to pay all TIPS Administration Fees pursuant to this provision may result in immediate cancellation of Vendor's TIPS Contract(s) for cause at TIPS' sole discretion as well as the initiation of collection and legal actions by TIPS against Vendor to the extent permitted by law. Any overpayment of participation fees to TIPS by Vendor will be refunded to the Vendor within ninety (90) days of receipt of notification if TIPS receives written notification of the overpayment not later than the expiration of six (6) months from the date of overpayment and TIPS determines that the amount was not legally due to TIPS pursuant to this agreement and applicable law. Any notification of overpayment received by TIPS after the expiration of six (6) months from the date that TIPS received the payment will render the overpayment non-refundable. Region 8 ESC and TIPS reserve the right to extend the

six (6) month deadline if approved by the Region 8 ESC Board of Directors. TIPS reserves all rights under the law to collect TIPS Administration Fees due to TIPS pursuant to this Agreement.

12. **Term of the Agreement.** This Agreement with TIPS is for approximately five years with a one-year, consecutive option for renewal as described herein. Renewal options are not automatic and shall only be effective if offered by TIPS at its sole discretion. If TIPS offers a renewal option, the Vendor will be notified via email issued to Vendor's then-listed Primary Contact. The renewal option shall be deemed accepted by Vendor unless Vendor notifies TIPS of its objection to the renewal option in writing and confirms receipt by TIPS.

    Actual Effective Date: Agreement is effective upon signature by authorized representatives of both Parties. The Effective Date does not affect the "Term Calculation Start Date."

    Term Calculation Start Date: To keep the contract term consistent for all vendors awarded under a single TIPS contract, Vendor shall calculate the foregoing term as starting on the last day of the month that "Award Notifications" are anticipated as published in the Solicitation, regardless of the actual Effective Date.

    Example of Term Calculation Start Date: If the anticipated "Award Date" published in the Solicitation is May 22, 2023, but extended negotiations delay award until June 27, 2023 (Actual Effective Date), the Term Calculation Start Date shall be May 31, 2023 in this example.

    Contract Expiration Date: To keep the contract term consistent for all vendors awarded under a single TIPS contract, the term expiration date shall be five-years from the Term Calculation Start Date.

    Example of Contract Expiration Date: If the anticipated "Award Date" published in the Solicitation is May 22, 2023, but extended negotiations delay award until June 27, 2023 (Actual Effective Date), the Term Calculation Start Date shall be May 31, 2023 and the Contract Expiration Date of the resulting initial "five-year" term, (which is subject to an extension(s)) will be May 31, 2028 in this example.

    Option(s) for Renewal: Any option(s) for renewal shall begin on the Contract Expiration Date, or the date of the expiration of the prior renewal term where applicable, and continue for the duration specified for the renewal option herein.

    Example of Option(s) for Renewal: In this example, if TIPS offers a one-year renewal and the Contract Expiration Date is May 31, 2028, then the one-year renewal is effective from May 31, 2028 to May 31, 2029.

    TIPS may offer to extend Vendor Agreements to the fullest extent the TIPS Solicitation resulting in this Agreement permits.

13. **TIPS Pricing.** Vendor agrees and understands that for each TIPS Contract that it holds, Vendor submitted, agreed to, and received TIPS' approval for specific pricing, discounts, and other pricing terms and incentives which make up Vendor's TIPS Pricing for that TIPS Contract ("TIPS Pricing"). Vendor confirms that Vendor will not add the TIPS Administration Fee as a charge or line-item in a TIPS Sale. Vendor hereby certifies that Vendor shall only offer goods and services through this TIPS Contract if those goods and services are included in or added to Vendor's TIPS Pricing and approved by TIPS. TIPS reserves the right to review Vendor's pricing update requests as specifically as line-item by line-item to determine compliance. However, Vendor contractually agrees that all submitted pricing updates shall be within the original terms of the Vendor's TIPS Pricing (scope, proposed discounts, price increase limitations, and other pricing terms and incentives originally proposed by Vendor) such that TIPS may accept Vendors price increase requests as submitted without additional vetting at TIPS discretion. Any pricing quoted by Vendor to a TIPS Member or on a TIPS Quote shall never exceed Vendor's TIPS Pricing for any good or service offered through TIPS. TIPS Pricing price increases and modifications, if permitted, will be honored according to the terms of the solicitation and Vendor's proposal, incorporated herein by reference.

14. **Indemnification of TIPS.** **VENDOR AGREES TO INDEMNIFY, HOLD HARMLESS, AND DEFEND TIPS, TIPS MEMBERS, TIPS OFFICERS, TIPS EMPLOYEES, TIPS DIRECTORS, AND TIPS TRUSTEES (THE "TIPS INDEMNITEES") FROM AND AGAINST ALL CLAIMS AND SUITS BY THIRD-PARTIES FOR DAMAGES, INJURIES TO PERSONS (INCLUDING DEATH), PROPERTY DAMAGES, LOSSES, EXPENSES, FEES, INCLUDING COURT COSTS, ATTORNEY'S FEES, AND EXPERT FEES, ARISING OUT OF OR RELATING TO VENDOR'S PERFORMANCE UNDER THIS AGREEMENT (INCLUDING THE PERFORMANCE OF VENDOR'S OFFICERS, EMPLOYEES, AGENTS, AUTHORIZED RESELLERS, SUBCONTRACTORS, LICENSEES, OR INVITEES), REGARDLESS OF THE NATURE OF THE CAUSE OF ACTION, INCLUDING WITHOUT LIMITATION CAUSES OF ACTION BASED UPON COMMON, CONSTITUTIONAL, OR STATUTORY LAW TO THE EXTENT ARISING FROM (I) ALLEGATIONS OF NEGLIGENT OR INTENTIONAL ACTS OR OMISSIONS ON THE PART OF VENDOR, ITS OFFICERS, EMPLOYEES, AGENTS, AUTHORIZED RESELLERS, SUBCONTRACTORS, LICENSEES, OR INVITEES, (II) BREACH OF CONTRACT, (III) VIOLATION OF APPLICABLE LAW, OR (IV) ALLEGATIONS OR CLAIMS THAT ANY VENDOR DATA (AS DEFINED IN SECTION 15) INFRINGES ON THE INTELLECTUAL PROPERTY RIGHTS OF A THIRD-PARTY OR VENDOR. FOR AVOIDANCE OF DOUBT, THIS INDEMNIFICATION OBLIGATION COVERS VENDORS PERFORMANCE UNDER THIS AGREEMENT, AND DOES NOT INCLUDE VENDOR'S INDEMNIFICATION RESPONSIBILITIES UNDER ANY SUPPLEMENTAL AGREEMENT BY AND BETWEEN VENDOR AND A TIPS**

MEMBER. EXCEPT AS EXPRESSLY SET FORTH HEREIN, VENDOR'S LIABILITY TO TIPS OR A TIPS INDEMNITEE UNDER THIS AGREEMENT SHALL IN NO EVENT EXCEED THREE TIMES (3X) THE AGGREGATE TIPS SALES PAYMENTS RECEIVED BY VENDOR RIN THE 12 MONTH PERIOD IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO THE CLAIM. THE PRECEDING LIMITATION OF LIABILITY SHALL NOT APPLY FOR LOSSES ARISING FROM PERSONAL INJURY OR PROPERTY DAMAGE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES, REGARDLESS OF WHETHER THE PARTY WAS MADE AWARE OF THE CIRCUMSTANCES GIVING RISE TO SUCH LOSSES. APART FROM THIS INDEMNIFICATION PROVISION REQUIRING INDEMNIFICATION OF THE TIPS INDEMNITEES' ATTORNEY'S FEES AS SET FORTH ABOVE, RECOVERY OF ATTORNEYS' FEES BY THE PREVAILING PARTY IS AUTHORIZED ONLY IF AUTHORIZED BY TEX. EDUC. CODE § 44.032(F).

15. **Waiver and Assumption of Risk – Vendor Data.** **VENDOR AGREES THAT IT IS VOLUNTARILY PROVIDING DATA (INCLUDING BUT NOT LIMITED TO: VENDOR INFORMATION, VENDOR DOCUMENTATION, VENDOR'S PROPOSALS, VENDOR PRICING SUBMITTED OR PROVIDED TO TIPS, TIPS CONTRACT DOCUMENTS, TIPS CORRESPONDENCE, VENDOR LOGOS AND IMAGES, VENDOR'S CONTACT INFORMATION, VENDOR'S BROCHURES AND COMMERCIAL INFORMATION, VENDOR'S FINANCIAL INFORMATION, VENDOR'S CERTIFICATIONS, AND ANY OTHER VENDOR INFORMATION OR DOCUMENTATION, INCLUDING WITHOUT LIMITATION SOFTWARE AND SOURCE CODE UTILIZED BY VENDOR, SUBMITTED TO TIPS BY VENDOR AND ITS AGENTS) ("VENDOR DATA") TO TIPS. FOR THE SAKE OF CLARITY, AND WITHOUT LIMITING THE BREADTH OF THE INDEMNITY OBLIGATIONS IN SECTION 14 ABOVE, VENDOR AGREES TO WAIVE ANY CLAIMS IT MAY HAVE AGAINST TIPS INDEMNITEES RELATING TO ANY UNAUTHORIZED, NEGLIGENT OR WRONGFUL USE OF VENDOR DATA BY VENDOR, TIPS, OR TIPS INDEMNITEES. S. FOR AVOIDANCE OF DOUBT, VENDOR DATA, AS USED HEREIN, MEANS THE INFORMATION PROVIDED BY VENDOR TO TIPS AS A PART OF ITS PARTICIPATION IN THE TIPS SOLICITATION AND EXPRESSLY EXCLUDES ANY INFORMATION, SOFTWARE OR OTHER PROPRIETARY INFORMATION THAT IS PROVISIONED OR OTHERWISE DELIVERED TO A TIPS MEMBER AS A PART OF THE VENDOR SERVICES.**

16. **Procedures Related to Indemnification.** In the event that an indemnity obligation arises, Vendor shall pay all amounts set forth in Section 14 above (including any settlements) and – if it has accepted its indemnity obligation without qualification – control the legal defense to such claim or cause of action, including without limitation attorney selection, strategy, discovery, trial, appeal, and settlement, and TIPS shall, at Vendor's cost and expense (with respect to reasonable out of pocket costs and expenses incurred by TIPS which shall be reimbursed to TIPS by Vendor), provide all commercially reasonable assistance requested by Vendor. In controlling any defense, Vendor shall ensure that all assertions of governmental immunity and all applicable pleas and defenses shall be promptly asserted.

17. **Indemnity for Underlying Sales and Supplemental Agreements.** As between Vendor and TIPS, Vendor shall be solely responsible for any customer claims or any disputes arising out of TIPS Sales or any Supplemental Agreement as if sold in the open-market, except to the extent such claim or dispute arises from a misrepresentation or other misconduct by TIPS. The Parties agree that TIPS shall not be liable for any claims arising out of Vendor's TIPS Sales or Supplemental Agreements, including but not limited to: allegations of product defect or insufficiency, allegations of service defect or insufficiency, allegations regarding delivery defect or insufficiency, allegations of fraud or misrepresentation (except where directly arising from TIPS fraud or misrepresentation), allegations regarding pricing or amounts owed for TIPS sales, and/or allegations regarding payment, over-payment, under-payment, or non-payment for TIPS Sales. Payment/Drafting, overpayment/over-drafting, under-payment/under-drafting, or non-payment for TIPS Sales between customer and Vendor and inspections, rejections, or acceptance of such purchases shall be the exclusive respective obligations of Vendor/Customer, and disputes shall be handled in accordance with the terms of the underlying Supplemental Agreement(s) entered into between Vendor and Customer. Vendor acknowledges that TIPS is not a dealer, subcontractor, agent, or reseller of Vendor's goods and services and shall not be responsible for any claims arising out of alleged insufficiencies or defects in Vendor's goods and services, should any arise.

18. **Confidentiality of Vendor Data.** Vendor understands and agrees that by signing this Agreement, all Vendor Data is hereby released to TIPS, TIPS Members, and TIPS third-party administrators to effectuate Vendor's TIPS Contract except as provided for herein. The Parties agree that Vendor Data is accessible by all TIPS Members as if submitted directly to that TIPS Member Customer for purchase consideration. If Vendor otherwise considers any portion of Vendor's Data to be confidential and not subject to public disclosure pursuant to Chapter 552 Texas Gov't Code (the "Public Information Act") or other law(s) and orders, Vendor must have identified the claimed confidential materials through proper execution of the Confidentiality Claim Form which is required to be submitted as part of Vendor's proposal resulting in this Agreement and incorporated by reference. The Confidentiality Claim Form included in Vendor's proposal and incorporated herein by reference is the sole indicator of whether Vendor considers any Vendor Data confidential in the event TIPS receives a Public Information Request. If TIPS receives a request, any responsive documentation not deemed confidential by you in this manner will be automatically released. For Vendor Data deemed confidential by you in this manner, TIPS will follow procedures of controlling statute(s) regarding any claim of confidentiality and shall not be liable for any release of information required by law, including Attorney General determination and opinion. In the event that TIPS receives a written request for information pursuant to the Public Information Act that affects Vendor's interest in any information or data furnished to TIPS by Vendor, and TIPS

requests an opinion from the Attorney General, Vendor may, at its own option and expense, prepare comments and submit information directly to the Attorney General stating why the requested information is exempt from disclosure pursuant to the requirements of the Public Information Act. Vendor is solely responsible for submitting the memorandum brief and information to the Attorney General within the time period prescribed by the Public Information Act. Notwithstanding any other information provided in this solicitation or Vendor designation of certain Vendor Data as confidential or proprietary, Vendor's acceptance of this TIPS Vendor Agreement constitutes Vendor's consent to the disclosure of Vendor's Data, including any information deemed confidential or proprietary, to TIPS Members or as ordered by a Court or government agency, including without limitation the Texas Attorney General. Vendor agrees that TIPS shall not be responsible or liable for any use or distribution of information or documentation by TIPS Members or as required by law.

19. **Vendor's Authorized Resellers.** TIPS recognizes that many vendors operate in the open market through the use of resellers or dealers. For that reason, TIPS permits Vendor to authorize Authorized Resellers within its Vendor Portal and make TIPS Sales through the Authorized Reseller(s). Once authorized by Vendor in the Vendor Portal, the Authorized Reseller(s) may make TIPS sales to TIPS Members. However, all purchase documents must include: (1) Authorized Reseller's Name; (2) Vendor's Name, as known to TIPS, and; (3) Vendor's TIPS Contract Name and Number under which it is making the TIPS Sale. Either Vendor or Reseller may report the sale pursuant to the terms herein. However, Vendor agrees that it is legally responsible for all reporting and fee payment as described herein for TIPS Sales made by Authorized Resellers. The TIPS Administration Fee is assessed on the amount paid by the TIPS Member, not on the Vendor's cost or on the amount for which the Vendor sold the item to a dealer or Authorized Reseller. The Parties intend that Vendor shall be responsible and liable for TIPS Sales made by Vendor's Authorized Resellers. Vendor agrees that it is voluntarily authorizing this Authorized Reseller and in doing so, Vendor agrees that it is doing so at its own risk and agrees to protect, indemnify, and hold TIPS harmless in accordance with Sections 14-17 above related to Authorized Reseller TIPS Sales made pursuant to this Agreement or purporting to be made pursuant to this Agreement that may be asserted against Vendor whether rightfully brought or otherwise. The Parties further agree that it is no defense to Vendor's breach of this Agreement that an Authorized Reseller caused Vendor of breach this Agreement.

20. **Circumvention of TIPS Sales**. When a public entity initiates a purchase with Vendor, if the Member inquires verbally or in writing whether Vendor holds a TIPS Contract, it is the duty of the Vendor to verify whether the Member is seeking a TIPS purchase. Any request for quote, customer communication, or customer purchase initiated through or referencing a TIPS Contract shall be completed through TIPS pursuant to this Agreement. Any encouragement or participation by Vendor in circumventing a TIPS sale being completed may result in immediate termination of Vendor's TIPS Contract(s) for cause as well as preclusion from future TIPS opportunities at TIPS sole discretion.

21. **State of Texas Franchise Tax.** By signature hereon, Vendor hereby certifies that Vendor is not currently delinquent in the payment of any franchise taxes owed to the State of Texas under Chapter 171 of the Texas Tax Code.

22. **Termination.**

A) Termination for Convenience. TIPS may, by written notice to Vendor, terminate this Agreement for convenience, in whole or in part, at any time by giving thirty (30) days' written notice to Vendor of such termination, and specifying the effective date thereof.

B) Termination for Cause. If Vendor fails to materially perform pursuant to the terms of this Agreement, TIPS shall provide written notice to Vendor specifying the default. If Vendor does not cure such default within thirty (30) days, TIPS may terminate this Agreement, in whole or in part, for cause. If TIPS terminates this Agreement for cause, and it is later determined that the termination for cause was wrongful, the termination shall automatically be converted to and treated as a termination for convenience.

C) Vendor's Termination. If TIPS fails to materially perform pursuant to the terms of this Agreement, Vendor shall provide written notice to TIPS specifying the default ("Notice of Default"). If TIPS does not cure such default within thirty (30) days, Vendor may terminate this Agreement, in whole or in part, for cause. If TIPS terminates this Agreement for cause, and it is later determined that the termination for cause was wrongful, the termination shall automatically be converted to and treated as a termination for convenience.

D) Upon termination, all TIPS Sale orders previously accepted by Vendor shall be fulfilled and Vendor shall be paid for all TIPS Sales executed pursuant to the applicable terms. All TIPS Sale orders presented to Vendor but not fulfilled by Vendor, prior to the actual termination of this agreement shall be honored at the option of the TIPS Member. TIPS shall submit to Vendor an invoice for any outstanding TIPS Administration Fees and approved expenses and Vendor shall pay such fees and expenses within 30 calendar days of receipt of such valid

TIPS invoice. Vendor acknowledges and agrees that continued participation in TIPS is subject to TIPS' sole discretion and that any Vendor may be removed from the TIPS program at any time with or without cause. This termination clause does not affect TIPS Sales Supplemental Agreements pursuant to this term regarding termination and the Survival Clause term

E) Vendor hereby waives any and all claims for damages, including, but not limited, to consequential damages or lost profits, that might arise from TIPS' act of terminating this Agreement.

23. Survival Clause. It is the intent of the Parties that this Agreement and procurement method applies to any TIPS Sale made during the life of this Agreement even if made on or near the Contract Expiration Date as defined herein. Thus, all TIPS Sales, including but not limited to: leases, service agreements, license agreements, open purchase orders, warranties, and contracts, even if they extend months or years past the TIPS Contract Expiration Date, shall survive the expiration or termination of this Agreement subject to the terms and conditions of the Supplemental Agreement between Customer and Vendor or unless otherwise specified herein.

24. Audit Rights. Due to transparency statutes and public accountability requirements of TIPS and TIPS Members, Vendor shall at their sole expense, maintain documentation of all TIPS Sales for a period of three years from the time of the TIPS Sale. In order to ensure and confirm compliance with this agreement, TIPS shall have authority to conduct audits of Vendor's TIPS Pricing or TIPS Sales with thirty-days' notice unless the audit is ordered by a Court Order or by a Government Agency with authority to do so without said notice. Notwithstanding the foregoing, in the event that TIPS is made aware of any pricing being offered to eligible entities that is materially inconsistent with Vendor's TIPS Pricing, TIPS shall have the ability to conduct the audit internally or may engage a third- party auditing firm to investigate any possible non-compliant conduct or may terminate the Agreement according to the terms of this Agreement. In the event of an audit, the requested materials shall be reasonably provided in the time, format, and at the location acceptable to TIPS. TIPS agrees not to perform a random audit the TIPS transaction documentation more than once per calendar year, but reserves the right to audit for just cause or as required by any governmental agency or court with regulatory authority over TIPS or the TIPS Member. These audit rights shall survive termination of this Agreement for a period of one (1) year from the effective date of termination.

25. Conflicts of Interest. The Parties confirm that they have not offered, given, or accepted, nor intend to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, service to the other in connection with this Agreement. Vendor affirms that, to the best of Vendor's knowledge, this Agreement has been arrived at independently, and is awarded without collusion with anyone to obtain information or gain any favoritism that would in any way limit competition or give an unfair advantage over other vendors in the award of this Agreement. Vendor agrees that it has disclosed any necessary affiliations with Region 8 Education Service Center and the TIPS Department, if any, through the Conflict of Interest attachment provided in the solicitation resulting in this Agreement.

26. Volume of TIPS Sales. Nothing in this Agreement or any TIPS communication may be construed as a guarantee that TIPS or TIPS Members will submit any TIPS orders to Vendor at any time.

27. Compliance with the Law. The Parties agree to comply fully with all applicable federal, state, and local statutes, ordinances, rules, and regulations applicable to their entity in connection with the programs contemplated under this Agreement.

28. Severability. If any term(s) or provision(s) of this Agreement are held by a court of competent jurisdiction to be invalid, void, or unenforceable, then such term(s) or provision(s) shall be deemed restated to reflect the original intention of the Parties as nearly as possible in accordance with applicable law and the remainder of this Agreement, and the remainder of the provisions of this Agreement shall remain in full force and effect and shall in no way be affected, impaired or invalidated, unless such holding causes the obligations of the Parties hereto to be impossible to perform or shall render the terms of this Agreement to be inconsistent with the intent of the Parties hereto.

29. Force Majeure. If by reason of Force Majeure, either party hereto shall be rendered unable wholly or in part to carry out its obligations under this Agreement through no fault of its own then such party shall give notice and full particulars of Force Majeure in writing to the other party within a reasonable time after occurrence of the event or cause relied upon. Upon delivering such notice, the obligation of the affected party, so far as it is affected by such Force Majeure as described, shall be suspended during the continuance of the inability then claimed but for no longer period, and such party shall endeavor to remove or overcome such inability with all reasonable dispatch. In the event that Vendor's obligations are suspended by reason of Force Majeure, all TIPS Sales accepted prior to the Force Majeure event shall be the legal responsibility of Vendor and the terms of the TIPS Sale Supplemental Agreement shall control Vendor's failure to fulfill for a Force Majeure event.

30. Immunity. Vendor agrees that nothing in this Agreement shall be construed as a waiver of sovereign or government immunity; nor constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to Region 8 Education Service Center or its TIPS Department. The failure to enforce, or any delay in the enforcement of, any privileges, rights, defenses,

remedies, or immunities available to Region 8 Education Service Center or its TIPS Department under this Agreement or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel.

31. **Insurance Requirements.** Vendor agrees to maintain the following minimum insurance requirements for the duration of this Agreement. All policies held by Vendor to adhere to this term shall be written by a carrier with a financial size category of VII and at least a rating of "A-" by A.M. Best Key Rating Guide. The coverages and limits are to be considered minimum requirements and in no way limit the liability of the Vendor(s). Any immunity available to TIPS or TIPS Members shall not be used as a defense by the contractor's insurance policy. Only deductibles applicable to property damage are acceptable, unless proof of retention funds to cover said deductibles is provided. "Claims made" policies will not be accepted. Vendor's required minimum coverage shall not be suspended, voided, cancelled, non-renewed or reduced in coverage or in limits unless replaced by a policy that provides the minimum required coverage except after thirty (30) days prior written notice by certified mail, return receipt requested has been given to TIPS or the TIPS Member if a project or pending delivery of an order is ongoing. Upon request, certified copies of all insurance policies shall be furnished to the TIPS or the TIPS Member. Vendor agrees that when Vendor or its subcontractors are liable for any damages or claims, Vendor's policy, shall be primary over any other valid and collectible insurance carried by the Member or TIPS.

General Liability:	$1,000,000 each Occurrence/Aggregate
Automobile Liability:	$300,000 Includes owned, hired & non-owned
Workers' Compensation:	Statutory limits for the jurisdiction in which the Vendor performs under this Agreement. If Vendor performs in multiple jurisdictions, Vendor shall maintain the statutory limits for the jurisdiction with the greatest dollar policy limit requirement.
Umbrella Liability:	$1,000,000 each Occurrence/Aggregate

32. **Waiver.** No waiver of any single breach or multiple breaches of any provision of this Agreement shall be construed to be a waiver of any breach of any other provision. No delay in acting regarding any breach of any provision shall be construed to be a waiver of such breach.

33. **Binding Agreement.** This Agreement shall be binding and inure to the benefit of the Parties hereto and their respective heirs, legal successors, and assigns.

34. **Headings.** The paragraph headings contained in this Agreement are included solely for convenience of reference and shall not in any way affect the meaning or interpretation of any of the provisions of this Agreement.

35. **Choice of Law and Venue.** This Agreement shall be governed by, construed, and enforced in accordance with the laws of the State of Texas. Any proceeding, claim, action, or alternative dispute resolution arising out of or relating to this Agreement or involving TIPS shall be brought in a State Court of competent jurisdiction in Camp County, Texas, or if Federal Court is legally required, a Federal Court of competent jurisdiction in the Eastern District of Texas, and each of the Parties irrevocably submits to the exclusive jurisdiction of said court in any such proceeding, waives any objection it may now or hereafter have to venue or to convenience of forum, agrees that all claims in respect of the proceeding shall be heard and determined only in any such court, and agrees not to bring any proceeding arising out of or relating to this procurement process or any contract resulting from or and contemplated transaction in any other court. The Parties agree that either or both of them may file a copy of this paragraph with any court as written evidence of the knowing, voluntary and freely bargained for agreement between the Parties irrevocably to waive any objections to venue or to convenience of forum.

36. **Relationship of the Parties.** Nothing contained in this Agreement shall be construed to make one Party an agent of the other Party nor shall either party have any authority to bind the other in any respect, unless expressly authorized by the other party in writing. The Parties are independent contractors and nothing in this Agreement creates a relationship of employment, trust, agency or partnership between them.

37. **Assignment.** No assignment of this Agreement or of any duty or obligation of performance hereunder, shall be made in whole or in part by a Party hereto without the prior written consent of the other Party. Written consent of TIPS shall not be unreasonably withheld.

38. **Minimum Condition and Warranty Requirements for TIPS Sales.** All goods quoted or sold through a TIPS Sale shall be new unless clearly stated otherwise in writing. All new goods and services shall include the applicable manufacturers minimum standard warranty unless otherwise agreed to in the Supplemental Agreement.

39. **Minimum Customer Support Requirements for TIPS Sales.** Vendor shall provide timely and commercially reasonable support for TIPS Sales or as agreed to in the applicable Supplemental Agreement.

40. **Minimum Shipping Requirements for TIPS Sales.** Vendor shall ship, deliver, or provide ordered goods and services within a commercially reasonable time after acceptance of the order. If a delay in delivery is anticipated, Vendor shall notify the TIPS Member as to why delivery is delayed and provide an updated estimated time for completion. The TIPS Member may cancel the order if the delay is not commercially acceptable or not consistent with the Supplemental Agreement applicable to the order.

41. **Minimum Vendor License Requirements.** Vendor shall maintain, in current status, all federal, state, and local licenses, bonds and permits required for the operation of the business conducted by Vendor. Vendor shall remain fully informed of and in compliance with all ordinances and regulations pertaining to the lawful provision of goods or services under the TIPS Agreement. TIPS and TIPS Members reserve the right to stop work and/or cancel a TIPS Sale or terminate this or any TIPS Sale Supplemental Agreement involving Vendor if Vendor's license(s) required to perform under this Agreement or under the specific TIPS Sale have expired, lapsed, are suspended or terminated subject to a 30-day cure period unless prohibited by applicable statue or regulation.

42. **Minimum Vendor Legal Requirements.** Vendor shall remain aware of and comply with this Agreement and all local, state, and federal laws governing the sale of products/services offered by Vendor under this contract. Such applicable laws, ordinances, and policies must be complied with even if not specified herein.

43. **Minimum Site Requirements for TIPS Sales (*when applicable to TIPS Sale*).**

Cleanup: When performing work on site at a TIPS Member's property, Vendor shall clean up and remove all debris and rubbish resulting from their work as required or directed by the TIPS Member or as agreed by the parties. Upon completion of work, the premises shall be left in good repair and an orderly, neat, clean and unobstructed condition.

Preparation: Vendor shall not begin a project for which a TIPS Member has not prepared the site, unless Vendor does the preparation work at no cost, or until TIPS Member includes the cost of site preparation in the TIPS Sale Site preparation includes, but is not limited to: moving furniture, installing wiring for networks or power, and similar pre-installation requirements.

Registered Sex Offender Restrictions: For work to be performed at schools, Vendor agrees that no employee of Vendor or a subcontractor who has been adjudicated to be a registered sex offender will perform work at any time when students are, or reasonably expected to be, present unless otherwise agreed by the TIPS Member. Vendor agrees that a violation of this condition shall be considered a material breach and may result in the cancellation of the TIPS Sale at the TIPS Member's discretion. Vendor must identify any additional costs associated with compliance of this term. If no costs are specified, compliance with this term will be provided at no additional charge.

Safety Measures: Vendor shall take all reasonable precautions for the safety of employees on the worksite, and shall erect and properly maintain all necessary safeguards for protection of workers and the public. Vendor shall post warning signs against all hazards created by the operation and work in progress. Proper precautions shall be taken pursuant to state law and standard practices to protect workers, general public and existing structures from injury or damage.

Smoking: Persons working under Agreement shall adhere to the TIPS Member's or local smoking statutes, codes, ordinances, and policies.

44. **Payment for TIPS Sales.** TIPS Members may make payments for TIPS Sales directly to Vendor, Vendor's Authorized Reseller, or as otherwise agreed to in the applicable Supplemental Agreement after receipt of the invoice and in compliance with applicable payment statutes. Regardless of how payment is issued or received for a TIPS Sale, Vendor is responsible for all reporting and TIPS Administration Fee payment requirements as stated herein.

45. **Marketing.** Vendor agrees to allow TIPS to use their name and logo within the TIPS website, database, marketing materials, and advertisements unless Vendor negotiates this term to include a specific acceptable-use directive. Any use of TIPS' name and logo or any form of publicity, inclusive of press release, regarding this Agreement by Vendor must have prior approval from TIPS which will not be unreasonably withheld. Request may be made by email to tips@tips-usa.com. For marketing efforts directed to TIPS Members, Vendor must request and execute a separate Joint Marketing Disclaimer, at marketing@tips-usa.com, before TIPS can release contact information for TIPS Member entities for the purpose of marketing your TIPS contract(s). Vendor must adhere to strict Marketing Requirements once a disclaimer is executed. The Joint Marketing Disclaimer is a supplemental agreement specific to joint marketing efforts and has no effect on the terms of the TIPS Vendor Agreement. Vendor agrees that any images, photos, writing, audio, clip art, music, or any other intellectual property ("Property") or Vendor Data utilized, provided, or approved by Vendor during the course of the joint marketing efforts are either the exclusive property of Vendor, or Vendor has all necessary rights, license, and permissions to utilize said Property in the joint marketing efforts. Vendor agrees that they shall indemnify and hold harmless TIPS and its employees, officers, agents, representatives, contractors, assignees, designees, and TIPS Members from any and all claims, damages, and judgments

involving infringement of patent, copyright, trade secrets, trade or services marks, and any other intellectual or intangible property rights and/or claims arising from the Vendor's (including Vendor's officers', employees', agents', Authorized Resellers', subcontractors', licensees', or invitees') unauthorized use or distribution of Vendor Data and Property.

46. **Tax Exempt Status of TIPS Members.** Most TIPS Members are tax exempt entities and the laws and regulations applicable to the specific TIPS Member customer shall control.

47. **Automatic Renewal Limitation for TIPS Sales.** No TIPS Sale may incorporate an automatic renewal clause that exceeds month to month terms with which the TIPS Member must comply. All renewal terms incorporated into a TIPS Sale Supplemental Agreement shall only be valid and enforceable when Vendor received written confirmation of acceptance of the renewal term from the TIPS Member for the specific renewal term. The purpose of this clause is to avoid a TIPS Member inadvertently renewing an Agreement during a period in which the governing body of the TIPS Member has not properly appropriated and budgeted the funds to satisfy the Agreement renewal. Any TIPS Sale Supplemental Agreement containing an "Automatic Renewal" clause that conflicts with these terms is rendered void and unenforceable.

48. **Choice of Law Limitation for TIPS Sales.** Vendor agrees that if any "Choice of Law" provision is included in any TIPS Sale agreement/contract between Vendor and a TIPS Member, that clause must provide that the "Choice of Law" applicable to the TIPS Sale agreement/contract between Vendor and TIPS Member shall be the state where the TIPS Member operates unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a "Choice of Law" clause that conflicts with these terms is rendered void and unenforceable.

49. **Venue Limitation for TIPS Sales.** Vendor agrees that if any "Venue" provision is included in any TIPS Sale Agreement/contract between Vendor and a TIPS Member, that clause must provide that the "Venue" for any litigation or alternative dispute resolution shall be in the state and county where the TIPS Member operates unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a "Venue" clause that conflicts with these terms is rendered void and unenforceable.

50. **Indemnity Limitation for TIPS Sales.** Texas and other jurisdictions restrict the ability of governmental entities to indemnify others. Vendor agrees that if any "Indemnity" provision which requires the TIPS Member to indemnify Vendor is included in any TIPS sales agreement/contract between Vendor and a TIPS Member, that clause must either be stricken or qualified by including that such indemnity is only permitted, "to the extent permitted by the laws and constitution of [TIPS Member's State]" unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing an "Indemnity" clause that conflicts with these terms is rendered void and unenforceable.

51. **Arbitration Limitation for TIPS Sales.** Vendor agrees that if any "Arbitration" provision is included in any TIPS Sale agreement/contract between Vendor and a TIPS Member, that clause may not require that the arbitration is mandatory or binding. Vendor agrees that if any "Arbitration" provision is included in any TIPS Sale agreement/contract between Vendor and a TIPS Member, that clause provides for only voluntary and non-binding arbitration unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a "Arbitration" clause that conflicts with these terms is rendered void and unenforceable.

In Witness Whereof, the parties hereto, each acting under due and proper authority, have signed this Agreement.

TIPS VENDOR AGREEMENT SIGNATURE FORM

TIPS RFP 230504 Information Technology Equipment, Software, and Services

Vendor Name: U. S. TelePacific Corp DBA TPx Communications

Vendor Address: 303 Colorado Street, Suite 2075

City: Austin State: Texas Zip Code: 78701

Vendor Authorized Signatory Name: Tasha Wilson

Vendor Authorized Signatory Title: Manager of RFP & Bid Management

Vendor Authorized Signatory Phone: 858-200-2728

Vendor Authorized Signatory Email: formrequest@tpx.com

Vendor Authorized Signature: DocuSigned by: Tasha Wilson BD69F33AF0FC4D0... Date: 06/29/2023

(*The following is for TIPS completion only*)

TIPS Authorized Signatory Name: Dr. Fitts

TIPS Authorized Signatory Title: Executive Director

TIPS Authorized Signature: David Wayne Fitts Date: 7/10/2023

230504
TPx Communications
U.S. TelePacific Corp.
Supplier Response

Event Information

Number: 230504
Title: Information Technology, Equipment, Software, and Services
Type: Request for Proposal
Issue Date: 5/4/2023
Deadline: 5/25/2023 03:00 PM (CT)
Notes: This is a solicitation issued by The Interlocal Purchasing System (TIPS), a department of Texas Region 8 Education Service Center. It is an Indefinite Delivery, Indefinite Quantity ("IDIQ") solicitation. It will result in contracts that provide, through adoption/"piggyback" an indefinite quantity of supplies/services, during a fixed period of time, to TIPS public entity and qualifying non-profit "TIPS Members" throughout the nation. Thus, there is no specific project or scope of work to review. Rather this solicitation is issued as a prospective award for utilization when any TIPS Member needs the goods or services offered during the life of the agreement.

THIS IS NOT A REPLACEMENT CONTRACT. IF YOU CURRENTLY HOLD ANY TIPS CONTRACT TITLED "TECHNOLOGY SOLUTIONS, PRODUCTS, AND SERVICES", THERE IS NO NEED TO RESPOND HEREIN UNLESS YOU WISH TO MANAGE MULTIPLE TIPS CONTRACTS THAT HAVE THE SAME TERMS AND COVER THE SAME OFFERINGS. IF YOU HOLD A TIPS CONTRACT WITH A TITLE OTHER THAN "TECHNOLOGY SOLUTIONS, PRODUCTS, AND SERVICES", WHICH COVERS ALL OF YOUR TECHNOLOGY OFFERINGS AND YOU ARE SATISFIED WITH IT, THERE IS NO NEED TO RESPOND TO THIS

SOLICITATION UNLESS YOU PREFER TO HOLD BOTH CONTRACTS.

Contact Information

Address: Region 8 Education Service Center
4845 US Highway 271 North
Pittsburg, TX 75686
Phone: +1 (866) 839-8477
Email: bids@tips-usa.com

TPx Communications Information

Contact: Tasha Wilson
Address: 303 Colorado St., Suite 2075
Suite 2075
Austin, TX 78701
Phone: (877) 248-7087
Email: twilson@tpx.com
Web Address: https://www.tpx.com/

By submitting your response, you certify that you are authorized to represent and bind your company.

Tasha Wilson
Signature

formrequest@tpx.com
Email

Submitted at 5/18/2023 03:25:47 PM (CT)

Requested Attachments

Pricing Form 1

230504 Pricing Form 1.xlsx

Pricing Form 1 must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed as instructed, and uploaded to this location.

Alternate or Supplemental Pricing Documents

Catalog Pricing for TPx 2023-2024 Advisory Services.xlsx

Optional. If when completing Pricing Form 1 & Pricing Form 2 you direct TIPS to view additional, alternate, or supplemental pricing documentation, you may upload that documentation.

Vendor Agreement

230504 Vendor Agreement Signature Form signed.pdf

The Vendor Agreement must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, Vendor Name placed in the line provided at the top, and uploaded to this location. If Vendor has proposed deviations to the Vendor Agreement, Vendor may assert so in the Attribute Questions and those shall be addressed during evaluation.

Reference Form

230504 Reference Form.xlsx

The Reference Form must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed, and uploaded to this location. The Reference Form must be uploaded in Excel format.

Required Confidentiality Claim Form

230504 Required Confidentiality Claim Form signed.pdf

The Required Confidentiality Claim Form must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed, and uploaded to this location. This is the only way for Vendor to assert confidentiality of any information submitted.

Conflict of Interest Questionnaire - Form CIQ

No response

Do not upload this form unless you have a reportable conflict with TIPS. There is an Attribute entitled “Conflict of Interest Questionnaire Requirement” immediately followed by an Attribute entitled “Conflict of Interest Questionnaire Requirement – Form CIQ – Continued.” Properly respond to those Attributes and only upload this form if applicable/instructed. If upload is required based on your response to those Attributes, the Conflict of Interest Questionnaire – Form CIQ must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed, and uploaded at this location.

Vendor’s Warranties, Terms, and Conditions (Supplemental Vendor Information Only)

TPx-Terms-and-Conditions-to-the-Agreement-v030121.pdf

Optional. If Vendor would like to display any standard warranties, terms, or conditions which are often applicable to their offerings for TIPS and TIPS Member Customer consideration, Vendor may upload those at this location. These supplemental documents shall not be considered part of the TIPS Contract. Rather, they are Vendor Supplemental Information for marketing and informational purposes only.

Supplemental Vendor Information (Supplemental Vendor Information Only) Product Datasheet.pdf

Optional. If Vendor would like to display or include any brochures, promotional documents, marketing materials, or other Vendor Information for TIPS and TIPS Member Customer consideration, Vendor may upload those at this location.
These supplemental documents shall not be considered part of the TIPS Contract. Rather, they are Vendor Supplemental Information for marketing and informational purposes only.

Disclosure of Lobbying Activities - Standard Form - LLL *No response*

Do not upload this form unless Vendor has reportable lobbying activities. There are Attributes entitled, “2 CFR Part 200 or Federal Provision - Byrd Anti-Lobbying Amendment – Continued.” Properly respond to those Attributes and only upload this form if applicable/instructed. If upload is required based on your response to those Attributes, the Disclosure of Lobbying Activities – Standard Form - LLL must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed, and uploaded to this location.

Current Form W-9 U.S. TelePacific W-9 signed.pdf

Vendor must upload their current IRS Tax Form W-9. The legal name, EIN, and d/b/a's listed should match the information provided herein exactly. This form will be utilized by TIPS to properly identify your entity.

Certificates & Licenses (Supplemental Vendor Information Only) *No response*

Optional. If Vendor would like to display any applicable certificates or licenses (including HUB certificates) for TIPS and TIPS Member Customer consideration, Vendor may upload those at this location. These supplemental documents shall not be considered part of the TIPS Contract. Rather, they are Vendor Supplemental Information for marketing and informational purposes only.

Pricing Form 2 230504 Pricing Form 2.xlsx

Pricing Form 2 must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed as instructed, and uploaded to this location.

Vendor Logo (Supplemental Vendor Information Only) logo_TPx_CMYK.ai.pdf

Optional. If Vendor desires that their logo be displayed on their public TIPS profile for TIPS and TIPS Member viewing, Vendor may upload that logo at this location. These supplemental documents shall not be considered part of the TIPS Contract. Rather, they are Vendor Supplemental Information for marketing and informational purposes only.

Vendor Agreement Signature Form 230504 Vendor Agreement Signature Form.pdf

The Vendor Agreement Signature Form must be downloaded from the “Attachments” section of the IonWave eBid System, reviewed, properly completed, and uploaded to this location. If Vendor has proposed deviations to the Vendor Agreement, Vendor may leave the signature line of this page blank and assert so in the Attribute Questions and those shall be addressed during evaluation.

Bid Attributes

1	**Disadvantaged/Minority/Women Business & Federal HUBZone** Some participating public entities are required to seek Disadvantaged/Minority/Women Business & Federal HUBZone ("D/M/WBE/Federal HUBZone") vendors. Does Vendor certify that their entity is a D/M/WBE/Federal HUBZone vendor? If you respond "Yes," you must upload current certification proof in the appropriate "Response Attachments" location. NO

2 Historically Underutilized Business (HUB)

Some participating public entities are required to seek Historically Underutilized Business (HUB) vendors as defined by the Texas Comptroller of Public Accounts Statewide HUB Program. Does Vendor certify that their entity is a HUB vendor?

If you respond "Yes," you must upload current certification proof in the appropriate "Response Attachments" location.

No

3 National Coverage

Can the Vendor provide its proposed goods and services to all 50 US States?

Yes

4 States Served

If Vendor answered "No" to the question entitled "National Coverage," please list all states where vendor can provide the goods and services proposed directly below. Your response may dictate which potential TIPS Member customers consider purchasing your offerings.

No response

5 Description of Vendor Entity and Vendor's Goods & Services

If awarded, this description of Vendor and Vendor's goods and services will appear on the TIPS website for customer/public viewing.

TPx Communications
Since 1998, TPx has helped businesses navigate a complicated and evolving IT landscape. Our passion is IT and we're committed to making IT easy for our customers. With a full suite of managed IT, cybersecurity, network connectivity and unified communications solutions, TPx helps businesses solve their IT challenges.

6 Primary Contact Name

Please identify the individual who will be primarily responsible for all TIPS matters and inquiries for the duration of the contract.

Tasha Wilson

7 Primary Contact Title

Primary Contact Title

Manager of RFP & Bid Management

8 Primary Contact Email

Please enter a valid email address that will definitely reach the Primary Contact.

formrequest@tpx.com

9 Primary Contact Phone

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

Please provide the accurate and current phone number where the individual who will be primarily responsible for all TIPS matters and inquiries for the duration of the contract can be reached directly.

8582002728

10 **Primary Contact Fax**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

No response

11 **Primary Contact Mobile**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

No response

12 **Secondary Contact Name**

Please identify the individual who will be secondarily responsible for all TIPS matters and inquiries for the duration of the contract.

Cindy Watts

13 **Secondary Contact Title**

Secondary Contact Title

Vice President of Sales Operations

14 **Secondary Contact Email**

Please enter a valid email address that will definitely reach the Secondary Contact.

clwatts@tpx.com

15 **Secondary Contact Phone**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

Please provide the accurate and current phone number where the individual who will be secondarily responsible for all TIPS matters and inquiries for the duration of the contract can be reached directly.

3032685428

16 **Secondary Contact Fax**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

No response

17 **Secondary Contact Mobile**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

No response

18 **Administration Fee Contact Name**

Please identify the individual who will be responsible for all payment, accounting, and other matters related to Vendor's TIPS Administration Fee due to TIPS for the duration of the contract.

Ryan Browne

19 **Administration Fee Contact Email**

Please enter a valid email address that will definitely reach the Administration Fee Contact.

vrcommissions@tpx.com

20 **Administration Fee Contact Phone**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

2132234876

21 **Purchase Order and Sales Contact Name**

Please identify the individual who will be responsible for receiving and processing purchase orders and sales under the TIPS Contract.

Tasha Wilson

22 **Purchase Order and Sales Contact Email**

Please enter a valid email address that will definitely reach the Purchase Order and Sales Contact.

formrequest@tpx.com

23 **Purchase Order and Sales Contact Phone**

Numbers only, no symbols or spaces (Ex. 8668398477). The system will auto-populate your entry with commas once submitted which is appropriate and expected (Ex. 8,668,398,477).

8582002728

24 **Company Website**

Company Website (Format - www.company.com)

www.tpx.com

25 **Entity D/B/A's and Assumed Names**

You must confirm that you are responding to this solicitation under your legal entity name. Go now to your Supplier Profile in this eBid System and confirm that your profile reflects your "Legal Name" as it is listed on your W9.

In this question, please identify all of your entity's assumed names and D/B/A's. Please note that you will be identified publicly by the Legal Name under which you respond to this solicitation unless you organize otherwise with TIPS after award.

TPx Communications

26 **Primary Address**

Primary Address

303 Colorado St, Suite 2075

27 **Primary Address City**

Primary Address City

Austin

28 **Primary Address State**

Primary Address State (2 Digit Abbreviation)

TX

29 **Primary Address Zip**

Primary Address Zip

78701

30 **Search Words Identifying Vendor**

Please list all search words and phrases to be included in the TIPS database related to your entity. ***Do not*** list words which are not associated with the bid category/scope (See bid title for general scope). This will help users find you through the TIPS website search function. You may include product names, manufacturers, specialized services, and other words associated with the scope of this solicitation.

SD-WAN, Networking, Velocloud, Meraki, Cisco, Fortinet, Fortigate, Endpoint Management, Endpoint Security, Servers, Workstations, Endpoint Detection and Response, Inbox Detection and Response, Security Advisory Services, Security Awareness Training, User Security, Business Cybersecurity, Firewall Access Points, Switches, Unified Communications, Cisco Webex, Polycom phones, Cisco phones, Algo phones, Smartvoice, VOIP service, Microsoft Office 365, Data Center Colocation, Backup and Disaster Recovery Solutions, Datto, 4G/5G Access, Internet Connectivity, Calling, Meetings, Messaging, Call Center Solutions, Microsoft Teams Calling, Business Phone Systems & Headsets

31 **Certification of Vendor Residency (Required by the State of Texas)**

Does Vendor's parent company or majority owner:

(A) have its principal place of business in Texas; ***or*** (B) employ at least 500 persons in Texas?

Texas Education Code Section 44.031 requires that this information be considered in evaluation for certain contracts. However, Vendor response does not affect points, scoring, or potential award.

Yes

32 **Vendor's Principal Place of Business (City)**

In what city is Vendor's principal place of business located?

Austin

33 **Vendor's Principal Place of Business (State)**

In what state is Vendor's principal place of business located?

Texas

34 **Vendor's Years in Business**

How many years has the business submitting this proposal been operating in its current capacity and field of work?

24

35 **Certification Regarding Entire TIPS Agreement**

Vendor agrees that, if awarded, Vendor's final TIPS Contract will consist of the provisions set forth in the finalized TIPS Vendor Agreement, Vendor's responses to these attribute questions, and: (1) The TIPS solicitation document resulting in this Agreement; (2) Any addenda or clarifications issued in relation to the TIPS solicitation; (3) All solicitation information provided to Vendor by TIPS through the TIPS eBid System; (3) Vendor's entire proposal response to the TIPS solicitation including all accepted required attachments, acknowledged notices and certifications, accepted negotiated terms, accepted pricing, accepted responses to questions, and accepted written clarifications of Vendor's proposal, and; any properly included attachments to the TIPS Contract.

Does Vendor agree?

Yes

36 **Minimum Percentage Discount Offered to TIPS Members on all Goods and Services (READ CAREFULLY)**

Please read thoroughly and carefully as an error on your response can render your contract award unusable.

TIPS Members often turn to TIPS Contracts for ease of use and to receive discounted pricing.

What is the minimum percentage discount that you can offer TIPS Members off of all goods and service pricing (whether offered through Pricing Form 1, Pricing Form 2, or in another accepted format) that you offer? Only limited goods/services specifically identified and excluded from this discount in Vendor's original proposal may be excluded from this discount.

Vendor must respond with a percentage from 0%-100%. The percentage discount that you input below will be applied to your "Catalog Pricing", as defined in the solicitation, for all TIPS Sales made during the life of the contract. You cannot alter this percentage discount once the solicitation legally closes. You will always be required to discount every TIPS Sale by the percentage included below with the exception of limited goods/services specifically identified and excluded from this discount in Vendor's original proposal. If you add goods or services to your "Catalog Pricing" during the life of the contract, you will be required to sell those new items with this discount applied.

Example: In this example, you enter a 10% minimum percentage discount below. In year-one of your TIPS Contract, your published "Catalog Pricing" (website/store/published pricing) for "Tablet A" is $100 and for "Tablet Set-Up Service" is $100. In this example, you must sell those items under the TIPS Contract at the proposed 10% discounted price of: "Tablet A" - $90, "Tablet Set-Up Service" - $90. In year two of your TIPS Contract, you update your "Catalog Pricing" with the market. You add "Tablet B" to your "Catalog Pricing" for $200 and have increased the price of "Tablet A" to $110 and the price of "Tablet Set-Up Service" to $110. In this example, after the "Catalog Pricing" update, you must still sell those items under the TIPS Contract at the proposed 10% discounted price of: "Tablet A" - $99, "Tablet Set-Up Service" - $99, and "Tablet B" - $180.00.

With the exception of limited goods/services specifically identified and excluded from this discount in Vendor's original proposal, if you cannot honor the discount on all goods and items now included or which may be added in the future with certainty, then you should offer a lesser discount percentage below.

What is the minimum percentage discount that you can offer TIPS Members off of all goods and service pricing (whether offered through Pricing Form 1, Pricing Form 2, or in another accepted format) that you offer?

1%

37 **Honoring Vendor's Minimum Percentage Discount**

Vendor is asked in these Attribute Questions to provide a Minimum Percentage Discount offered to TIPS Members on all goods and services sold under the TIPS Contract. Points will be assigned for your response and scoring of your proposal will be affected. A "YES" answer will be awarded the maximum 10 points and a "NO" answer will be awarded 0 points.

Does Vendor agree to honor the Minimum Percentage Discount off of their TIPS "Catalog Pricing" that Vendor proposed for all TIPS Sales made for the duration of the TIPS Contract?

Yes

38 **Volume and Additional Discounts**

In addition to the Minimum Percentage Discount proposed herein, does Vendor ever expect and intend to offer additional, greater, or volume discounts to TIPS Members?

Point(s) may be assigned for your response in the category of "Pricing" during scoring and evaluation.

Yes

39 **"Catalog Pricing" and Pricing Requirements**

This is a requirement of the TIPS Contract and is non-negotiable.

In this solicitation and resulting contract, "Catalog Pricing" shall be defined as:

"The then available list of goods or services, in the most current listing regardless of date, that takes the form of a catalog, price list, price schedule, shelf-price or other viewable format that:

A. is regularly maintained by the manufacturer or Vendor of an item; and

B. is either published or otherwise available for review by TIPS or a customer during the purchase process;

C. to which the Minimum Percentage Discount proposed by the proposing Vendor may be applied.

If awarded on this TIPS Contract, for the duration of the contract, Vendor agrees to provide, upon request, their then current "Catalog Pricing." Or, in limited circumstances where Vendor has proposed the Percentage Mark-Up method of pricing in this proposal, proof of Vendor's "cost" may be accepted by TIPS in place of catalog pricing.

YES

40

EXCEPTIONS & DEVIATIONS TO TIPS STANDARD TERMS AND CONDITIONS

Vendor agrees that, if awarded, Vendor's final TIPS Contract will consist of the provisions set forth in the finalized TIPS Vendor Agreement, Vendor's responses to these attribute questions, and: (1) The TIPS solicitation document resulting in this Agreement; (2) Any addenda or clarifications issued in relation to the TIPS solicitation; (3) All solicitation information provided to Vendor by TIPS through the TIPS eBid System; (3) Vendor's entire proposal response to the TIPS solicitation including all accepted required attachments, acknowledged notices and certifications, accepted negotiated terms, accepted pricing, accepted responses to questions, and accepted written clarifications of Vendor's proposal, and; any properly included attachments to the TIPS Contract. In the event of conflict between the terms of the finalized Vendor Agreement and one of the incorporated documents the terms and conditions which are in the best interest of governmental/qualifying non-profit TIPS Members shall control at TIPS sole discretion.

If Vendor responds, "No, Vendor does not agree" to this Attribute, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. This is the only proper way to submit proposed deviations for TIPS consideration. TIPS reserves the right to accept, decline, or modify Vendor's requested negotiated terms. For this reason, answering "No, Vendor does not agree" may ultimately delay or prevent award.

Does Vendor agree with TIPS standard terms and conditions as presented in the TIPS solicitation document (RFP, RCSP, RFQ, or other) and the TIPS Vendor Agreement document?

No

41

TIPS Sales Reporting Requirements

This is a requirement of the TIPS Contract and is non-negotiable.

By submitting this proposal, Vendor certifies that Vendor will properly report all TIPS sales. With the exception of TIPS Automated Vendors, who have signed an exclusive agreement with TIPS regarding reporting, all TIPS Sales must be reported to TIPS by either:

(1) Emailing the purchase order or similar purchase document (with Vendor's Name, as known to TIPS, and the TIPS Contract Name and Number included) to TIPS at tipspo@tips-usa.com with "Confirmation Only" in the subject line of the email within three business days of Vendor's acceptance of the order, or;

(2) Within 3 business days of the order being accepted by Vendor, Vendor must login to the TIPS Vendor Portal and successfully self-report all necessary sale information within the Vendor Portal and confirm that it shows up accurately on your current Vendor Portal statement.

No other method of reporting is acceptable unless agreed to by the Parties in writing. Failure to report all sales pursuant to this provision may result in immediate cancellation of Vendor's TIPS Contract(s) for cause at TIPS' sole discretion.

42	**TIPS Administration Fee Requirement and Acknowledgment** **This is a requirement of the TIPS Contract and is non-negotiable.** The collection of fees by TIPS, a government entity, for performance of these procurement services is required pursuant to Texas Government Code Section 791.011 et. seq. The TIPS Administration Fee is the amount legally owed by Vendor to TIPS for TIPS Sales made by Vendor. The TIPS Administration Fee amount is typically a set percentage of each TIPS Sale legally due to TIPS, but the exact TIPS Administration Fee for this Contract is published in the corresponding RFP or RCSP document. TIPS Administration Fees are due to TIPS immediately upon Vendor's receipt of payment, including partial payment, for a TIPS Sale. By submitting a proposal, Vendor agrees that it has read, understands, and agrees to the published TIPS Administration Fee amount, calculation, and payment requirements. By submitting a proposal Vendor further confirms that all TIPS Pricing includes the TIPS Administration Fee and Vendor will not show adding the TIPS Administration Fee as a charge or line-item in any TIPS Sale.
43	**TIPS Member Access to Vendor Proposal & Documentation** **This is a requirement of the TIPS Contract and is non-negotiable.** Notwithstanding any other information provided in this solicitation or Vendor designation of certain documentation as confidential or proprietary, Vendor's submission of this proposal constitutes Vendor's express consent to the disclosure of Vendor's comprehensive proposal, including any information deemed confidential or proprietary, **to TIPS Members**. The proposing Vendor agrees that TIPS shall not be responsible or liable for any use or distribution of information or documentation to TIPS Members or by TIPS Members. By submitting this proposal, Vendor certifies the foregoing.
44	**Non-Collusive Bidding Certificate** **This is a requirement of the TIPS Contract and is non-negotiable.** By submission of this proposal, the Vendor certifies that: 1) This proposal has been independently arrived at without collusion with any other entity, bidder, or with any competitor; 2) This proposal has not been knowingly disclosed and will not be knowingly disclosed, prior to the opening of bids, or proposals for this project, to any other bidder, competitor or potential competitor: 3) No attempt has been or will be made to induce any other person, partnership or corporation to modify, submit, or not to submit a bid or proposal; and 4) The person signing this bid or proposal certifies that they are duly authorized to execute this proposal/contract on behalf of Vendor and they have fully informed themselves regarding the accuracy of the statements contained in this certification, and under the penalties being applicable to the bidder as well as to the person signing in its behalf;

45	**Antitrust Certification Statements (Tex. Government Code § 2155.005)** **This is a requirement of the TIPS Contract and is non-negotiable.** By submission of this bid or proposal, Vendor certifies under penalty of perjury of the laws of the State of Texas that: (1) I am duly authorized to execute this proposal/contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Vendor) identified herein; (2) In connection with this proposal, neither I nor any representative of Vendor has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15; (3) In connection with this proposal, neither I nor any representative of the Vendor has violated any federal antitrust law; (4) Neither I nor any representative of Vendor has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.
46	**Limitation on Out-of-State Litigation - Texas Business and Commerce Code § 272** **This is a requirement of the TIPS Contract and is non-negotiable.** Texas Business and Commerce Code § 272 prohibits a construction contract, or an agreement collateral to or affecting the construction contract, from containing a provision making the contract or agreement, or any conflict arising under the contract or agreement, subject to another state's law, litigation in the courts of another state, or arbitration in another state. If included in Texas construction contracts, such provisions are voidable by a party obligated by the contract or agreement to perform the work. By submission of this proposal, Vendor acknowledges this law and ***if Vendor enters into a construction contract with a Texas TIPS Member*** under this procurement, Vendor certifies compliance.
47	**Required Confidentiality Claim Form** **This is a requirement of the TIPS Contract and is non-negotiable.** TIPS provides the required TIPS Confidentiality Claim Form in the "Attachments" section of this solicitation. Vendor must execute this form by either signing and waiving any confidentiality claim, or designating portions of Vendor's proposal confidential. If Vendor considers any portion of Vendor's proposal to be confidential and not subject to public disclosure pursuant to Chapter 552 Texas Gov't Code or other law(s) and orders, Vendor must have identified the claimed confidential materials through proper execution of the Confidentiality Claim Form. If TIPS receives a public information act or similar request, any responsive documentation not deemed confidential by you in this manner will be automatically released. For Vendor documents deemed confidential by you in this manner, TIPS will follow procedures of controlling statute(s) regarding any claim of confidentiality and shall not be liable for any release of information required by law, including Attorney General determination and opinion. Notwithstanding any other Vendor designation of Vendor's proposal as confidential or proprietary, Vendor's submission of this proposal constitutes Vendor's agreement that proper execution of the required TIPS Confidentiality Claim Form is the only way to assert any portion of Vendor's proposal as confidential.

48 **Non-Discrimination Statement and Certification**

This is a requirement of the TIPS Contract and is non-negotiable.

In accordance with Federal civil rights law, all U.S. Departments, including but not limited to the USDA, USDE, FEMA, are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by federal funds (not all bases apply to all programs).

Vendor certifies that Vendor will comply with applicable Non-Discrimination and Equal Opportunity provisions set forth in TIPS Member Customers' policies and other regulations at the local, state, and federal levels of governments.

☑ Yes, I certify (Yes)

49 **Limitation of Vendor Indemnification and Similar Clauses**

This is a requirement of the TIPS Contract and is non-negotiable.

TIPS, a department of Region 8 Education Service Center, a political subdivision, and local government entity of the State of Texas, is prohibited from indemnifying third-parties (pursuant to the Article 3, Section 52 of the Texas Constitution) except as otherwise specifically provided for by law or as ordered by a court of competent jurisdiction. Article 3, Section 52 of the Texas Constitution states that "no debt shall be created by or on behalf of the State … " and the Texas Attorney General has opined that a contractually imposed obligation of indemnity creates a "debt" in the constitutional sense. Tex. Att'y Gen. Op. No. MW-475 (1982). Thus, contract clauses which require TIPS to indemnify Vendor, pay liquidated damages, pay attorney's fees, waive Vendor's liability, or waive any applicable statute of limitations must be deleted or qualified with "to the extent permitted by the Constitution and Laws of the State of Texas."

Does Vendor agree?

☑ Yes, I Agree (Yes)

50 **Alternative Dispute Resolution Limitations**

This is a requirement of the TIPS Contract and is non-negotiable.

TIPS, a department of Region 8 Education Service Center, a political subdivision, and local government entity of the State of Texas, does not agree to binding arbitration as a remedy to dispute and no such provision shall be permitted in this Agreement with TIPS. Vendor agrees that any claim arising out of or related to this Agreement, except those specifically and expressly waived or negotiated within this Agreement, may be subject to non-binding mediation at the request of either party to be conducted by a mutually agreed upon mediator as prerequisite to the filing of any lawsuit arising out of or related to this Agreement. Mediation shall be held in either Camp or Titus County, Texas. Agreements reached in mediation will be subject to the approval by the Region 8 ESC's Board of Directors, authorized signature of the Parties if approved by the Board of Directors, and, once approved by the Board of Directors and properly signed, shall thereafter be enforceable as provided by the laws of the State of Texas.

Does Vendor agree?

Yes

5 1 No Waiver of TIPS Immunity

This is a requirement of the TIPS Contract and is non-negotiable.

Vendor agrees that nothing in this Agreement shall be construed as a waiver of sovereign or government immunity; nor constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to Region 8 Education Service Center or its TIPS Department. The failure to enforce, or any delay in the enforcement, of any privileges, rights, defenses, remedies, or immunities available to Region 8 Education Service Center or its TIPS Department under this Agreement or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel.

Does Vendor agree?

☑ Yes, Vendor agrees (Yes)

5 2 Payment Terms and Funding Out Clause

This is a requirement of the TIPS Contract and is non-negotiable.

Vendor agrees that TIPS and TIPS Members shall not be liable for interest or late-payment fees on past-due balances at a rate higher than permitted by the laws or regulations of the jurisdiction of the TIPS Member.

Funding-Out Clause: Vendor agrees to abide by the applicable laws and regulations, including but not limited to Texas Local Government Code § 271.903, or any other statutory or regulatory limitation of the jurisdiction of any TIPS Member, which requires that contracts approved by TIPS or a TIPS Member are subject to the budgeting and appropriation of currently available funds by the entity or its governing body.

Does Vendor agree?

☑ Yes, Vendor agrees (Yes)

5 3 Certification Regarding Prohibition of Certain Terrorist Organizations (Tex. Gov. Code 2270)

Vendor certifies that Vendor is not a company identified on the Texas Comptroller's list of companies known to have contracts with, or provide supplies or services to, a foreign organization designated as a Foreign Terrorist Organization by the U.S. Secretary of State.

Does Vendor certify?

Yes

5 4 Certification Regarding Prohibition of Boycotting Israel (Tex. Gov. Code 2271)

If (a) Vendor is not a sole proprietorship; (b) Vendor has ten (10) or more full-time employees; and (c) this Agreement or any agreement with a TIPS Member under this procurement has value of $100,000 or more, the following certification shall apply; otherwise, this certification is not required. Vendor certifies, where applicable, that neither the Vendor, nor any affiliate, subsidiary, or parent company of Vendor, if any, boycotts Israel, and Vendor agrees that Vendor and Vendor Companies will not boycott Israel during the term of this Agreement. For purposes of this Agreement, the term "boycott" shall mean and include refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory but does not include an action made for ordinary business purposes.

When applicable, does Vendor certify?

Yes

55	**Certification Regarding Prohibition of Contracts with Certain Foreign-Owned Companies (Tex. Gov. Code 2274)** Certain public entities are prohibited from entering into a contract or other agreement relating to critical infrastructure that would grant Vendor direct or remote access to or control of critical infrastructure in this state, excluding access specifically allowed by a customer for product warranty and support purposes. Vendor certifies that neither it nor its parent company nor any affiliate of Vendor or its parent company, is (1) owned by or the majority of stock or other ownership interest of the company is held or controlled by individuals who are citizens of China, Iran, North Korea, Russia, or a designated country; (2) a company or other entity, including governmental entity, that is owned or controlled by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or a designated country; or (3) headquartered in China, Iran, North Korea, Russia, or a designated country. For purposes of this certification, “critical infrastructure” means “a communication infrastructure system, cybersecurity system, electric grid, hazardous waste treatment system, or water treatment facility.” Vendor certifies that Vendor will not grant direct or remote access to or control of critical infrastructure, except for product warranty and support purposes, to prohibited individuals, companies, or entities, including governmental entities, owned, controlled, or headquartered in China, Iran, North Korea, Russia, or a designated country, as determined by the Governor. When applicable, does Vendor certify? Yes

56	**Certification Regarding Prohibition of Discrimination Against Firearm and Ammunition Industries (Tex. Gov. Code 2274)** If (a) Vendor is not a sole proprietorship; (b) Vendor has at least ten (10) full-time employees; and (c) this Agreement or any Supplemental Agreement with certain public entities have a value of at least $100,000 that is paid wholly or partly from public funds; (d) the Agreement is not excepted under Tex. Gov. Code 2274 and (e) the purchasing public entity has determined that Vendor is not a sole-source provider or the purchasing public entity has not received any bids from a company that is able to provide this written verification, the following certification shall apply; otherwise, this certification is not required. Vendor certifies that Vendor, or association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including a wholly owned subsidiary, majority-owned subsidiary parent company, or affiliate of these entities or associations, that exists to make a profit, does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and will not discriminate during the term of this contract against a firearm entity or firearm trade association. For purposes of this Agreement, “discriminate against a firearm entity or firearm trade association” shall mean, with respect to the entity or association, to: “(1) refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (2) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (3) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association.” “Discrimination against a firearm entity or firearm trade association” does not include: “(1) the established policies of a merchant, retail seller, or platform that restrict or prohibit the listing or selling of ammunition, firearms, or firearm accessories; and (2) a company’s refusal to engage in the trade of any goods or services, decision to refrain from continuing an existing business relationship, or decision to terminate an existing business relationship to comply with federal, state, or local law, policy, or regulations or a directive by a regulatory agency, or for any traditional business reason that is specific to the customer or potential customer and not based solely on an entity’s or association’s status as a firearm entity or firearm trade association.” When applicable, does Vendor certify? Yes

57	**Certification Regarding Termination of Contract for Non-Compliance (Tex. Gov. Code 552.374)** If Vendor is not a governmental body and (a) this Agreement or any Supplemental Agreement with a public entity has a stated expenditure of at least $1 million in public funds for the purchase of goods or services by certain public entities; or (b) this Agreement or any Supplemental Agreement results in the expenditure of at least $1 million in public funds for the purchase of goods or services by certain public entities in their fiscal year, the following certification shall apply; otherwise, this certification is not required. As required by Tex. Gov. Code 552.374, the following statement is included in the RFP and the Agreement (unless the Agreement is (1) related to the purchase or underwriting of a public security; (2) is or may be used as collateral on a loan; or (3) proceeds from which are used to pay debt service of a public security of loan): “The requirements of Subchapter J, Chapter 552, Government Code, may apply to this solicitation and Agreement and the Vendor agrees that this Agreement and any applicable Supplemental Agreement can be terminated if Vendor knowingly or intentionally fails to comply with a requirement of that subchapter.” Pursuant to Chapter 552 of the Texas Government Code, Vendor certifies that Vendor shall: (1) preserve all contracting information related to this Agreement as provided by the records retention requirements applicable to TIPS or the purchasing TIPS Member for the duration of the Agreement; (2) promptly provide to TIPS or the purchasing TIPS Member any contracting information related to the Agreement that is in the custody or possession of Vendor on request of TIPS or the purchasing TIPS Member; and (3) on completion of the Agreement, either (a) provide at no cost to TIPS or the purchasing TIPS Member all contracting information related to the Agreement that is in the custody or possession of Vendor, or (b) preserve the contracting information related to the Agreement as provided by the records retention requirements applicable to TIPS or the purchasing TIPS Member. When applicable, does Vendor certify? Yes

58 **Certification Regarding Prohibition of Boycotting Certain Energy Companies (Tex. Gov. Code 2274)**

If (a) Vendor is not a sole proprietorship; (b) Vendor has ten (10) or more full-time employees; and (c) this Agreement or any Supplemental Agreement with certain public entities has a value of $100,000 or more that is to be paid wholly or partly from public funds, the following certification shall apply; otherwise, this certification is not required.

Vendor certifies that Vendor, or any wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate of these entities or business associations, if any, do not boycott energy companies and will not boycott energy companies during the term of the Agreement or any applicable Supplemental Agreement.

For purposes of this certification the term “company” shall mean an organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, that exists to make a profit.

The term “boycott energy company” shall mean “without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company (a) engages in the exploration, production, utilization, transportation, sale, or manufacturing of fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law, or (b) does business with a company described by paragraph (a).” (See Tex. Gov. Code 809.001).

When applicable, does Vendor certify?

Yes

59 **Felony Conviction Notice - Texas Education Code 44.034**

Texas Education Code, Section 44.034, Notification of Criminal History, Subsection (a), states, "a person or business entity that enters into a contract with a school district must give advance notice to the district if the person or an owner or operator of the business entity has been convicted of a felony. The notice must include a general description of the conduct resulting in the conviction of a felony.”

Subsection (b) states, "a school district may terminate a contract with a person or business entity if the district determines that the person or business entity failed to give notice as required by Subsection (a) or misrepresented the conduct resulting in the conviction. The district must compensate the person or business entity for services performed before the termination of the contract.”

Subsection (c) states, "This section does not apply to a publicly held corporation.

Vendor certifies one of the following:

A. My firm is a publicly held corporation; therefore, this reporting requirement is not applicable, or;

B. My firm is not owned nor operated by anyone who has been convicted of a felony, or;

C. My firm is owned or operated by the following individual(s) who has/have been convicted of a felony.

If Vendor responds with Option (C), Vendor is required to provide information in the next attribute.

B. My firm is not owned nor operated by felon.

60 **Felony Conviction Notice - Texas Education Code 44.034 - Continued**

If Vendor selected Option (C) in the previous attribute, Vendor must provide the following information herein:

1. Name of Felon(s)

2. The Felon(s) title/role in Vendor's entity, and

3. Details of Felon(s) Conviction(s).

No response

61 **Conflict of Interest Questionnaire Requirement**

Vendor agrees that it has looked up, read, and understood the current version of Texas Local Government Code Chapter 176 which generally requires disclosures of conflicts of interests by Vendor hereunder if Vendor:

(1) has an employment or other business relationship with a local government officer of our local governmental entity, or a family member of the officer, described by Section 176.003(a)(2)(A);

(2) has given a local government officer of our local governmental entity, or a family member of the officer, one or more gifts with the aggregate value specified by Section 176.003(a)(2)(B), excluding any gift described by Section 176.003(a-1); or

(3) has a family relationship with a local government officer of our local governmental entity.

(4) Any other financial, commercial, or familial relationship with our local government that may warrant reporting under this statute.

Does Vendor certify that it has NO reportable conflict of interest?

Yes

62 **Conflict of Interest Questionnaire Requirement - Form CIQ - Continued**

If you responded "No, Vendor does not certify - VENDOR HAS CONFLICT" to the Conflict of Interest Questionnaire question above, you are required by law to fully execute and upload the form attachment entitled "Conflict of Interest Questionnaire - Form CIQ." If you accurately claimed no conflict above, you may disregard the form attachment entitled "Conflict of Interest Questionnaire - Form CIQ."

Have you uploaded this form if applicable?

Not Applicable

63 **Upload of Current W-9 Required**

Vendors are required by TIPS to upload a current, accurate W-9 Internal Revenue Service (IRS) Tax Form for your entity. This form will be utilized by TIPS to properly identify your entity.

You must confirm that you are responding to this solicitation under your legal entity name. Go now to your Supplier Profile in this eBid System and confirm that your profile reflects your "Legal Name" as it is listed on your W9.

64 **Regulatory Good Standing Certification**

Does Vendor certify that its entity is in good standing will all government entities and agencies, whether local, state, or federal, that regulate any aspect of Vendor's field of work or business operations?

If Vendor selects "No", Vendor must provide explanation on the following attribute question.

Yes

65 **Regulatory Good Standing Certification - Explanation - Continued**

If Vendor responded to the prior attribute that "No", Vendor is not in good standing, Vendor must provide an explanation of that lack of good standing here for TIPS consideration.

No response

66 **Instructions Only - Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion**

Instructions for Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion

1. By answering yes to the next Attribute question below, the vendor and prospective lower tier participant is providing the certification set out herein in accordance with these instructions.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification in addition to other remedies available to the federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and / or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

4. The terms “covered transaction,” “debarred,” “suspended,” “ineligible,” “lower tier covered transaction,” “participants,” “person,” “primary covered transaction,” “principal,” “proposal” and “voluntarily excluded,” as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this form that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this form that it will include this clause titled “Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction” without modification in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible or voluntarily excluded from participation in this transaction, in addition to other remedies available to the federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and / or debarment.

67 **Suspension or Debarment Certification**

Read the instructions in the attribute above and then answer the following accurately.

Vendor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

Does Vendor certify?

Yes

68 **Vendor Certification of Criminal History - Texas Education Code Chapter 22**

Texas Education Code Chapter 22 requires entities that contract with school districts to provide services to obtain criminal history record information regarding covered employees. Contractors must certify to the district that they have complied. Covered employees with disqualifying criminal histories are prohibited from serving at a school district pursuant to this law.

DEFINITIONS

Covered employees: Employees of a contractor or subcontractor who have or will have continuing duties related to the service to be performed at the District and have or will have direct contact with students. The District will be the final arbiter of what constitutes direct contact with students.

Disqualifying criminal history: Any conviction or other criminal history information designated by the District, or one of the following offenses, if at the time of the offense, the victim was under 18 or enrolled in a public school: (a) a felony offense under Title 5, Texas Penal Code; (b) an offense for which a defendant is required to register as a sex offender under Chapter 62, Texas Code of Criminal Procedure; or (c) an equivalent offense under federal law or the laws of another state.

Vendor certifies:

NONE (Section A): None of the employees of Vendor and any subcontractors are covered employees, as defined above. If this box is checked, I further certify that Contractor has taken precautions or imposed conditions to ensure that the employees of Vendor and any subcontractor will not become covered employees. Contractor will maintain these precautions or conditions throughout the time the contracted services are provided under this procurement.

OR

SOME (Section B): Some or all of the employees of Vendor and any subcontractor are covered employees. If this box is checked, I further certify that: (1) Vendor has obtained all required criminal history record information regarding its covered employees. None of the covered employees has a disqualifying criminal history; (2) If Vendor receives information that a covered employee subsequently has a reported criminal history, Vendor will immediately remove the covered employee from contract duties and notify the purchasing entity in writing within 3 business days; (3) Upon request, Vendor will provide the purchasing entity with the name and any other requested information of covered employees so that the purchasing entity may obtain criminal history record information on the covered employees; (4) If the purchasing entity objects to the assignment of a covered employee on the basis of the covered employee's criminal history record information, Vendor agrees to discontinue using that covered employee to provide services at the purchasing entity.

Which option does Vendor certify?

Some

69	**Certification Regarding "Choice of Law" Terms with TIPS Members** Vendor agrees that if any "Choice of Law" provision is included in any sales agreement/contract between Vendor and a TIPS Member, that clause must provide that the "Choice of Law" applicable to the sales agreement/contract between Vendor and TIPS Member shall be the state where the TIPS Member operates unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a "Choice of Law" clause that conflicts with these terms is rendered void and unenforceable. If Vendor disagrees, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. Does Vendor agree? Yes
70	**Certification Regarding "Venue" Terms with TIPS Members** Vendor agrees that if any "Venue" provision is included in any sales agreement/contract between Vendor and a TIPS Member, that clause must provide that the "Venue" for any litigation or alternative dispute resolution is shall be in the state and county where the TIPS Member operates unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a "Venue" clause that conflicts with these terms is rendered void and unenforceable. If Vendor disagrees, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. Does Vendor agree? Yes
71	**Certification Regarding "Automatic Renewal" Terms with TIPS Members** Vendor agrees that no TIPS Sale may incorporate an "Automatic Renewal" clause that exceeds month to month terms with which the TIPS Member must comply. All renewal terms incorporated into a TIPS Sale Supplemental Agreement shall only be valid and enforceable when Vendor received written confirmation of acceptance of the renewal term from the TIPS Member for the specific renewal term. The purpose of this clause is to avoid a TIPS Member inadvertently renewing a Supplemental Agreement during a period in which the governing body of the TIPS Member has not properly appropriated and budgeted the funds to satisfy the Agreement renewal. Any TIPS Sale Supplemental Agreement containing an "Automatic Renewal" clause that conflicts with these terms is rendered void and unenforceable. If Vendor disagrees, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. Does Vendor agree? Yes

72	**Certification Regarding "Indemnity" Terms with TIPS Members** Texas and other jurisdictions restrict the ability of governmental entities to indemnify others. Vendor agrees that if any "Indemnity" provision which requires the TIPS Member to indemnify Vendor is included in any sales agreement/contract between Vendor and a TIPS Member, that clause must either be stricken or qualified by including that such indemnity is only permitted, "to the extent permitted by the laws and constitution of [TIPS Member's State]" unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing an "Indemnity" clause that conflicts with these terms is rendered void and unenforceable. If Vendor disagrees, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. Does Vendor agree? Yes
73	**Certification Regarding "Arbitration" Terms with TIPS Members** Vendor agrees that if any "Arbitration" provision is included in any TIPS Sale agreement/contract between Vendor and a TIPS Member, that clause may ***not*** require that the arbitration is mandatory or binding. Vendor agrees that if any "Arbitration" provision is included in any TIPS Sale agreement/contract between Vendor and a TIPS Member, that clause provides for only voluntary and non-binding arbitration unless the TIPS Member expressly agrees otherwise. Any TIPS Sale Supplemental Agreement containing a “Arbitration” clause that conflicts with these terms is rendered void and unenforceable. If Vendor disagrees, after this solicitation legally closes and TIPS begins evaluating Vendor's file, TIPS will provide Vendor with a draft Word Document version of the Vendor Agreement and will be instructed to include all requested negotiations as redline edits for TIPS consideration. Does Vendor agree? Yes
74	**2 CFR PART 200 AND FEDERAL CONTRACT PROVISIONS EXPLANATION** TIPS and TIPS Members will sometimes seek to make purchases with federal funds. In accordance with 2 C.F.R. Part 200 of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (sometimes referred to as “EDGAR”),Vendor's response to the following questions labeled "2 CFR Part 200 or Federal Provision" will indicate Vendor's willingness and ability to comply with certain requirements which may be applicable to TIPS purchases paid for with federal funds, if accepted by Vendor. Your responses to the following questions labeled "2 CFR Part 200 or Federal Provision" will dictate whether TIPS can list this awarded contract as viable to be considered for a federal fund purchase. **Failure to certify all requirements labeled "2 CFR Part 200 or Federal Provision" will mean that your contract is listed as not viable for the receipt of federal funds. However, it will not prevent award.** If you do enter into a TIPS Sale when you are accepting federal funds, the contract between you and the TIPS Member will likely require these same certifications.

75	**2 CFR Part 200 or Federal Provision - Vendor Willingness to Accept Federal Funds** This certification is not required by federal law. However, TIPS Members are public entities and qualifying non-profits which often receive federal funding and grants (ESSER, CARES Act, EDGAR, etc.) ***Accepting such funds often requires additional required certifications and responsibilities for Vendor.*** The following attribute questions include these required certifications. Your response to this questions, the following certifications, and other factors will determine whether your contract award will be deemed as eligible for federal fund expenditures by TIPS Members. If awarded, is Vendor willing to accept payment for goods and services offered under this contract paid for by a TIPS Member with federal funds? Yes
76	**2 CFR Part 200 or Federal Provision - Contracts** Contracts for more than the simplified acquisition threshold currently set at $250,000 (2 CFR § 200.320), which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate. Notice: Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, ESC Region 8 and TIPS Members reserve all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party. Does vendor agree? Yes
77	**2 CFR Part 200 or Federal Provision - Termination** Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of $10,000) Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, ESC Region 8 and TIPS Members reserve the right to terminate any agreement in excess of $10,000 resulting from this procurement process for cause after giving the vendor an appropriate opportunity and up to 30 days, to cure the causal breach of terms and conditions. ESC Region 8 and TIPS Members reserve the right to terminate any agreement in excess of $10,000 resulting from this procurement process for convenience with 30 days notice in writing to the awarded vendor. The Vendor would be compensated for work performed and goods procured as of the termination date if for convenience of the ESC Region 8 and TIPS Members. Any award under this procurement process is not exclusive and the ESC Region 8 and TIPS reserves the right to purchase goods and services from other vendors when it is in the best interest of the ESC Region 8 and TIPS. Does vendor agree? Yes

78	**2 CFR Part 200 or Federal Provision - Clean Air Act** Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended—Contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). Pursuant to the Clean Air Act, et al above, when federal funds are expended by ESC Region 8 and TIPS Members, ESC Region 8 and TIPS Members require that the proposer certify that during the term of an award by the ESC Region 8 and TIPS Members resulting from this procurement process the vendor agrees to comply with all of the above regulations, including all of the terms listed and referenced therein. Does vendor agree? Yes
79	**2 CFR Part 200 or Federal Provision - Byrd Anti-Lobbying Amendment** Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, ESC Region 8 and TIPS Members require the proposer certify that during the term and during the life of any contract with ESC Region 8 and TIPS Members resulting from this procurement process the vendor certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). Does Vendor agree? Yes

80	**2 CFR Part 200 or Federal Provision - Byrd Anti-Lobbying Amendment - Continued** Applicable to Grants, Subgrants, Cooperative Agreements, and Contracts Exceeding $100,000 in Federal Funds Submission of this certification is a prerequisite for making or entering into this transaction and is imposed by the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure. **The undersigned certifies, to the best of his or her knowledge and belief, that:** (1) No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement. (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “disclosure Form to Report Lobbying,” in accordance with its instructions. (3) The undersigned shall require that the language of this certification be included in the award documents for all covered subawards exceeding $100,000 in Federal funds at all appropriate tiers and that all subrecipients shall certify and disclose accordingly. Does Vendor certify that it has NOT lobbied as described herein? Yes

81	**2 CFR Part 200 or Federal Provision - Byrd Anti-Lobbying Amendment - Continued** If you answered "No, Vendor does not certify - Lobbying to Report" to the above attribute question, you must download, read, execute, and upload the attachment entitled "Disclosure of Lobbying Activities - Standard Form - LLL", as instructed, to report the lobbying activities you performed or paid others to perform.

82	**2 CFR Part 200 or Federal Provision - Federal Rule** Compliance with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act (42 U.S.C. 1857(h)), section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15). (Contracts, subcontracts, and subgrants of amounts in excess of $100,000) Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, ESC Region 8 and TIPS Members requires the proposer certify that in performance of the contracts, subcontracts, and subgrants of amounts in excess of $250,000, the vendor will be in compliance with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act (42 U.S.C. 1857(h)), section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15). Does vendor certify compliance? Yes

83	**2 CFR Part 200 or Federal Provision - Procurement of Recovered Materials** A non-Federal entity that is a state agency or agency of a political subdivision of a state and its contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include: (1) procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; (2) procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines. Does vendor certify that it is in compliance with these provisions? Yes
84	**2 CFR Part 200 or Federal Provision - Rights to Inventions** If the Federal award meets the definition of “funding agreement” under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency. Pursuant to the above, when the foregoing applies to ESC Region 8 and TIPS Members, Vendor certifies that during the term of an award resulting from this procurement process, Vendor agrees to comply with all applicable requirements as referenced in the Federal rule above. Does vendor certify? Yes

85	**2 CFR Part 200 or Federal Provision - Domestic Preferences for Procurements and Compliance with Buy America Provisions** As appropriate and to the extent consistent with law, TIPS Member Customers, to the greatest extent practicable under a Federal award, may provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). Vendor agrees that the requirements of this section will be included in all subawards including all contracts and purchase orders for work or products under this award, to the greatest extent practicable under a Federal award. For purposes of 2 CFR Part 200.322, “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stag through the application of coatings, occurred in the United States. Moreover, for purposes of 2 CFR Part 200.322, “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum, plastics and polymer-based products such as polyvinyl chloride pipe, aggregates such as concrete, glass, including optical fiber, and lumber. Vendor certifies that it is in compliance with all applicable provisions of the Buy America Act. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition. For purposes of 2 CFR Part 200.322, “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber. Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, Vendor certifies that to the greatest extent practicable Vendor will provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). Does Vendor Certify? Yes

86

2 CFR Part 200 or Federal Provision - Ban on Foreign Telecommunications

ESC 8 and TIPS Members are prohibited from obligating or expending Federal financial assistance, to include loan or grant funds, to: (1) procure or obtain, (2) extend or renew a contract to procure or obtain, or (3) enter into a contract (or extend or renew a contract) to procure or obtain, equipment, services, or systems that use "covered telecommunications" equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. "Covered telecommunications" equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities), and physical security surveillance of critical infrastructure and other national security purposes, and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities) for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes detailed in 2 CFR § 200.216.

Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, Vendor certifies that Vendor will not purchase equipment, services, or systems that use "covered telecommunications", as defined by 2 CFR §200.216 equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Does vendor certify?

Yes

87

2 CFR Part 200 or Federal Provision - Contract Cost & Price

For contracts more than the simplified acquisition threshold currently set at $250,000, a TIPS Member may, in very rare circumstances, be required to negotiate profit as a separate element of the price pursuant to 2 C.F.R. 200.324(b). Under those circumstances, Vendor agrees to provide information and negotiate with the TIPS Member regarding profit as a separate element of the price. However, Vendor certifies that the total price charged by the Vendor shall not exceed the Vendor's TIPS pricing and pricing terms proposed.

Does Vendor certify?

Yes

88

2 CFR Part 200 or Federal Provision - Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members on any federally assisted construction contract, the equal

opportunity clause is incorporated by reference here.

Does Vendor Certify?

Yes

89	**2 CFR Part 200 or Federal Provision - Davis Bacon Act Compliance** Texas Statute requires compliance with Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146- 3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non- Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. Pursuant to state and federal requirements, Vendor certifies that it will be in compliance with all applicable Davis-Bacon Act provisions if/when applicable. Does Vendor certify? Yes
90	**2 CFR Part 200 or Federal Provision - Contract Work Hours and Safety Standards** Where applicable, all contracts awarded by ESC 8 and TIPS Members in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence. Pursuant to the above, when federal funds are expended by ESC Region 8 and TIPS Members, Vendor certifies that during the term of an award for all contracts resulting from this procurement process, Vendor will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act. Does Vendor certify? Yes

91 **2 CFR Part 200 or Federal Provision - FEMA Fund Certification & Certification of Access to Records**

If and when Vendor accepts a TIPS purchase paid for in full or part with FEMA funds, Vendor certifies that:

(1) Vendor agrees to provide the TIPS Member, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to and rights to reproduce any books, documents, papers, and records of the Contractor which are directly pertinent to this contract, or any contract resulting from this procurement, for the purposes of making audits, examinations, excerpts, and transcriptions. This right also includes timely and reasonable access to Vendor's personnel for the purpose of interview and discussion relating to such documents. Vendor agrees to provide the FEMA Administrator or an authorized representatives access to construction or other work sites pertaining to the work being completed under the contract. Vendor acknowledges and agrees that no language in this contract or the contract with the TIPS Member is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

(2) The Vendor shall not use the Department of Homeland Security's seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

(3) The Vendor will comply with all applicable Federal law, regulations, executive orders, FEMA policies, procedures, and directives.

(4) The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the non-Federal entity, contractor, or any other party pertaining to any matter resulting from the contract.

(5) The Vendor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Vendor's actions pertaining to this contract.

Does Vendor certify?

Yes, Vendor certifies

92 **2 CFR Part 200 or Federal Provision - Certification of Compliance with the Energy Policy and Conservation Act**

When appropriate and to the extent consistent with the law, Vendor certifies that it will comply with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq; 49 C.F.R. Part 18) and any state mandatory standards and policies relating to energy efficiency which are contained in applicable state energy conservation plans issued in compliance with the Act.

Does Vendor certify?

Yes

93	**2 CFR Part 200 or Federal Provision - Certification of Compliance with Never Contract with the Enemy** Where applicable, all contracts awarded by ESC 8 and TIPS Members in excess of $50,000.00, within the period of performance, and which are performed outside of the United States, including U.S. territories, are subject to the regulations implementing Never Contract with the Enemy in 2 CFR part 183. Per 2 CFR part 183, in the situation specified, ESC 8 and TIPS Members shall terminate any contract or agreement resulting from this procurement which violates the Never Contract with the Enemy regulation in 2 CFR part 183, including if Vendor is actively opposing the United States or coalition forces involved in a contingency operation in which members of the the Armed Forces are actively engaged in hostilities. Vendor certifies that it is neither an excluded entity under the System for Award Management (SAM) nor Federal Awardee Performance and Integrity Information System (FAPIIS) for any contract terminated due to Never Contract with the Enemy as a Termination for Material Failure to Comply. Does Vendor certify? Yes
94	**2 CFR Part 200 or Federal Provision - Certification of Compliance with EPA Regulations** For contracts resulting from this procurement, in excess of $100,000.00 and paid for with federal funds, Vendor certifies that Vendor will comply with all applicable standards, orders, regulations, and/or requirements issued pursuant to the Clean Air Act of 1970, as amended (42 U.S.C. 1857(h)), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15. Does Vendor certify? Yes
95	**2 CFR Part 200 or Federal Provision - Record Retention Requirements** For contracts resulting from this procurement, paid for by ESC 8 or TIPS Members with federal funds, Vendor certifies that Vendor will comply with the record retention requirements detailed in 2 CFR § 200.334. Vendor certifies that Vendor will retain all records as required by 2 CFR § 200.334 for a period of three years after final expenditure or financial reports, as applicable, and all other pending matters are closed. Does Vendor certify? Yes
96	**2 CFR Part 200 or Federal Provision - Subcontracting and Affirmative Steps for Small and Minority Businesses, Women's Business Enterprises, and Labor Surplus Area Firms.** Do you ever anticipate the possibility of subcontracting any of your work under this award if you are successful? If you respond "Yes", you must respond to the following attribute question accurately. If you respond "No", you may skip the following attribute question. Yes

97	**2 CFR Part 200 or Federal Provision - If "Yes" Response to Above Attribute - Continued - Subcontracting and Affirmative Steps for Small and Minority Businesses, Women's Business Enterprises, and Labor Surplus Area Firms.** **Only respond to this question if you responded "Yes" to the attribute question directly above. Skip this question if you responded "No" to the attribute question directly above.** Does Vendor certify that it will follow the following affirmative steps? Federal Regulation 2 CFR §200.321 Contracting with small and minority businesses, women's business enterprises, and labor surplus area firms. (a)The non-Federal entity must take all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. (b) Affirmative steps must include: (1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists; (2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources; (3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises; (4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises; (5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce ; and (6) Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs(1) through (5) of this section. Does Vendor certify? Yes
98	**ACKNOWLEDGMENT & BINDING CORPORATE AUTHORITY** By submitting this proposal, the individual(s) submitting on behalf of the Vendor certify that they are authorized by Vendor to complete and submit this proposal on behalf of Vendor and that this proposal was duly submitted on behalf of Vendor by authority of its governing body, if any, and within the scope of its corporate powers. Vendor further certifies that it has read, examined, and understands all portions of this solicitation including but not limited to all attribute questions, attachments, solicitation documents, bid notes, and the Vendor Agreement(s). Vendor certifies that, if necessary, Vendor has consulted with counsel in understanding all portions of this solicitation.

TIPS 230504 Information Technology Equipment, Software, and Services	U. S. TelePacific Corp DBA

TIPS REFERENCE FORM

All requested information must be typed and uploaded in Excel format. Do not handwrite or upload in any format other than Excel. Emails provided must be current and active. Do not include TIPS/Region 8 employees as a reference. The entities that you provide must be paying customers, not affiliates/partners/manufacturers/resellers, etc.

You must provide below at least three (3) references from three different entity customers, preferably government or non-profit entities, who have purchased goods or services from your vendor entity within the last three years.

Customer Entity Name	Customer Contac	Valid Contact Email	Valid Contact Phone
Example: ABC University	Director John Do	jdoe@abcuniverisity.edu	800-111- 2222
Workforce Solutions of Greater Dallas	Alex Perez	aperez@wfsdallas.com	214-290-1029
Falls County Courthouse	Joan Kostiha	auditor@co.falls.tx.us	254-883-1406
Boys & Girls Club of Central Texas, Inc	Brandon Fogle	bfogle@bgctx.org	254-699-5808

TIPS CONTRACT 230504

REQUIRED CONFIDENTIALITY CLAIM FORM

(*VENDOR MUST COMPLETE THE FOLLOWING VENDOR INFORMATION*)

Vendor Entity Name: U.S. TelePacific Corp db TPx Communications

Vendor Authorized Signatory Name: Tasha Wilson

Vendor Authorized Signatory Title: Manager of RFP & Bid Management

Vendor Authorized Signatory Email: formrequest@tpx.com

Vendor Address: 303 Colorado Street, Suite 2075

City: Austin State: Texas Zip Code: 78701

Vendor agrees that it is voluntarily providing its data (including but not limited to: Vendor information, Vendor documentation, Vendor's proposal, Vendor pricing submitted or provided to TIPS, TIPS contract documents, TIPS correspondence, Vendor logos and images, Vendor's contact information, Vendor's brochures and commercial information, Vendor's financial information, Vendor's certifications, and any other Vendor information or documentation submitted to TIPS by Vendor and its agents) (Hereinafter, "Vendor Data") to TIPS. Vendor understands and agrees that TIPS is a government entity subject to public information laws including but not limited to Texas Government Code (TGC) Chapter 552. Vendor agrees that regardless of confidentiality designations herein, Vendor's submission of a proposal constitutes Vendor's consent to the disclosure and release of Vendor's Data and comprehensive proposal, including any information deemed confidential or proprietary herein, to and by TIPS Members.

Notwithstanding the foregoing permissible release to TIPS Members, if Vendor considers any portion of Vendor's proposal to be otherwise confidential and not subject to public disclosure pursuant to public information laws, including but not limited to TGC Chapter 552, Vendor must properly execute ***Option 1 only*** below, attach to this PDF all documents and information that Vendor deems confidential, and upload the consolidated documentation. Regardless of the Option selected below, this form must be completed and uploaded to the "Response Attachments" section of the eBid System entitled "Required Confidentiality Claim Form." Execution and submission of this form is the sole indicator of whether Vendor considers any Vendor Data confidential in the event TIPS receives a request, a Public Information Request, or subpoena. If TIPS receives a request, any responsive documentation not deemed confidential by you through proper execution of Option 1 of this form will be automatically released. For information deemed confidential by you through proper execution of Option 1 of this form, TIPS will follow procedures of controlling statute(s) regarding withholding that documentation and shall not be liable for any release of information required by law, including Attorney General opinion or court order.

(*VENDOR MUST COMPLETE ONE OF THE TWO OPTIONS AND UPLOAD IN THE EBID SYSTEM*)

OPTION 1 – DESIGNATING CONFIDENTIAL MATERIALS – YES, VENDOR HAS ATTACHED CONFIDENTIAL MATERIALS

(*Confirm each bullet point and sign below*)

- Vendor claims some Vendor Data confidential to the extent permitted by TGC Chapter 552 and other applicable law.
- Vendor attached to this PDF all potentially confidential Vendor Data and listed the number of attached pages below.
- Vendor's authorized signatory has signed below and shall upload this document in the proper location in the eBid System.
- Vendor agrees that TIPS shall not be liable for any release of confidential information required by law.

Number of pages attached deemed confidential: _____

Authorized Signature: _____

OPTION 2 – WAIVER OF CONFIDENTIALITY – NO, VENDOR HAS NOT ATTACHED CONFIDENTIAL MATERIALS

(*Confirm each bullet point and sign below*)

By signing for Option 2 below, Vendor expressly waives any confidentiality claim for all Vendor Data submitted in relation to this proposal and resulting contract. Vendor confirms that TIPS may freely release Vendor Data submitted in relation to this proposal or resulting contract to any requestor. Vendor agrees that TIPS shall not be responsible or liable for any use or distribution of Vendor Data by TIPS or TIPS Members.

- Vendor's authorized signatory has signed below and shall upload this document in the proper location in the eBid System.
- Vendor agrees that TIPS shall not be liable for any release of confidential information required by law.

Authorized Signature: DocuSigned by: Tasha Wilson BD69F33AF0FC4D0... _____

VENDOR SUPPLEMENTAL INFORMATION

TIPS permits Vendors to submit supplemental documentation and information ("Vendor Supplemental Information") with their proposals to display to TIPS Member Customers their qualifications, offerings, and special terms. The following documents are for marketing and informational purposes only. They are not terms of Vendor's TIPS Contract. If the Vendor Supplemental Information herein contains any warranties, terms, or conditions, the TIPS Member Customer may review and determine whether or not those are applicable and acceptable for any TIPS purchase before proceeding. If the Vendor Supplemental Information contains any licenses or certificates, TIPS encourages the TIPS Member Customer to ensure current accuracy at the time of a TIPS purchase.

Endpoint Security
Managed DNS Protection

Protect devices from Internet threats anytime, anywhere

Domain Name System (DNS) Protection can greatly reduce the effectiveness of ransomware, phishing, botnet, and malware campaigns by blocking known-malicious domains[1]. This important security solution can be used to protect all endpoints, including servers, workstations, and IoT devices. It blocks as much as 88% of Internet-based threats before they hit your network or endpoints[2].

Why should I implement DNS Protection?

Protect against Internet threats Defend against Internet-based threats by blocking and filtering traffic to/from malicious sites, sites infected with malware, or sites with questionable or dangerous content.

Enforce compliance and policy DNS protection offers increased visibility and control over Internet use, which helps you maintain compliance and enforce corporate Internet use policy.

Safeguard remote users Endpoint DNS Protection helps remote devices and users maintain strong security when outside the corporate network.

Why should I choose TPx?

Leading threat intelligence TPx DNS Protection service is powered by Webroot's world-class Threat Intelligence, which is trusted by over 90 network and security technology vendors worldwide to enhance their own solutions.

Flexible deployment options TPx DNS protection can be used to safeguard any device that accesses the Internet. Deploy TPx DNS protection on Windows devices to protect users while on your network or while traveling. Need to protect IoT devices, servers, or devices accessing your Wi-Fi network? Deploying TPx DNS at the network edge allows complete protection regardless of device type.

Fully managed TPx delivers a turn-key solution that leaves you free to run your business. Our team professionally onboards your service and our support team is available 24x7x365 to assist.

[1] Cybersecurity & Infrastructure Security Agency (CISA) [2] Webroot

How It Works

Traffic Redirection Internet-based traffic to/from your endpoints is routed through a secure cloud infrastructure to create a highly secure, resilient, private, and manageable connection to the Internet.

Advanced Filtering Automated filtering blocks requests to undesirable, dangerous, or malicious internet domains. Support for DNS over HTTPS (DoH) is included to increase security through filtering encrypted Internet traffic.

Best-in-class Threat Intelligence Data correlation between domains, URLs, IPs, files, mobile apps, and more provides a comprehensive and continuously updated view of the Internet threat landscape — not just URLs and IPs.

What's Included?

Anytime, Anywhere Protection Individual device agents protect Windows systems and users from Internet threats while on your network or roaming.

Security for Any Device DNS Protection installed on your network gateway protects servers, IoT devices, wireless users, and other systems for comprehensive location-based security.

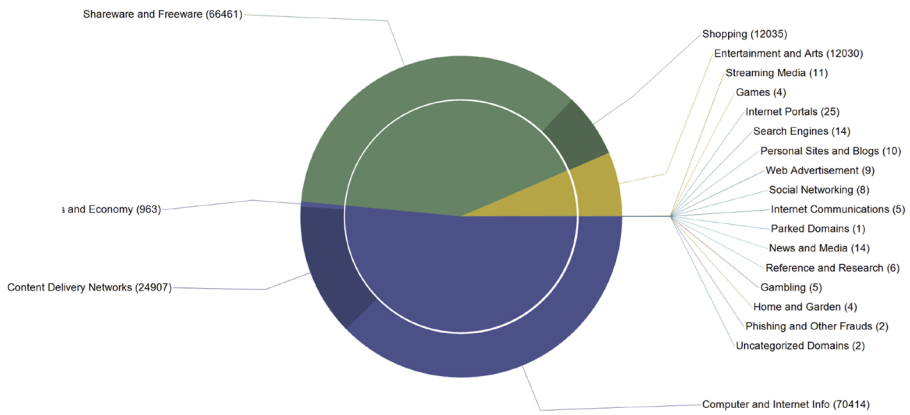
Customized Security Policies DNS protection policies can be customized using TPx recommended templates to address the different security needs of your users.

Monthly Reporting Customers automatically receive a comprehensive monthly report that provides visibility into your organization's Internet use and security.

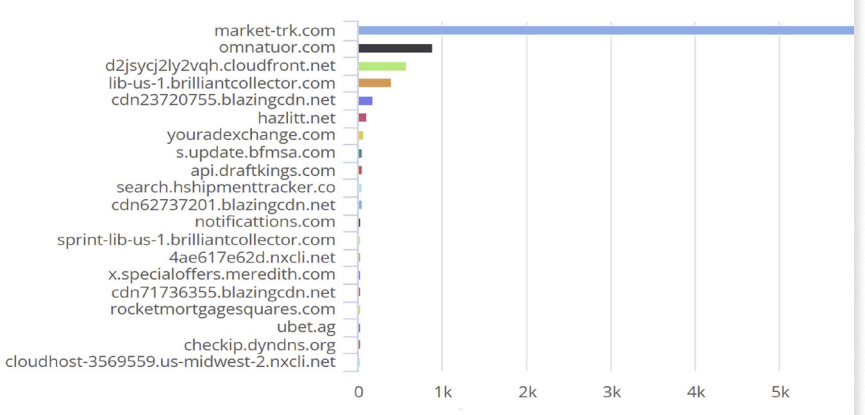
24/7/365 Helpdesk Support You can rely on our experienced resources to ensure that your DNS protection solution remains effective and meets your compliance and policy requirements.

TPx's Managed Detection and Response is powered by WEBROOT an opentext company Webroot BrightCloud® Internet Threat Intelligence

DNS: TOP BLOCKED CATEGORY



DNS: TOP BLOCKED DOMAIN



Managed DNS Protection is an integral part of TPx's security services portfolio for protecting endpoints and users from ransomware and other cyberattacks. Bundling multiple services can increase your overall value and improve your organization's security. Below is our current portfolio of Endpoint and User Security and Management services.

Service Features	Description	Endpoint Management	Endpoint Security	User Security
Monitoring, Alerting, and Reporting	TPx provides automated monitoring and alerting and scheduled reports for device availability, health and performance, and inventory. Monitoring and alerting are per TPx's recommended practices. Alerts are received and actionable by either TPx or the customer, based on service level.	■		
System Patching	TPx provides managed, automated patching of operating systems and select third-party applications. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting are also included.	■		
Remote System Support	TPx provides 24/7 troubleshooting and repair of covered devices. Service includes proactive support based on TPx recommended practice and responsive support for customer requests or identified alerts. Remote Systems support features may be included in the fixed monthly charge or billable based on the chosen service level.	■		
Lifecycle Management	TPx provides proactive reporting and communication of end-of-life status on covered servers. Service includes hardware warranty expiration as well as manufacturer end-of-support status for operating systems and select applications. Post-warranty hardware support packages are available at additional cost.	■		
Managed NGAV	TPx provides managed Next-Generation Antivirus support. Service includes the use and management of the NGAV software as well as monitoring, alerting, and reporting on NGAV status. Virus remediation is available as a billable service.		■	
Endpoint Managed Detection and Response	TPx provides MDR services to identify and prevent advanced security attacks. The service includes the use and management of leading EDR software, SaaS platform hosting, SOC threat hunting, alert response, and event mitigation with an industry-leading 15-minute response time.		■	
DNS Protection	TPx provides DNS Protection for covered devices to combat Internet-born threats and enforce Internet usage policy. Service includes the use and management of the DNS Agent software, configuration of security policies, and monitoring and reporting on browsing activity and security events.		■	
Security Awareness Training	TPx provides automated Security Awareness Training campaigns. Service includes campaign setup, ongoing phishing simulations, and monthly training courses delivered automatically to enrolled users. Scheduled reporting of campaign status and activity is also included.			■
Inbox Detection and Response	TPx Inbox Detection and Response service allows users to easily report potential phishing emails. Reported emails are quarantined then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inbox and all instances of malicious emails are automatically removed from all other users' mailboxes.			■

All service features are available in pre-packaged solution bundles to meet a variety of use cases. Endpoint Security and User Security service features are also available as stand-alone offerings.

Managed detection and response (MDR)

Traditional security solutions like anti-virus software can no longer adequately protect your network and systems from cyberattacks. Protection today, and in the future, requires a more sophisticated and proactive approach that combines advanced technology with skilled and dedicated security professionals to deliver 24/7/365 detection and response.

Strong defense against cyber threats doesn't have to be difficult or pricey. MDR from TPx helps you discover, prevent, and recover from cyber threats faster.

[1] *Ponemon Institute – State of Endpoint Security 2020*

[2] *2020 Cost of Data Breach Report*

Why should I use MDR?

Identify more threats Antivirus solutions miss an average of 60% of attacks.[1] MDR significantly increases the number and type of attacks that are detected and stopped.

Reduce attack dwell time The average time to identify and contain a breach (its dwell time or "lifecycle") is 280 days, according to a 2020 study.[2] The lifecycle of a breach factors heavily into the overall cost. MDR reduces this time exponentially which limits the impact of any attacks.

Proactively mitigate attacks MDR uses a proactive approach to more quickly mitigate attacks so they can't spread across your network and cause additional damage.

Why should I choose TPx?

Leading technology Best-in-class detection and response technology delivers powerful visibility, detection, alerting, and mitigation of cyberattacks.

Advanced threat hunting Dedicated Security Operations Center staff work 24/7 to quickly identify advanced threats that evade existing security solutions and provides expert analysis on attack details and mitigation activity.

Fully Managed Having the right software is not enough. You also need the right team to deliver a turnkey solution that leaves you free to run your business.

Available TPx MDR Services

At TPx, we specialize in providing IT management and security services that provide customers with multiple opportunities to prevent and recover from cyberattacks like ransomware.

Firewall MDR Our cybersecurity experts manage and monitor your firewall, so that when threats are found, they immediately take action to help ensure your business is protected.

Endpoint MDR Protects individual servers and workstations against advanced threats anytime, anywhere.

User Security
Managed Inbox Detection & Response

Professional evaluation and handling of suspicious emails reported by users — right from the inbox

Phishing continues to be the number one cause of data breaches. In 2021, 53% of organizations reported a phishing-related breach[1]. Email security filters, while generally effective, are not foolproof. Increasingly, organizations are augmenting these solutions with user-driven reporting of suspicious emails. But how do already overburdened Security teams keep up with monitoring and evaluating suspicious emails that are being reported? The answer is Inbox Detection and Response (IDR).

Why should I use IDR?

Efficiently report suspicious emails IDR gives users a faster, easier way to take the guesswork out of questionable messages. Reporting suspicious emails is done with a single click right from their inbox.

Quickly validate reported emails Using advanced technology and human security experts, reported emails are validated and either returned or removed within minutes. This reinforces the users' security awareness, which better protects the organization.

Identify and remove all malicious emails Reported emails deemed malicious will be automatically and globally removed from the customer's domain, eliminating the opportunity for others to fall victim to the phishing attempt.

Why should I choose TPx?

Leading technology Best-in-class security technology and automated machine learning engines are used to quickly and accurately identify and mitigate malicious emails.

Advanced security analysis Inconclusive messages are further analyzed by a team of security experts 24/7/365 to accurately make a final determination.

Exceptional user experience Reporting is done via a single click using a button in the Outlook Ribbon. Regardless of whether the email is malicious or not, a clear status is communicated to the user.

Comprehensive support TPx takes care of all technical support for the solution to ensure that it works as designed and your organization receives maximum value.

[1] *Dark Reading, 2021 Strategic Security Survey*

Employee notices suspicious email and clicks the GoSecure Titan IDR button to submit for review

Real-time reporting gives the in-house security team clear visibility into the incident and its resolution.

Email is automatically quarantined and routed through the Active Response Center.

Within minutes, a status message is returned. The message is either verified or removed.

Automated machine learning engines investigate the suspicious email.

Human security experts conduct a further review on inconclusive messages through a multi-faceted analysis.

What's included?

Onboarding Services TPx's professional onboarding process allows you to quickly achieve value for your investment. TPx configures the IDR platform, provides expert guidance to configure your Office 365 environment and manages the entire implementation project.

Technical Support TPx will manage the system to ensure that it is functioning as designed. This includes delivering platform support as well as guidance on troubleshooting Office 365 and the Outlook add-in. Our team is available 24/7/365 to assist and enhance the success of our solution for your organization.

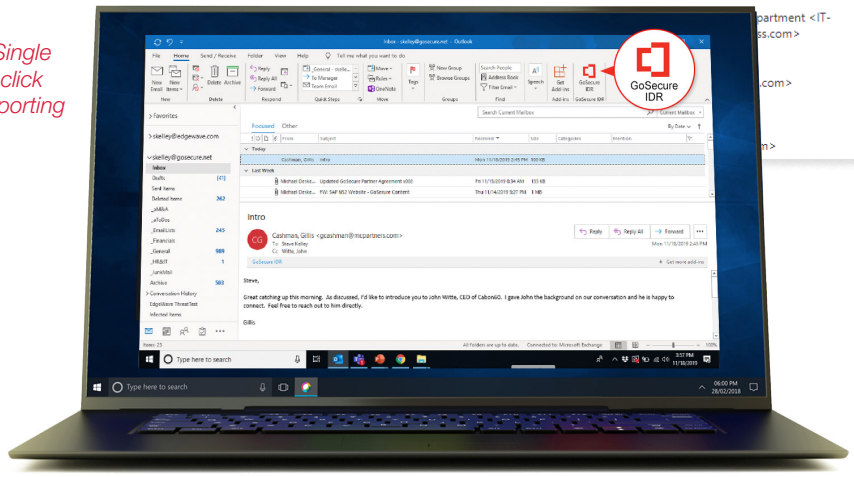
Change Management Adding new licenses and assigning users is easy. We'll handle all requests to ensure that licenses and users are added quickly and effectively.

Platform Management and Updates Security threats evolve, and our solution evolves with them. Enhancements to the security capabilities and performance of the IDR platform are automatically provided to maximize efficacy.

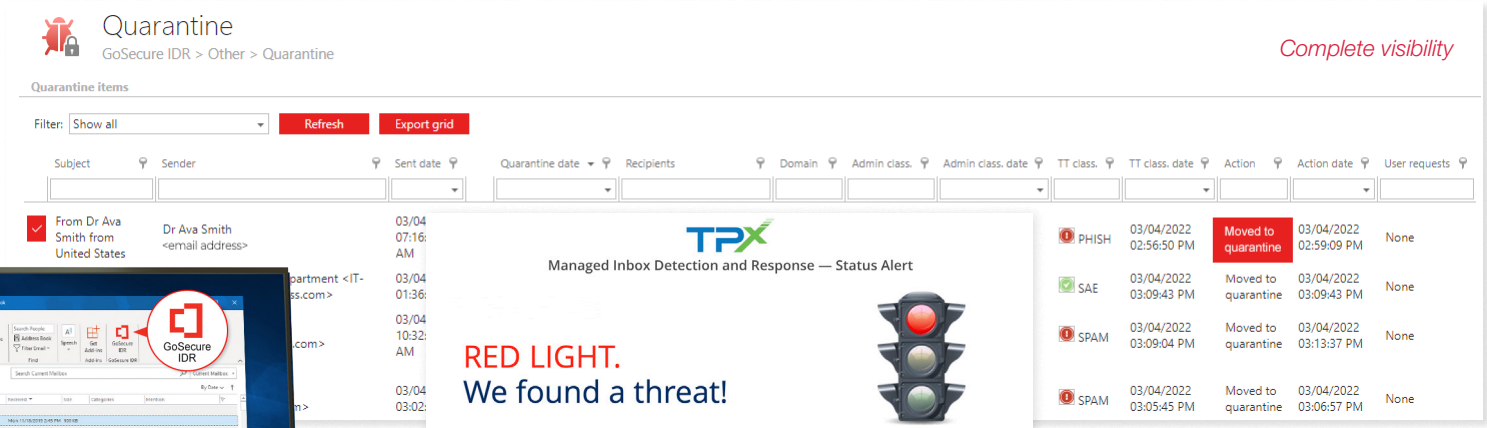
Cost-effective Security This complete turn-key solution is provided for a fixed per-user monthly cost. You benefit from having exceptional security without the expense of acquiring and managing the technology in-house.

TPx Inbox Detection and Response is powered by the GoSecure Titan Platform

Single click reporting



Complete visibility



Quick, efficient analysis

Managed Inbox Detection and Response is an integral part of TPx's security services portfolio for protecting endpoints and users from ransomware and other cyberattacks. Bundling multiple services can increase your overall value and improve your organization's security. Below is our current portfolio of Endpoint and User Security and Management services.

Service Features	Description	Endpoint Management	Endpoint Security	User Security
Monitoring, Alerting, and Reporting	TPx provides automated monitoring and alerting and scheduled reports for device availability, health and performance, and inventory. Monitoring and alerting are per TPx's recommended practices. Alerts are received and actionable by either TPx or the customer, based on service level.	■		
System Patching	TPx provides managed, automated patching of operating systems and select third-party applications. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting are also included.	■		
Remote System Support	TPx provides 24/7 troubleshooting and repair of covered devices. Service includes proactive support based on TPx recommended practice and responsive support for customer requests or identified alerts. Remote Systems support features may be included in the fixed monthly charge or billable based on the chosen service level.	■		
Lifecycle Management	TPx provides proactive reporting and communication of end-of-life status on covered servers. Service includes hardware warranty expiration as well as manufacturer end-of-support status for operating systems and select applications. Post-warranty hardware support packages are available at additional cost.	■		
Managed NGAV	TPx provides managed Next-Generation Antivirus support. Service includes the use and management of the NGAV software as well as monitoring, alerting, and reporting on NGAV status. Virus remediation is available as a billable service.		■	
Endpoint Managed Detection and Response	TPx provides MDR services to identify and prevent advanced security attacks. The service includes the use and management of leading EDR software, SaaS platform hosting, SOC threat hunting, alert response, and event mitigation with an industry-leading 15-minute response time.		■	
DNS Protection	TPx provides DNS Protection for covered devices to combat Internet-born threats and enforce Internet usage policy. Service includes the use and management of the DNS Agent software, configuration of security policies, and monitoring and reporting on browsing activity and security events.		■	
Security Awareness Training	TPx provides automated Security Awareness Training campaigns. Service includes campaign setup, ongoing phishing simulations, and monthly training courses delivered automatically to enrolled users. Scheduled reporting of campaign status and activity is also included.			■
Inbox Detection and Response	TPx Inbox Detection and Response service allows users to easily report potential phishing emails. Reported emails are quarantined then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inbox and all instances of malicious emails are automatically removed from all other users' mailboxes.			■

All service features are available in pre-packaged solution bundles to meet a variety of use cases. Endpoint Security and User Security service features are also available as stand-alone offerings.

Security artisans bring expertise, passion, and technology to cybersecurity.

Cybersecurity technology is meaningless unless properly configured, monitored and maintained

Outdated software and unmanaged devices leave your company open to cyber threats. Erroneous configurations give hackers a way around your security assets.

The TPx team and its group of highly trained security professionals based in our two Security Operations Centers (SOC) will configure, deploy, manage, and monitor your next generation firewall (NGFW) to help protect your business from cyber threats.

Our people defending your business and your people

TPx Managed Firewall service shields organizations and their employees with enterprise-grade security for a fraction of the cost of a single security analyst. The service includes certified security analysts who combine human intelligence with AI and threat intelligence driven data to find and terminate threats before they impact your business.

Our cybersecurity experts manage and monitor your firewall and when threats are found they immediately take action to

We can provide a co-managed solution that allows TPx to work closely with your IT team through a common change management system and process.

neutralize them. While in-house solutions can take years and hundreds of thousands of dollars to develop to full maturity, our rapidly deployed service offers immediate value and added safeguards for businesses. You may know firewalls for security and their ability to block today's advanced threats, but with MSx Managed Firewalls, the benefits go far beyond that. Secure access, visibility and control are major advantages that can help your business be more productive.

Secure Access SD-WAN enables organizations to leverage multiple transport services (e.g. broadband internet, 5G, etc.) to connect users securely and economically to applications and each other, while a Virtual Private Network (VPN) connects remote workers.

Visibility With detailed reporting by TPx, know what is happening on your network — from the top applications running and the top websites being visited, down to which users are on the VPN.

Control Once you know what is happening on your network, you can take action to control your network, so your productivity is maximized. Want to stop bandwidth and time-draining applications like video streaming? The choice and control are in your hands.

76% of SMBs in the United States reported a cyber-attack last year.

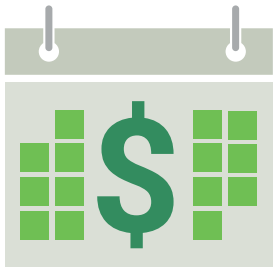
Managed Detection and Response

MSx Firewalls with Managed Detection and Response does more than block suspicious IP addresses and preconfigured static signatures, it augments existing firewall controls with dedicated security analysts who combine context, deep security understanding and expertise with today's advanced technology to make data actionable. We detect the threats other technologies miss. But it isn't enough to just detect threats. When a breach happens or an attack is transpiring, response time is critical as is knowing how to respond. We know and treat your network like our own and this allows us to orchestrate a rapid, coordinated, and effective response to threats ensuring your business thrives and your people are better protected.

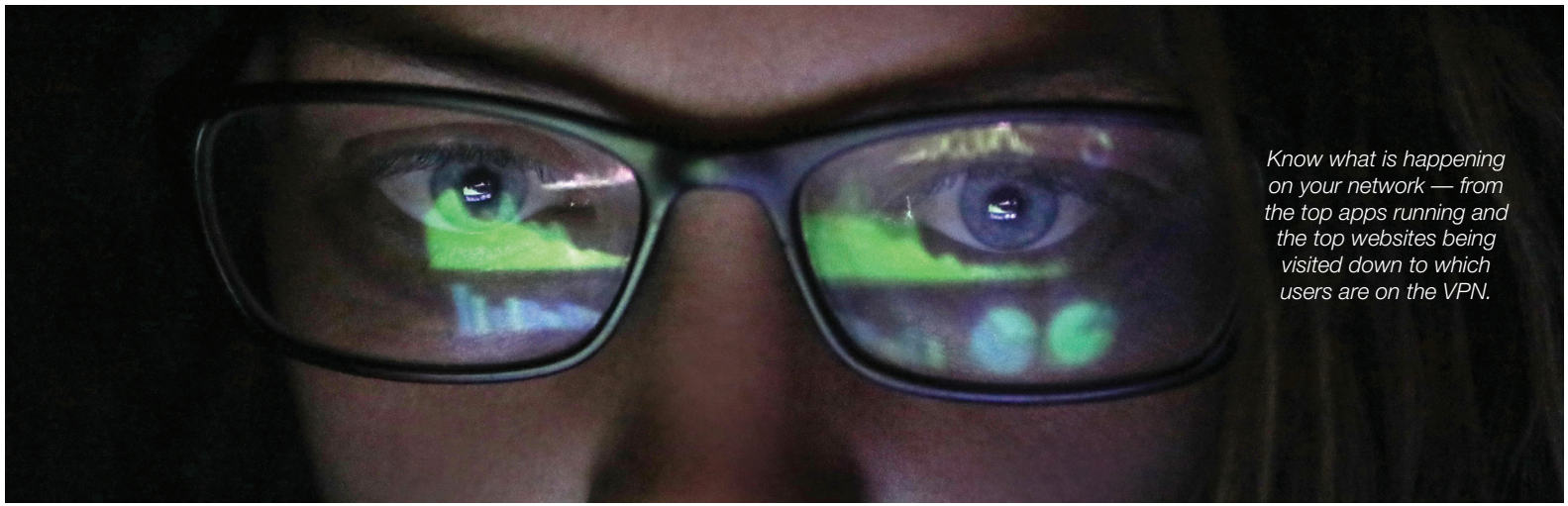
Avoid business debilitating threats

Our managed firewall solution will help you:

- Fortify your security posture
- Limit downtime due to network outages or crippling cyber attacks
- Meet your compliance challenges
- Free up resources to focus on business-driving initiatives
- Enable productivity with safe, secure, high-performance communications with partners, suppliers, customers, and remote employees
- Realize immediate value of your security investment



Organizations that contained a breach in under 30 days saved more than $1 million compared to those who took longer.



Know what is happening on your network — from the top apps running and the top websites being visited down to which users are on the VPN.

Protect investments

We ensure businesses realize the full value of their firewall investments and we help protect their critical assets by providing:

- Dedicated US-based security professionals
- 24/7 health monitoring and troubleshooting
- Customized device configuration and tuning
- Updates and patch management
- Log retention and reporting
- Licensing
- Hardware assurance
- Configuration backup and storage

HIPAA and PCI Compliant

Our people and processes undergo the scrutiny of third-party audits to ensure we meet and exceed HIPAA and PCI industry standards.

Solution features include:

- Managed detection and response
- Threat intelligence
- Sandboxing
- Vulnerability scans
- SD-WAN
- Anti-virus
- Web filtering
- Application control
- Intrusion prevention
- SSL deep packet inspection
- Web application firewall
- Data leak prevention
- Traffic shaping
- Policy scheduling
- Site to site IPsec
- Active directory integration
- VPNs with 2-factor authentication
- 5G / 4G failover
- Third-party access vendor support
- Wireless access point and switch integration and management

For SMBs, the average cost of downtime in 2019 was $141,000.

TPx has a group of highly trained security professionals based in two US-based Security Operations Centers.

Our people and processes undergo the scrutiny of third-party audits to ensure we meet and exceed HIPAA and PCI industry standards.

Service Descriptions

MSx Firewalls

All base administrative features available for MSx Firewalls are supported in all the service tiers. The on-boarding and implementation process for all service levels are identical. The difference between the service levels lies in how the changes to the equipment profile are managed, feature availability, and the amount of monitoring provided.

MSx Firewalls: Core — Customer Administrative Responsibility
MSx Firewalls: Optimum & Secure — TPx Administrative Responsibility
MSx Firewalls: Optimum & Secure — TPx and Customer Shared Administrative Responsibility

Service Features	Core	Optimum	Secure
24/7/365 Support Center	■	■	■
Base Administrative Features			
PCI and HIPAA Compliance	■	■	■
24/7 Firewall Monitoring		■	■
(Product) Licensing	■	■	■
Mgmt of Manufacturer Support/Response	+	■	■
Hardware Assurance/Equipment RMA	+	■	■
Configuration Management	+	■	■
Firewall Configuration Backup and Storage		■	■
Troubleshooting	+	■	■
Firmware Research and Upgrades	+	■	■
Firewall Vulnerability Patching	+	■	■
Log Retention	40 days Upgrade available	120 days Upgrade available	365 days
Reporting	+	All template reports	Custom reports
Firewall Access	Read/ write	Default read only	Default read only
Solution Features			
SD-WAN	+	■	■
Gateway Anti-Virus	+	■	■
Web Filtering	+	■	■
Application Control	+	■	■
Intrusion Prevention (IDS/IPS)	+	■	■
SSL Deep Packet Inspection		■	■
Traffic Shaping	+	■	■

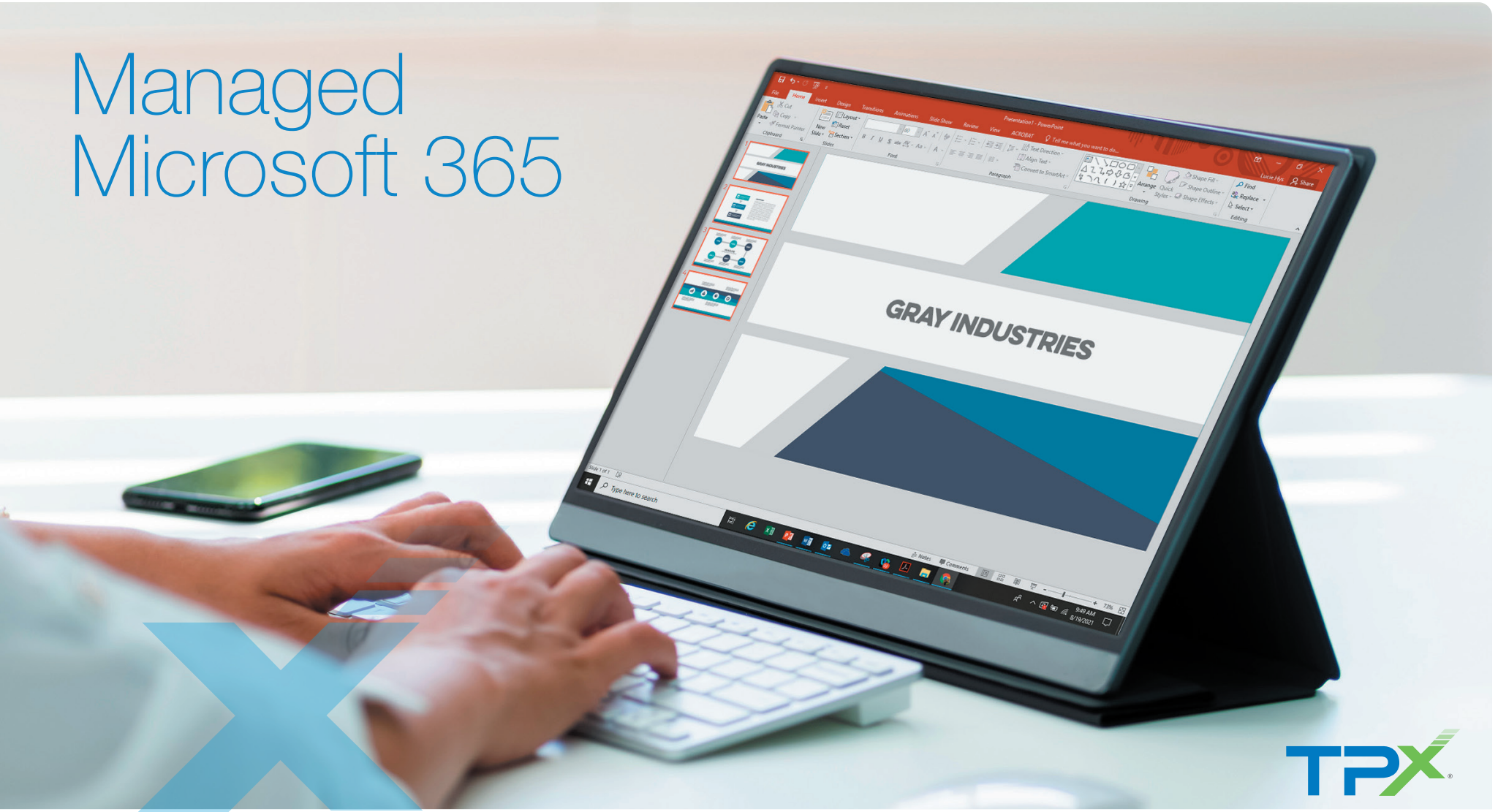
Solution Features (cont.)	Core	Optimum	Secure
Policy Scheduling	+	■	■
Site-to-Site IPsec VPN Tunnels	Limit 5	■	■
SSL-VPN for Remote Users	Limit 20 No Limit with AD	Limit 20 No Limit with AD	Limit 20 No Limit with AD
Routing	+	■	■
Single Sign On	+	■	■
Portal	■	■	■
Managed Detection Response — SOC Active Log Monitoring	□	n/a	■
Threat Intelligence	n/a	n/a	■
Data Leak Prevention (DLP)	n/a	n/a	■
Sandboxing	□	n/a	■
Monthly Vulnerability Scan	□	□	■
Web Application Firewall	n/a	n/a	■
Add-on Features**			
Wireless Access Point (Wi-Fi) Management	□	□	□
Switch Management	□	□	□
Firewall Accessories	□	□	□
High Availability	□	□	□
2-Factor Authentication	□	□	□
5G / 4G Failover	□	□	□
Third Party Vendor Support	□	□	□

■ *Included – monthly cost*
□ *Available – additional cost*
\+ *Included – time & materials cost for post install support*

TPX®

TPX.COM

Managed Microsoft 365



With Microsoft 365, businesses of all sizes can work easier, work together and worry less. And we handle the IT so you don't have to.

Microsoft 365 (formerly Office 365) is a cloud-based platform that provides flexible and familiar tools for collaboration and productivity anytime, anywhere, and from any device. It's specifically designed to help you achieve more with innovative Office apps, intelligent cloud services and world-class security.

TPx delivers Microsoft 365 as a managed service. We help you maximize your investment in Microsoft 365 by working with you to assess your unique requirements, design the right Microsoft solution for your business, efficiently implement service, provide expert ongoing support, and optimize your experience.

Managed Microsoft 365 Features

	Core	Optimum
Assess		
Review your collaboration, productivity, and security requirements	■	■
Evaluate available Microsoft 365 license options	■	■
Design		
Determine the most appropriate Microsoft 365 licenses	■	■
Plan the optimal service configuration to maximize collaboration, productivity and security	■	■
Develop and document the implementation and migration plan	■	■
Implement		
Create new Microsoft 365 Tenant and apply new licensing[1]	■	■
Transfer/Update existing Microsoft licensing and perform a tenant Health Check[2]	■	■
Configure Microsoft 365 tenant and application settings[3]	■	■
Migrate existing users and data[3]	■	■
Implement group permissions, policies, and security settings[3]	■	■
Support		
License billing management	■	■
Technical support management, with escalation to Microsoft for Platform issues	■	■
User administration — moves/adds/changes of users, mailboxes, groups, distribution lists	+	■
Managed Cloud Backup — unlimited cloud backup for Exchange, OneDrive/SharePoint and Teams	+	■
Optimize		
Manage multi-factor authentication	+	■
Manage mail flow and security rules	+	■
Manage policy and alert settings	+	■

[1] New Microsoft 365 tenant creation applies to new Microsoft 365 users.

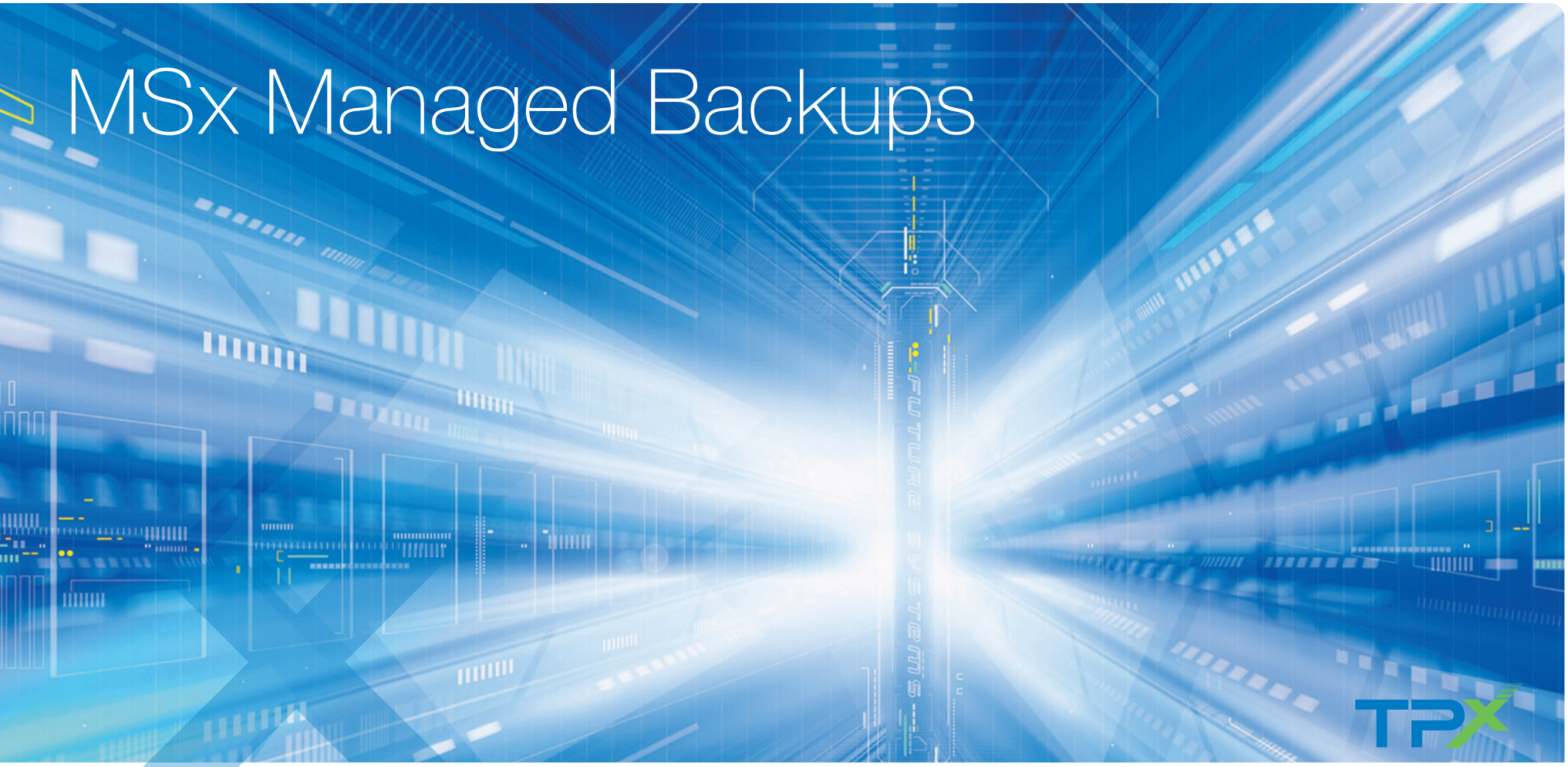
[2] Microsoft 365 tenant and license transfer/update applies to users with Microsoft 365 currently provided by a different partner.

[3] A customized Scope of Work is required. Contact TPx sales for more information on implementation services.

■ *Included: monthly cost*

\+ *Available: time & materials cost*

MSx Managed Backups



With Managed Backups, your data is automatically backed up daily to a secure offsite location and recoverable instantly to any place you need it.

Data backup, recovery and business continuity for local, virtual and cloud environments, within a single platform.

MSx Managed Backups is a fully featured total data protection platform delivered in one integrated package. Easily protect any physical, virtual and cloud infrastructure running on Windows, Mac or Linux, and spin up lost servers in seconds without the need for additional tools. Backup automatically on your schedule to a local device, and replicate backups to the TPx cloud. Recover granular data quickly from multiple points in time, or use local virtualization, TPx Cloud virtualization — or both — to get back to business in minutes.

Backup and restore

In today's world, users lose files by deleting them, overwriting them or when hardware fails. With Managed Backups, simply schedule regular backups for a device. If you need to recover files, a few clicks in the intuitive portal and Backup Insights™ will generate a list of files for comparison between backups. A few more clicks will restore specifically the files you are looking for to the current running device. No more guessing, booting images or digging through command lines. With Managed Backups, restoring files is fast and easy.

Point-in-time rollback is designed to recover from just these scenarios. With the click of a few buttons, it can be as if the ransomware attack never happened.

Disaster recovery and business continuity

When infrastructure fails, business comes to a grinding halt. Replacement hardware takes time to order and install, infrastructure needs to be rebuilt, and backups need to be parsed and applied. This can take hours or days, even with a good backup solution. Unfortunately, when business is down, every second counts. That is why Managed Backups provides image based backups that can be booted directly from the Managed Backups device with the click of a button.

Get more than just one server back up and running; virtualize your entire Infrastructure with the click of a few buttons. Combine local and cloud infrastructure to boot an entire office on the local device or hybrid via the TPx secure cloud, and be back up and running as fast as the images can boot. Once the crisis is past, TPx makes it easy to get back to normal operations.

Ransomware

No matter how hard you try, someone that depends on you for support will eventually get an email that convinces them to open a file and infect their PC with ransomware. The compromised machine will then encrypt user files and demand a ransom for the key to unlock the system. Worse, the threat will often spread across the network and infect other machines, seriously impacting the business. Of course, paying the ransom may not solve the problem. The only sure way to resolve a ransomware attack is to roll back the affected systems to make it as if it never happened. Point-in-time rollback is designed to recover from just these scenarios. With the click of a few buttons, it can be as if the ransomware attack never happened.

FEATURES & BENEFITS

Fast failback Returning to normal operations on a physical server does not have to be a complex and involved process. With Fast Failback, simply provide a new server for failback, create a Bare Metal Restore bootable USB and boot the new server. Updates to the failover VM are automatically applied to the USB image over the network so that when you are ready, failback is a few clicks and a few minutes away.

Agentless and agent-based backup Supports both physical and virtual systems through agentless and agent-based backup. Agentless protection enables fast and easy pairing of any number of VMware systems or templates. Agent-based protection provides scalable backup for your physical device.

Inverse chain technology Eliminates the problem of broken backup chains — the place where most issues arise in the backup process. You have the freedom to change retention and delete recovery points without resetting the chain or having to take a new base image. Since each backup is always in a fully constructed state, and is a fully bootable virtual machine, there is no need for complex, time consuming conversion processes before performing a restore.

End-to-end encryption All data is protected by AES-256 encryption both in transit and in the cloud. Users have the option to encrypt data locally, and passphrases can be specified per appliance or per protected machine.

Advanced screenshot verification After backups are completed, the appliances can be scheduled to boot backups as virtual machines right on the local device. Once they boot, we capture an image of the login page to give you visual proof that your data has been successfully backed up. And what's more, we can ensure your critical applications boot as well.

NAS and iSCSI Provision capacity on the appliance to serve as shared NAS file storage (NFS and CIFS), or as IP block storage with iSCSI. Apply a snapshot schedule and protect in the Cloud.

eDiscovery software Granular Application Search and Restore. eDiscovery gives users the ability to search keywords within their backup data, emails, and attachments and review in an easy to read format. Powered by the industry-leading Kroll Ontrack software, it is compatible with dozens of file formats and systems, including Microsoft Exchange, SharePoint, and SQL.

Backup insights Identify file and application changes between any two backup points, recovering files and applications directly from the interface with almost no information about when they were lost or even where on the machine they resided. Because all backups are fully constructed, in a matter of seconds you can simultaneously mount points and see all files broken down with an easy to read file tree.

Available Features		Core	Optimum
Customer Support Center	TPx will provide remote support for backup-based issues	8am - 8pm ET	24/7
Hybrid On-Premises Backup Device + Cloud Backup Solution	On-premises backup device with replication and recovery to secure cloud environment for Windows, Linux, Mac & VMware systems	■	■
Off-Site Retention of Backups to Cloud Environment	Eliminates the capacity thresholds of an on-site device and allows customers cloud storage options with unlimited amounts of data in the cloud for either a rolling 12-month period or the entire life of the account	■	■
Backup Screenshot Verification	Automated verification of successful backups where backups boot as virtual machines, capturing the login page, to prove your data has been successfully backed up	■	■
Fast Failback Bare Metal Restore	Perform a Bare Metal Restore from the snapshot of the original backup chain, while further backup operations continue	■	■
Disaster Recovery Virtualization	Ability to virtualize backed-up systems from on-premises backup device or from the cloud until on-site resources are restored	■	■
Bandwidth Optimization	Logical full backups only move incremental changes over the network, saving bandwidth utilization	■	■
Device and Cloud Audit Reports	Daily, weekly, and monthly reporting on assets being backed up, backup jobs success or failures, and screenshot backup verifications	■	■
Ongoing Maintenance and Rapid Replace	MSx Support team will update software and facilitate 48-hour replacement of defective hardware under warranty		■
Self-Service Backup Administration	Customer is provided access to the MSx Backups Admin Portal to configure and manage their own backup jobs	■	■
MSx-Managed Backup Administration	MSx Support Team delivers comprehensive management, service administration and change control	+	■
Proactive Monitoring and Reporting for Backup Job Failures	MSx Support Team is notified of backup job failure 15 minutes after first failure. After two consecutive one-hour failures MSx Support will notify customer TPOC.	+	■
Configuration of Backup Jobs	MSx Support Team will configure the backup frequency and retention schedules for local backup jobs as well as replication to the secure cloud environment	+	■

(continued on back)

Available Features (continued)

		Core	Optimum
Configuration of Exchange/SQL Aware Backups	Application aware backups reduce potential for corrupted data on these critical systems	+	■
Configuration of Ransomware Detection	Scan of backups for detection of ransomware via analysis of the backup image	+	■
Reinitiate Backup Jobs in the Event of a Backup Job Failure	MSx Support Team will re-initiate failed backup jobs within 1 hour during business hours. After-hours failures will be re-initiated the following morning	+	■
Recovery of FILE/FOLDER from Backups	MSx Support Team will assist client with single file/folder restoration or complex restoration of directories as needed	+	■
Backup Restore Assistance	MSx Support Team will assist client to deploy backup image in the event of a covered device failure	+	■
Disaster Recovery Virtualization	In the event of a covered device failure, the MSx Support Team will assist client in initiating server virtualization on the on-premises backup appliance or from the secure cloud environment	+	■
On-Site Troubleshooting Assistance	TPx will dispatch a field technician to work on-site, along with the remote MSx Support Team to resolve system issues	+	+

Included — monthly cost ■ Available — time & materials cost +

MSx Datacenter Solutions

TPx operates seven geo-diverse SSAE 18 facilities. Colocation is an efficient, economical way to ensure that your IT systems, applications, and data are available 24/7/365.

SSAE 18 accountability

External auditing provides verifiable peace of mind. TPx's SSAE 18 datacenter designation means our controls, organization structure, administrative processes, environmental security, system backups and system operations have been successfully audited. We undergo annual audits by an independent, nationally recognized firm to assure customer systems and data are protected.

Facility redundancy

Protect your network availability according to leading industry standards. TPx's datacenters are protected with multiple layers of redundancy delivering a high performance tier that ensures mission critical demands. All critical infrastructure — power access, cooling, and data paths — is redundant, operating in parallel, protected configuration

Save on infrastructure

Third party local-loop access is expensive, offers limited capacity, lacks physical diversity, and offers limited scalability. Our datacenters and carrier-grade facilities offer scalable bandwidth solutions that provide increased connectivity at a manageable price point.

Maximize your uptime

Keep your business critical applications accessible. TPx has physically redundant fiber optic network paths from multiple network carriers terminating at our datacenters, which guarantee a minimum of 99.999% network availability.

Meet regulatory compliance

Colocating your IT systems in a TPx datacenter, particularly an SSAE 18 facility, can help your company achieve compliance with Sarbanes/Oxley, HIPAA, FED banking regulations, Payment Card Industry and other stringent standards.

Remote assistance

TPx's Remote Hands service gives you the peace of mind you need when you've colocated your critical data operations. One call or email to our support center gets you connected with a highly skilled technician who will call you, walk over to your equipment and perform these regularly needed tasks:

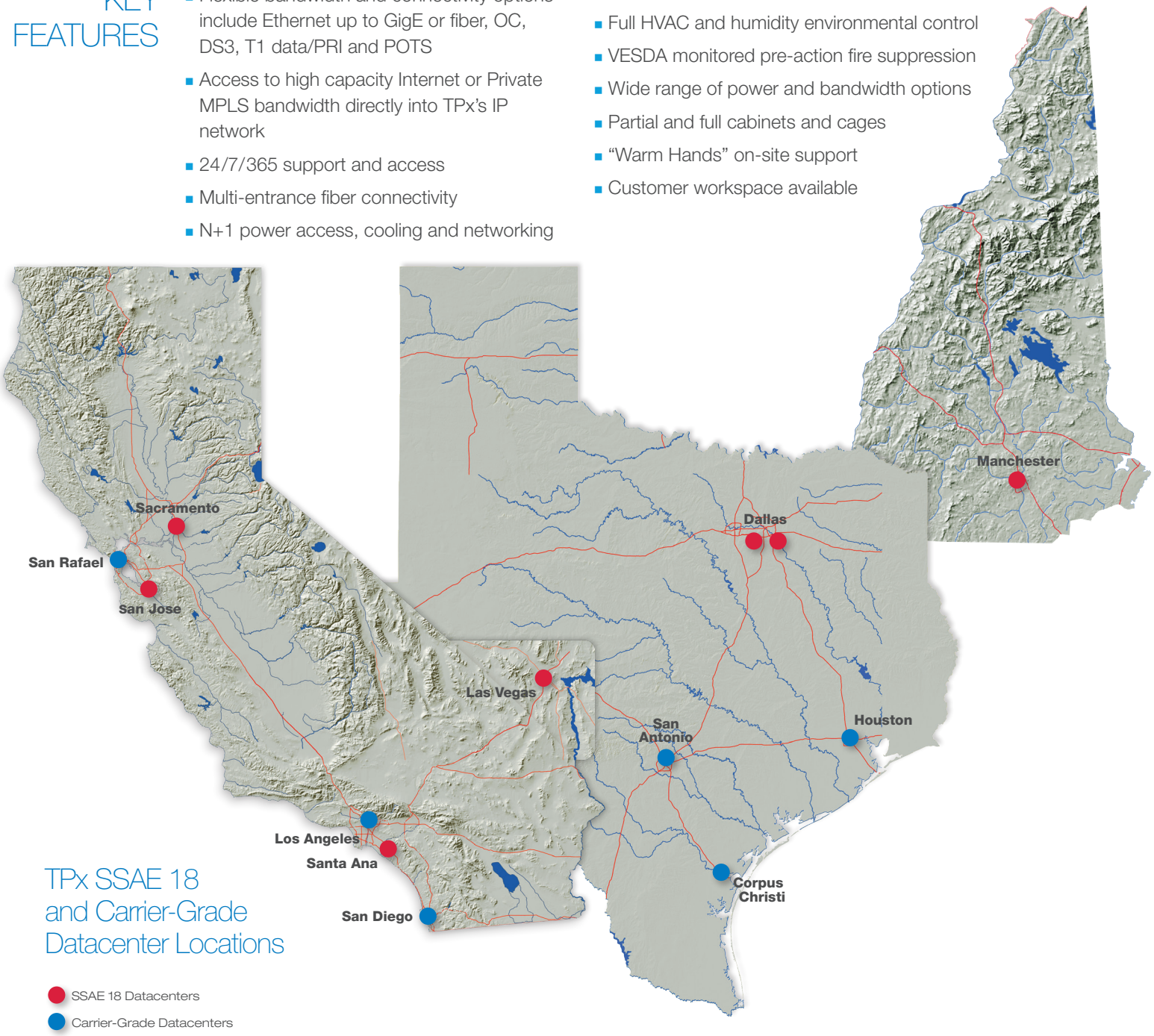
- Visual confirmations
- Reboots
- Basic command programing
- Modular media swaps
- Rack-and-stack
- Establish remote desktop connections, e.g. WebEx/remote access session establishment

Remote Hands service is there for you 24/7/365. We guarantee our rapid response times so you don't have to wonder when you'll get a call that help is at hand.

KEY FEATURES

- Flexible bandwidth and connectivity options include Ethernet up to GigE or fiber, OC, DS3, T1 data/PRI and POTS
- Access to high capacity Internet or Private MPLS bandwidth directly into TPx's IP network
- 24/7/365 support and access
- Multi-entrance fiber connectivity
- N+1 power access, cooling and networking
- Active video surveillance monitoring system
- Full HVAC and humidity environmental control
- VESDA monitored pre-action fire suppression
- Wide range of power and bandwidth options
- Partial and full cabinets and cages
- "Warm Hands" on-site support
- Customer workspace available

TPx SSAE 18 and Carrier-Grade Datacenter Locations



Technology Deployed

24/7/365 Datacenter Management	TPx trained and experienced staff manage the datacenter operations 24/7/365. Staff is also available for local “smart hands” support.	■
Guaranteed 99.99% Network Availability	Physically redundant fiber network paths and a financially backed SLA.	■
Security and Compliance	Continuous endpoint security monitoring and analytics using AI, network analysis, and behavioral analysis to quickly identify and automatically mitigate advanced cyber threats.	■
Geographic Redundancy	TPx operates seven datacenters around the country to provide geographic fault tolerance.	■
Facility Redundancy	All critical infrastructure — power, cooling, and network paths — is redundant to ensure high performance and availability.	■
Customer Workspace Available	Workspace for customers is available in designated areas with our datacenters when disaster strikes your business.	■
Multiple Space Options	Choose from a flexible range of space options from partial racks to full cabinets.	■

Included with service ■

MSx Managed Endpoints

Minimize the risk of downtime and data loss from cyberattacks, system failures, and human error by letting TPx secure and manage your critical systems.

Keeping your organization's servers and workstations healthy, secure, and performing optimally is simply too important to leave to chance. Cybercriminals are launching ever-increasing and more sophisticated attacks against organizations of all sizes, slow and unreliable system performance can frustrate users and cause productivity to suffer, and unplanned downtime can increase costs and impact customer relationships and revenue.

Unfortunately, for most organizations it's a major challenge to maintain the advanced technologies, skilled expertise, and dedicated focus it takes to properly secure and support these critical systems. This puts them at a significant risk.

The MSx Managed Endpoints service from TPx helps organizations of any size solve these challenges by delivering comprehensive IT management and security services that improve system reliability and performance, reduce downtime, increase employee productivity, enforce corporate policy and compliance, and protect against cyberthreats.

Combining sophisticated technology with our expert support personnel and security analysts, as well as proven support methodologies, MSx Managed Endpoints provides an "always on", best-in-class, 24x7x365 service.

FEATURES & OPTIONS

Technology Deployed		Core	Optimum	Secure	Secure Bundle
Remote Monitoring and Management Agent (RMM)	System inventory, comprehensive auditing, real-time monitoring and alerting, flexible reporting, built-in patch management, secure remote control	■	■	■	
Next Generation Anti-virus Agent (NGAV)	Advanced protection against known and unknown viruses and malware	■	■	■	■
Endpoint Detection and Response Agent (EDR)	Continuous endpoint security monitoring and analytics using AI, network analysis, and behavioral analysis to quickly identify and automatically mitigate advanced cyberthreats			■	■
Endpoint DNS Protection Agent	Advanced security for Windows devices by blocking unwanted or dangerous Internet content			■	■
Administrative And Support Services Provided					
24/7 Monitoring and Alerting	Monitoring and alerting for actionable events, key performance metrics, incidents and problems	■	■	■	
Automated Patch Management	Managed remote deployment of performance and reliability patches for Microsoft OS, and select Microsoft and 3rd party applications	■	■	■	
RMM Portal Access	View system audit and inventory, access systems via secure remote control, manage alert notifications, access TPx library of automated procedures	■	■	■	
Scheduled Standard Reporting	Scheduled monthly standard reports delivered via email. Reports include: Executive Summary, Device Health Summary, Hardware Lifecycle, Patch Management Summary	■	■	■	
On-Demand Reporting	Ability to run all available reports on demand	■	■	■	
System Lifecycle Management	Proactive notification of pending hardware and operating system end-of-life, and hardware warranty expirations	■	■	■	
Remote System Administration	Managed, proactive system administration to maintain health and performance of covered systems		■	■	
Remote Troubleshooting and Remediation of Software	24x7 on-demand troubleshooting and remediation of TPx supported operating systems, and select Microsoft and 3rd party applications in response to system alerts or customer requests		■	■	
Remote Troubleshooting and Hardware Ticket Management	24x7 remote troubleshooting of hardware failures and ticket management in conjunction with 3rd party hardware support provider		■	■	
Peripherals Troubleshooting	Remote software and driver troubleshooting for peripherals, including but not limited to monitors, keyboards, mice and printers		■	■	
Security Patch Management	Managed remote deployment of security patches for Microsoft OS, and select Microsoft and 3rd party applications	■	■	■	

Included – monthly cost ■ Available – monthly cost □ Available – time & materials cost +

Security Services Provided		Core	Optimum	Secure	Secure Bundle
Antivirus Software Management	Monitor and manage the installation status and health of TPx integrated next generation antivirus software	■	■	■	■
Endpoint AV/AM Deep Scan Assistance	Assistance running Deep Scan capability of Endpoint Protection Agent for viruses or malware	+	■	■	■
Managed Detection and Response (MDR)	24x7 security monitoring and alerting, automated threat detection and mitigation, advanced threat hunting and mitigation, security incident reporting, scheduled monthly reporting			■	■
Managed Endpoint DNS Protection	Management and configuration of endpoint DNS protection software on supported Windows systems, scheduled DNS protection reports delivered via email			■	■
Security Awareness Training	Monthly phishing simulation emails, monthly online courses covering general security topics, security best practices and regulatory compliance, weekly campaign reports showing results and trending, security awareness posters			■	■
Add-on Services					
Active Directory Server Add-on	Health and performance management/administration of Microsoft Active Directory (per AD server)		□	□	
Remote Desktop Services Add-on	Health and performance management/administration of Microsoft RDS Servers (per RDS server)		□	□	
Microsoft Exchange / SQL Server Add-on	Health and performance management and administration of Microsoft Exchange or SQL Servers (per server)		□	□	
Additional MDR Devices	Managed Detection and Response (MDR) services are included for all devices covered under MSx Endpoints service. Additional devices, such as Linux and MAC devices can be added to the service			□	□
Additional Domains & Email Addresses	Security Awareness Training includes a single domain per account and an email address for all devices covered by MSx Endpoints. Additional domains and email addresses can be added			□	□
Network DNS Protection	Protection at the network gateway to protect any on-network devices that make Internet DNS requests, including non-Windows systems, guest wireless, BYOD and mobile devices			□	□
Endpoint AV/AM Remediation	Research and remediation assistance for virus and malware incidents	+	+	+	+
On-Site Troubleshooting Assistance	Nationwide dispatch of technicians to work on-site with MSx staff remotely	+	+	+	+

** TPx support resources are available 24x7x365 for all service levels by contacting the support center via phone, email, or online ticket*

Included – monthly cost ■ Available – monthly cost □ Available – time & materials cost +

Reduce costs and keep your endpoints running at peak performance so business productivity remains high.

KEY ADMINISTRATIVE & SUPPORT FEATURES

24x7 monitoring and alerting We'll proactively monitor and notify you about your endpoints up/down status, as well as useful metrics such as available drive space, CPU utilization, and memory utilization.

Proactive patch maintenance Consistent and efficient patch management is one of the most important things you can do to keep systems healthy and secure. It's also often overlooked when overburdened IT staffs get busy. Our MSx support team will NEVER overlook this important task. We provide recommended operational and security patches to ensure your systems are up-to-date.

Remote troubleshooting and repair From our 24x7 support center, TPx's team of experts acts as an extension of your IT/helpdesk staff. Using our leading Remote Monitoring and Management software, TPx technicians can securely remote into a supported system to quickly and efficiently diagnose and repair issues.

Hardware support TPx will open and manage tickets on your behalf with your 3rd party hardware support vendor. We'll jointly troubleshoot issues and provide requested diagnostics to the provider so you don't have to. We can also provide post-warranty support contracts.

System lifecycle management You need to know when hardware or software goes End-of-Life (EOL) from the manufacturer. EOL systems can increase your risk of system downtime and your vulnerability to cyberattack because the manufacturer no longer supports or provides patches for these systems. TPx will proactively notify you of EOL events so you have time to plan for replacements.

Comprehensive reporting We'll send scheduled reports each month so that you know your inventory of devices as well as key metrics on their health, such as patch status, anti-virus status, and available drive space. Additional on-demand reports are also available.

KEY SECURITY FEATURES

Next generation anti-virus software We provide leading NGAV software and monitor and manage its status to ensure that it is installed and functioning as intended on all covered systems. We also help with running manual deep scans on-demand.

Security patch management Urgent security patches for Microsoft Operating Systems, and select Microsoft and 3rd party applications will be applied as needed outside of the normal patching schedule to address specific vulnerabilities.

Managed detection and response Even proper patching and the right NGAV solution isn't enough to protect businesses against today's advanced cyberattacks. Our MDR service delivers added protection using sophisticated software that provides automatic threat detection and mitigation. Security Analysts will also monitor your endpoints 24x7 and provide advanced threat hunting and response.

DNS protection We protect systems and users from malicious websites using leading DNS Protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, Guest Wireless, and Non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Security awareness and anti-phishing Users are your last line of defense. The more they know the less prone they are to fall victim to a phishing scam or other security incident. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.

TPX®

TPX.COM

MSx Managed Networks

MSx Managed Networks service helps you increase productivity, lower costs, and remove the complexity of managing your network.

Successful companies need reliable and powerful networks that boost business performance and provide essential security for the entire organization. However, many businesses struggle with network management and security due to lack of time, resources, expertise, and training. Outdated or misconfigured network components can cause bottlenecking as well as costly downtime and open up vulnerabilities for hackers.

A solution to common struggles

MSx Managed Networks service combines human expertise with today's most powerful technology to create a better and more secure user experience across the entire network, allowing businesses to thrive. TPx can complement your team and deliver an end-to-end management of your network infrastructure, giving you peace of mind that comes from knowing you have a reliable, high-performing, modern network backed 24/7 by the experts at TPx.

- Increased performance and productivity
- Security and compliance
- Peace of mind and always on — 24/7/365
- Reduced IT costs
- Simplified management and billing
- Expert network specialists

MSx Managed Networks combines human expertise with today's most powerful technology to create a better and more secure user experience.

Features

MSx Networks provides the components that businesses value:

- 24/7 Monitoring and Alerting
- Troubleshooting
- Configuration Deployment/Management
- Backups/Disaster Recovery
- Firmware Upgrades
- Hardware Assurance
- Licensing/Inventory
- Certified Vendor Expertise from market-leading hardware partners

Benefits

Increased performance and productivity.
A high-performance network helps ensure everyday operations run with better speed and efficiency. Greater network uptime with prioritized traffic and reduced IT costs means employees are more productive and can spend more time on strategic business goals.

Security and compliance Our security experts provide a properly designed and configured network, allowing you to take advantage of secured encrypted traffic and network segmentation, making your business less prone to cyber attacks. TPx can help you with your compliance needs as well.

Peace of mind and always-on — 24/7/365 A network slowdown or outage can stop a business in its tracks. TPx monitors your network equipment 24/7/365 to make sure it is running properly and troubleshoots and resolves issues quickly, even overnight.

Reduced IT costs No need to hire expensive and hard-to-find IT professionals you have to continuously invest in, so that they stay current on the newest technologies — only to have them leave. TPx augments your existing IT staff for a fraction of the cost and frees them up to focus on revenue-generating projects instead.

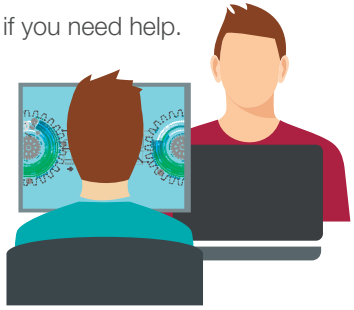
Simplified management and billing All of your IT issues and billing across multiple sites, multiple ISPs and multiple devices is handled with a single phone call or email and a single bill. Replace that costly legacy MPLS network with secure networking devices managed by TPx.

Expert network specialists Finding and hiring a staff of trained and certified network specialists is a challenge for businesses. Because of this, IT staff is often asked to perform a variety of functions from desktop support to network security, which doesn't allow them to focus on any one area. Our Managed Service team is made up of experts in all areas that we support so we can provide the in-depth attention your network systems require.

Multiple Service Levels

You choose the level of support that fits your needs. You can leverage full Optimum support where we handle everything or Core support where TPx configures, deploys, and licenses the solution and you manage it and call us if you need help.

Optimum Support



Core Support

Why TPx?

- We provide a cost-effective, enterprise-grade service
- Our experts become your team members
- Superior support in multiple support centers available 24/7
- Extensive experience — TPx brings its carrier network DNA to your local network
- Every service is customized for the needs of our customers
- Easily turn-on a new service
- Use our superior network or go over the top of any carrier — all with guaranteed performance since we can manage the delivery
- One-stop shop for everything your business needs from internet connectivity to UCaaS to management of all your IT resources

Installation Options

Professional on-site and remote installations options available.

SD-WAN/Firewall

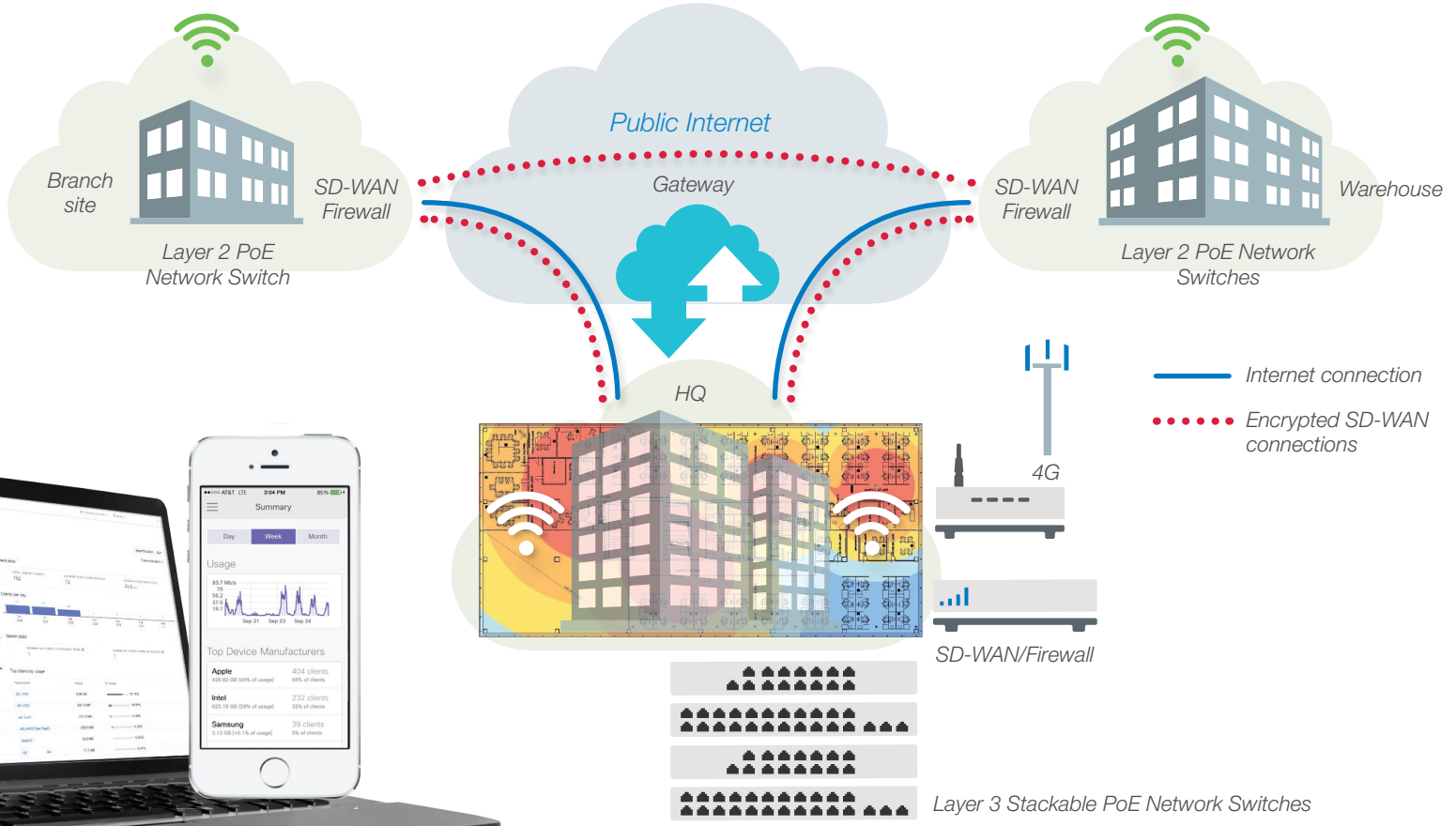
Out-of-date routers, firewalls and expensive legacy MPLS networks can hold back businesses by driving up costs, limiting performance and exposing your network to advanced threats. New software-defined networks (SD-WAN) along with next generation firewalls (NGFW) with advanced security features can combat today's newest threats and provide cost savings by replacing old technologies and providing network visibility and control like never before.

Network Switches

Legacy network switches are often outdated and lack the speed today's businesses need. TPx can help your business with the latest switch technologies, which have advanced troubleshooting and reporting capabilities along with redundant power and stackable features, giving your business the fastest and most reliable network possible and boosting your productivity.

Wireless LAN

With the exponential increase in wireless devices, legacy Wi-Fi networks are struggling to keep pace. A new or updated managed wireless LAN solution from TPx can help increase productivity by allowing your employees to work more freely and on more devices while providing security and control.



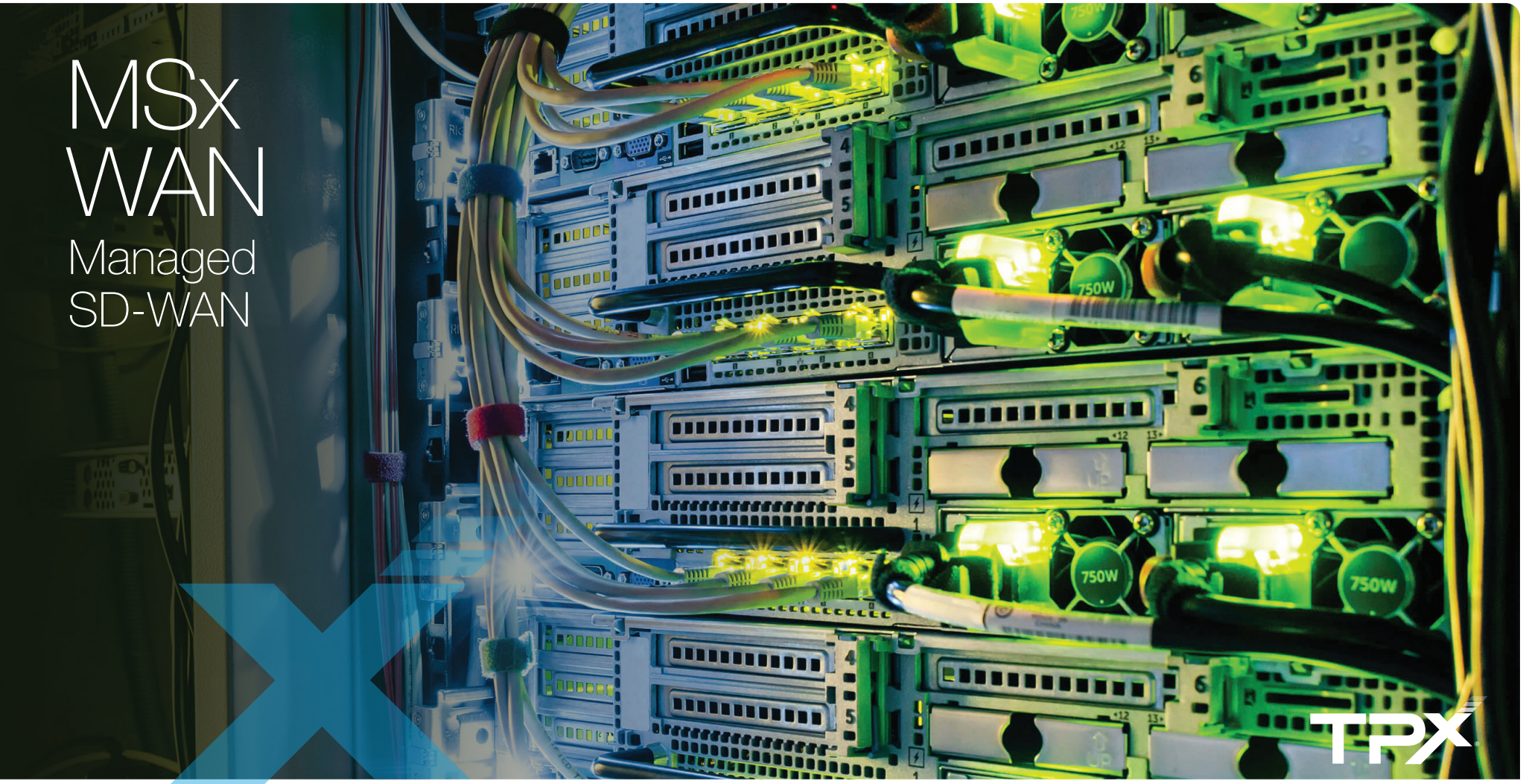
The MSx Networks portal provides status and metrics information for all of your network devices

Available Features		Core	Optimum
24/7/375 Support	Providing anytime remote support	■	■
24x7 Monitoring	Calls to the managed device to determine its status and TPx specialists are informed of availability problems as they develop.In the event an outage has been confirmed, a trouble ticket is created and a specialist will be notified to begin troubleshooting. The status of all system health tickets will be available through TPx ticketing system (DASH). All support SLAs are per the MSx Services Addendum. Customer may rbe esponsible for hosting a small monitoring agent on their network.		■
Configuration Management	Customer may submit change requests via telephone, email or TPx ticketing system. All change requests will be verified to ensure only authorized contacts requests are implemented and the identity of the authorized contact is verified. Change SLAs are per the MSx Services Addendum	+	■
Configuration Backup	Maintaining a current hardware config for the managed device	■	■
Firmware Research and Upgrades	Firmware is researched for standard implementations, approved and deployed at predetermined maintenance windows as agreed to with a customer to address concerns or to enable new features	+	■
Hardware Assurance/Equipment	Replacement of TPx provided device in the event of equipment failure. Assist customers with equipment replacement if the customer has provided their own equipment and there is a current support contract. Not responsible for equipment replacement on customer-provided equipment with no support contract.	■	■
Troubleshooting	Troubleshooting and remediation of network issues related to the alerting or configuration of the managed equipment	+	■
Product) Licensing	Maintain the support/service licensing for the managed equipment for the duration of the customer's service contract. Additional service options for licenses may be available for an additional charge. If a customer is providing their own hardware, they may decline this licensing feature as part of their service and TPx will no longer be responsible for licensing including license renewals. Failure to properly renew a license may result in a service disruption.	■	■
Administrative Portal	Provide access to the device's management portal where the customer may view key information about the performance of their device	■	■
Device Reporting	Available summary reports sent to the customer upon request	+	
DASH Portal	Access to the TPx DASH portal provides the customer with the ability to open tickets and see the status of tickets	■	■

Included — monthly cost ■ Available — time & materials cost +

MSx WAN

Managed SD-WAN



Guaranteed performance over the cloud without headaches like multiple provider footprints, complex routing, skyrocketing expense, and connectivity or redundancy limitations.

Congratulations! You've added new locations and now look to grow on a regional and national stage. Your business is expanding — but can your network keep up?

With MSx WAN, you can count on guaranteed performance delivered over the cloud that creates seamless enterprise connectedness.

We'll take deployment headaches like multiple provider footprints, complex routing, skyrocketing expense and limited connectivity and redundancy options off your desk.

Migraine-inducing spotty Internet performance, inflexible static architecture and slow response times for critical apps can be distant memories. Distance, network hops, slow run times and bandwidth issues can go away.

The business map today reflects the greatly expanded, increasingly complicated world out there — and that presents challenges and opportunities that demand new tools, responses and approaches. MSx Managed SD-WAN gives you the resources you need to successfully navigate it, prosper and grow.

SD-WAN is game-changing technology

MSx WAN uses our state-of-the-art managed platform to deliver three key advantages that make your life less stressful:

Assured application performance Transport-independent performance leverages economical bandwidth and enables Internet as enterprise grade WAN (Over-the-Top or OTT)

Business policy automation Simplified IT operation, zero-touch deployments and one-click service insertion

End-to-end management Direct cloud access with performance, reliability and security enable powerful end-to-end management

FEATURES & BENEFITS

Any transport MSx WAN supports all Internet transport options (EoX, Fixed Wireless, TDM, DSL/cable, and 4G LTE)

MPLS Integrates IPVPN and MPLS into a single private network. This includes both TPx MPLS, ①Net, and third party MPLS solutions

Any network Flexibility to leverage any Internet access regardless of service provider

Nationwide availability Option to "Bring your own Bandwidth" allows for national off-net connectivity

Flexible bandwidth options Upgrade and downgrade bandwidth service licenses whenever you choose, at a prorated rate and no term renewal. (Equipment must support the allotted bandwidth.)

Quality performance We provide QoS over any network — no "best effort" here

Secure connectivity MPLS traffic encrypted with VPN access to our MPLS network

Cloud VPN Dynamic edge-to edge communication via IPSec VPN connectivity

Active-active Leverage the total bandwidth of dual Internet connections

Flexible continuity options Failover options in the event of an unplanned circuit outage is bi-directional; both circuits back up each other

Inbound continuity Provides static public IPs between core network and gateway so internal devices can always be reached by remote users

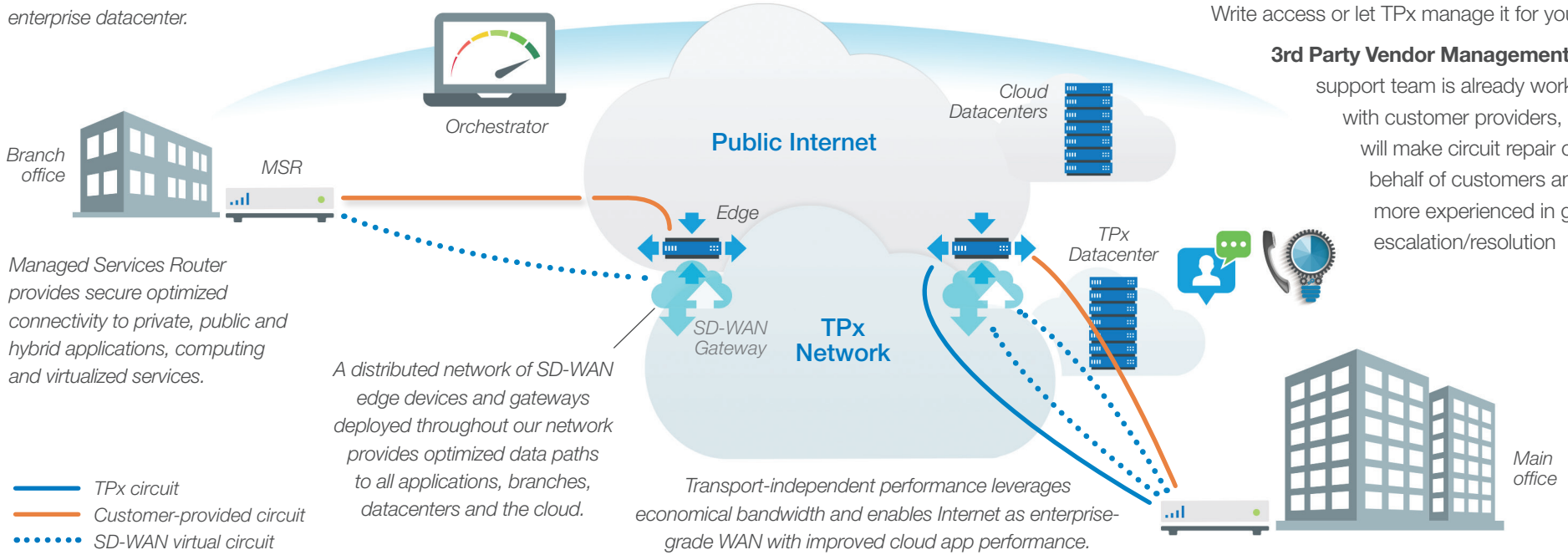
Application Aware/Smart QoS Customized prioritization of key application data traffic

WAN optimization Forward error correction and Unity Boost improve circuit performance, reducing jitter, packet loss, and latency of apps

Orchestrator Read/Write Access Self-manage your SD-WAN orchestrator with Read/Write access or let TPx manage it for you

3rd Party Vendor Management Our support team is already working with customer providers, so they will make circuit repair calls on behalf of customers and are more experienced in getting escalation/resolution

Centralized installation, configuration and monitoring software orchestrates the data flow through the cloud network. It enables one-click provisioning of virtual services in the branch, the cloud, or the enterprise datacenter.



Managed Services Router provides secure optimized connectivity to private, public and hybrid applications, computing and virtualized services.

A distributed network of SD-WAN edge devices and gateways deployed throughout our network provides optimized data paths to all applications, branches, datacenters and the cloud.

Transport-independent performance leverages economical bandwidth and enables Internet as enterprise-grade WAN with improved cloud app performance.

MSx WAN USE CASES

Custom Profiles

A TPx Managed Services Router (MSR) enables your most critical applications, using smart control customer profiles that take the load off of your IT department. Out-of-the-box defaults set the Quality of Service (QoS) policies for common business objectives so IT simply has to establish traffic priority. Knowledge of application profile enables automation of QoS configurations and bandwidth allocations.

UCx/SIP Over the Top (OTT)

Get our UCx Unified Communications and SmartVoice SIP trunking solutions coast-to-coast anywhere there's a broadband connection. All voice traffic has a high priority policy so that it doesn't compete with public Internet traffic. The circuit may not be TPx, but the Managed Services Router, UCx and SmartVoice are — and we guarantee our performance.

Hybrid WAN

Our customers depend on us to provide them with secure, reliable VPNs leveraging an MPLS network. Expand your networking options with a hybrid private network by adding to or replacing expensive T1s with a low-cost, high-bandwidth Internet connection on your existing MPLS network. The resulting solution enables superior customer engagement and end-user experience while removing geographic barriers coast to coast. And you'll have the ideal foundation for future SD-WAN solutions as your needs and applications evolve.

WAN Optimization

WAN connections don't always perform as we expect. When performance degrades there is a hit to your productivity and revenue streams. We can help make sure your connections are optimized by maximizing the efficiency of data flow across your WAN. SD-WAN technology allows the MSR at your site to mitigate packet loss and latency to the managed services network and helps increase the speed and quality of access to critical apps and information.

Multi-circuit Connectivity/Continuity

Mix and match any type of transport provided by TPx or your local Internet or wireless provider to securely and seamlessly fail over to any or all of our core services — MPLS, DIA, SmartVoice, and UCx.

Two Circuits In this setup, both connections, are in active/active mode. That means that the MSR decides, for each traffic session, which path is the best path in that moment. You do not need to feel like you are paying for bandwidth you aren't using.

Three Circuits For added peace of mind, you can utilize three circuits — all active or one in standby mode — for the ultimate measure of connection certainty.

4G LTE TPx is the first to offer SD-WAN over 4G LTE as primary, secondary and redundant options to reduce or eliminate the need for wireline connectivity. In primary configuration, all traffic SD-WAN is transported over the 4G network. In secondary mode, the 4G circuit is active but sharing throughput with a primary wired circuit. In failover mode, the 4G link is dormant until needed for automated failover of the primary circuit.

Inbound continuity This provides static public IPs between core network and gateway to support inbound Internet failover for remote users and web traffic. Without it, inbound traffic is limited to one circuit, which means that if it goes down, external sources can't reach the site or VPN.

Our managed services architects will work with you to build a customized solution

Your WAN can become a symphony of private network and OTT Internet connectivity.

Managed Services Routers (MSR) performs deep application recognition, app/packet steering, and performance metrics to deliver end-to-end QoS.

WHY TPx

We're implementing MSx WAN so that you can stay ahead of evolving next-gen networks and take full advantage of the latest SD-WAN technology.

- Easily turn on new service
- Enjoy even better customer support
- Have increased application awareness
- Use whatever transport makes the most sense for your enterprise

Network flexibility

- Use our superior network or go over the top of any carrier — all with guaranteed performance since we manage the delivery
- We prioritize the cloud traffic according to your business priorities
- UCx and SmartVoice are always high priority
- Adjust bandwidth capacity seasonally with our flexible bandwidth option

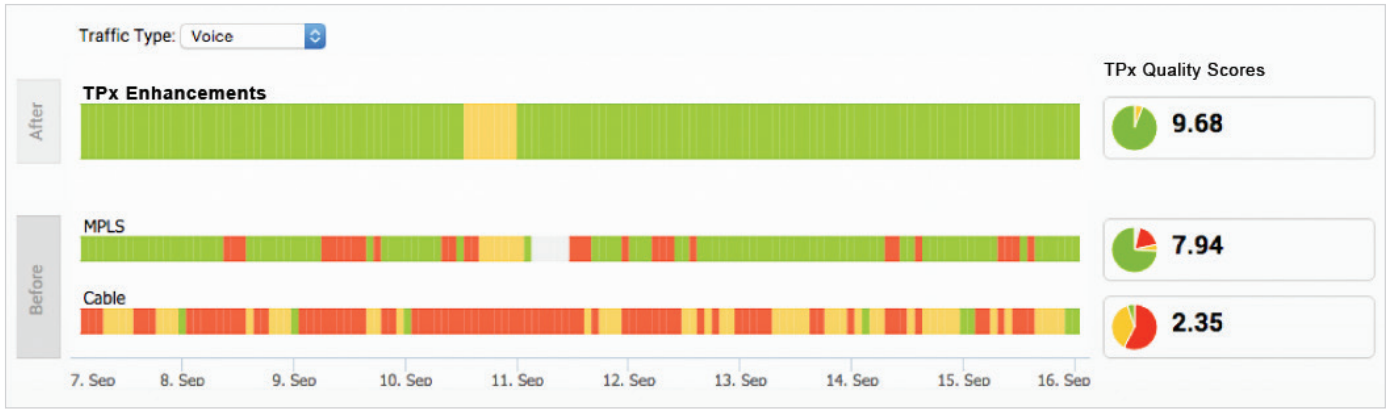
Continuity service options

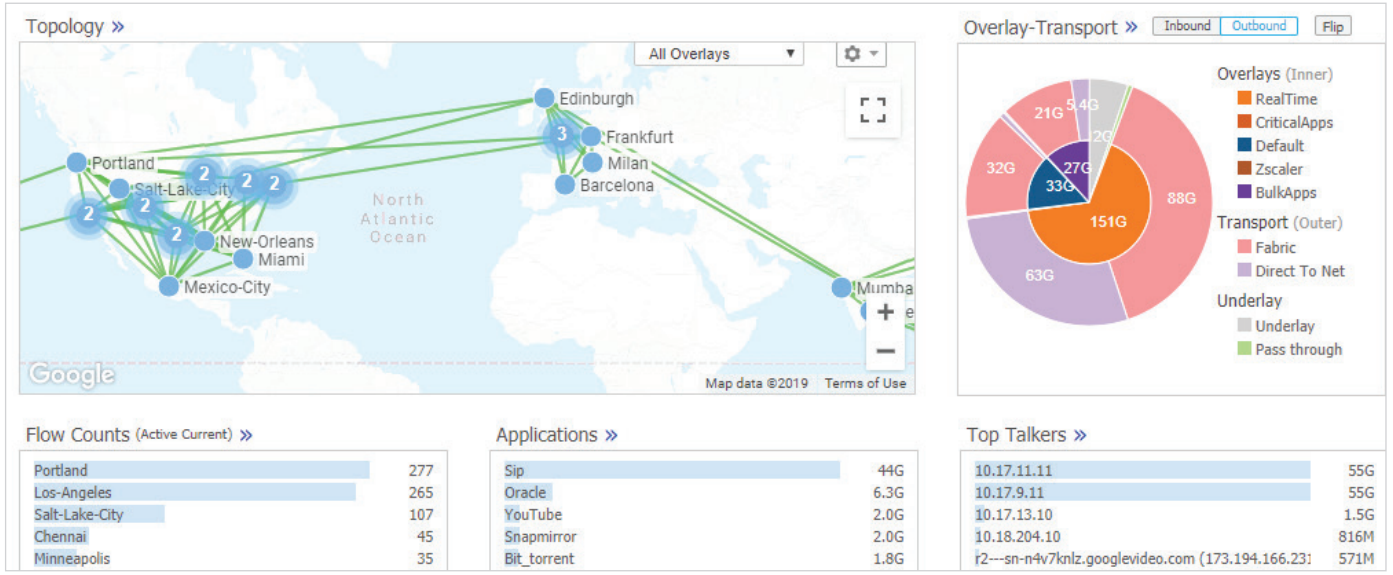
- Seamless failover/continuity
- Active/active circuit design
- Active 4G LTE primary or secondary line
- Inbound continuity
- MPLS, Internet, and voice

Managed services experience

- We *know* networks
- We *know* continuity
- We *know* customer service
- Third-party vendor support
- Smoother implementation
- Much faster trouble ticket resolution

MSx WAN provides optimized data paths across multiple active-active transport options through forward error correction and packet steering to maximize end-to-end quality of service.





Performance monitoring can uncover utilization and throughput issues by tracking application usage and identifying traffic spikes with specific apps.

111120

Service Availability		Core	Optimum
Worldwide 24/7/365 Support		■	■
Administrative Services			
Multi Services Router (MSR) Monitoring & Alerting	Utilizes a two minute threshold, that alerts on MSR(s) down status	■	■
VPN Tunnels Monitoring & Alerting	Utilizes a two minute threshold, that alerts on Links down supported by the MSR	■	■
CPC/OTT Monitoring and Alerting	Notification to let customer know that the WAN interface is unavailable and the customer needs to contact their Internet provider	■	■
Hardware Assurance/Equipment RMA	In the event of an equipment failure, TPx will manage the replacement of the MSR.	■	■
Configuration Management	TPx will respond to customer's requests to make configuration changes	■	■
Features			
Compliance	TPx's SD-WAN solution is PCI and HIPPA complaint	■	■
Physical and Virtual MSR options		■	■
Static routes or dynamic routing protocols such as BGP and OSPF supported		■	■
Orchestrator Access	– Review up/down status of each connection and MSR – Connection overview that shows bandwidth statistics – Quality of Experience (QoE): Voice, Video, and transactional – Monitor WAN connections and total packets received/sent, utilization, jitter, and latency – Monitor network usage of application, app categories, devices, and operation systems – Monitor network usage data of the destinations of the network traffic – Monitor business policy characteristics according to the priority and the associated network usage data for a specific MSR	■	■
Multiple circuit design options	Active-Active…Active-Active Standby…Active-Active-Active … Active-Active-Active/Standby	■	■
MPLS Integration		■	■
Routing Policies		■	■
Two-Factor Authentication		■	■

Available Features		Core	Optimum
Third Party Vendor Support	TPx will submit trouble tickets to a customer's third party Internet provider on their behalf when the OTT connection becomes unavailable. The vendor will provide a LOA that they have our mutual customer sign that authorizes us to work with the vendor on the customer's behalf.	■	■
High Availability	High availability utilizes two MSRs with mirror configurations to provide redundancy	■	■
Clustering	Clustering provides horizontal scalability for throughput and tunnel scale, by clustering multiple MSRs. MSR clustering also provides resiliency via the Active/Active High Availability (HA) topology that a cluster of SD-WAN MSRs would provide.	■	■
TPx-provided 4G Connectivity		■	■
Inbound Internet Failover Public IPs		■	■
Nonstandard MSx WAN IPSec Tunnels	VPN tunnel configurations to access one or more non-VeloCloud sites	■	■
Boost	Significantly improves application response times across the WAN	■	■
Installation Options			
Remote Installation	The pre-configured MSR will be shipped at the specified customer location	■	■
Professional Installation	TPx Technicians will assist with your service installation. If you choose to use TPx Professional Services for your installation we will preschedule a time for a Qualified Professional to arrive at your install address.	■	■
Expedited Implementation	An expedited MSx Managed SD-WAN project is based on a twenty-one business day schedule, versus 45 days	■	■

UCx with Webex

Transform the way you work.

UCx with Webex transforms the way employees work with a single solution that includes video meetings, whiteboarding, secure messaging, file sharing, built-in call control functionality and more to increase employee productivity and streamline teamwork.

UCX WITH WEBEX

Collaboration

Enhanced team collaboration tools enable everyone to see and share all the information they need to work together productively.

Messaging

Exchange secure messages and share files with individuals and groups, inside or outside your organization.

Meetings

Host large and small meetings from anywhere, with audio, video and screen sharing.

Enterprise VoIP

Make, receive and manage calls on any device, anywhere.

THE BENEFITS OF UCx WITH WEBEX

Dozens of features in one app

How many apps do you have for video, phone calling, call center, messaging, and meetings? Now you can get them all in one app. One platform means fewer headaches and less money.

Use the tools you like most

UCx plays well with others. There are plenty of pre-built integrations available for third-party applications from Google, Salesforce, Microsoft and more. You can even find and implement bots that will help enhance your conferencing and workflow experiences.

Integrated calling and call control

UCx includes native video and voice calling and extensive calling features and call control within a single collaboration app. You can make or receive calls from anywhere with VoIP calling via desk phone or mobile We back all of this up with an industry-best 100% voice network uptime guarantee.

Business continuity

The distributed nature of UCx means that your infrastructure will still be available in the event of a power outage, storm, fire, or other disaster. Because UCx resides on the TPx network and not on your premises, it's easy to redirect calls to an alternate location or device if you can no longer take calls at your primary location.

Enhanced teamwork and collaboration

Since UCx integrates many powerful features into a single application, your teams can collaborate with others internally and externally faster and easier than ever before.

Custom design around our teams

High-quality video meetings, annotation-rich screen sharing, and whiteboarding are all available to access from any device with UCx. Anyone can start a conference and access in-meeting tools like the ability to add guests or record conversations. There's also the option to save all your files and whiteboards for viewing later. You can even work offline.

Enterprise-grade security and compliance

UCx keeps your meetings and conversations secure with enterprise-grade safety, including end-to-end encryption, built into everything you do. UCx has achieved HIPAA compliance and we'll sign a Business Associate Agreement (BAA) for you.

Future-proof

An easy evolution to cutting-edge communication and collaboration services. Because UCx is a hosted service, you'll always have immediate access to new features and updates as soon as they become available, without having to do anything.

CAPABILITIES

Collaboration

Spaces and teams Create dedicated Spaces and teams to stay organized with people and subjects that are relevant to you.

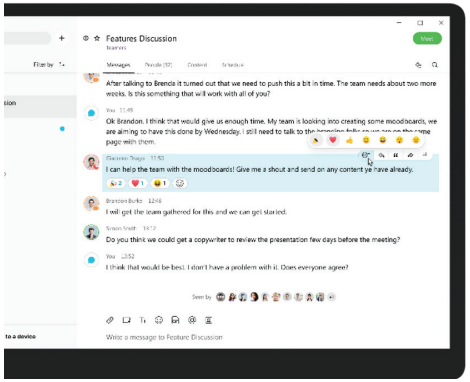
File sharing Simply drag and drop files within messages or in a team Space where they are neatly organized, searchable, and saved.

Whiteboarding Quickly and easily create a quick sketch on the whiteboard to share your ideas.

Powerful search Easily search across Spaces, people, messages, and files to find what you need, when you need it.

Application integration Pre-built solutions with third-party applications from vendors such as Microsoft, Google, and Salesforce deliver a complete collaboration experience

External collaboration Communicate with external people, such as vendors or customers, by inviting them to collaborate with you in your meeting room



Messaging

Direct chat and group chats Secure and easy-to-use messaging at your fingertips for instant message exchange

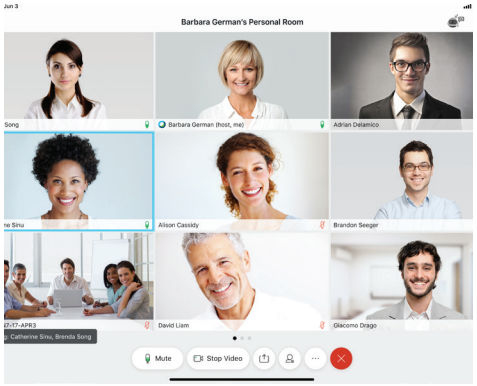
Messaging capabilities Enjoy extra flexibility with your chat messages — deleting, forwarding, flagging for follow-up, quoting, reactions, and threading

History Everything is saved so you never lose track of your chats — and they are safely archived

Notifications Minimize distractions without missing critical updates by customizing your notifications so you only receive alerts that matter to you

Presence status Stay in the know on your colleagues' availability, removing the guesswork from when to reach out

Offline messaging Always stay productive with the ability to view your messages and listen to voicemails when you're offline



Meetings

Personal meeting room Enjoy your own private and secure online meeting room with a dedicated phone number for teams up to 1000 participants

Screen sharing Share your entire screen or a specific app or document, without additional downloads or separate web collaboration apps.

In-meeting chat During meetings, desktop and mobile participants can chat with one another to increase meeting effectiveness

Guest collaboration Invite external people to join you in a multimedia collaboration session

Recordings Record meetings and share recordings for those who couldn't attend

Presenter controls Manage the meeting the way you want with administrative controls

Enterprise VoIP

One number Publish one business phone number and all your business calls will go to the device of your choice.

VoIP Place and receive business calls on the mobile app using Voice over IP (VoIP) and the cellular network, or via Wi-Fi network, using your business phone number.

Robust phone calling No matter where, you can always be available. Route inbound calls, queue multiple calls, and work remotely to ensure productivity and happy customers.

CRM integrations For call center agents, receptionists, or sales, UCx CRM integrates with hundreds of common applications including Salesforce, Netsuite and Zoho.

IP phones We offer phones from industry leaders Poly and Cisco. All phones are high definition, preconfigured, and customizable. Our team will work with you to find the best phone solution to meet your business needs.

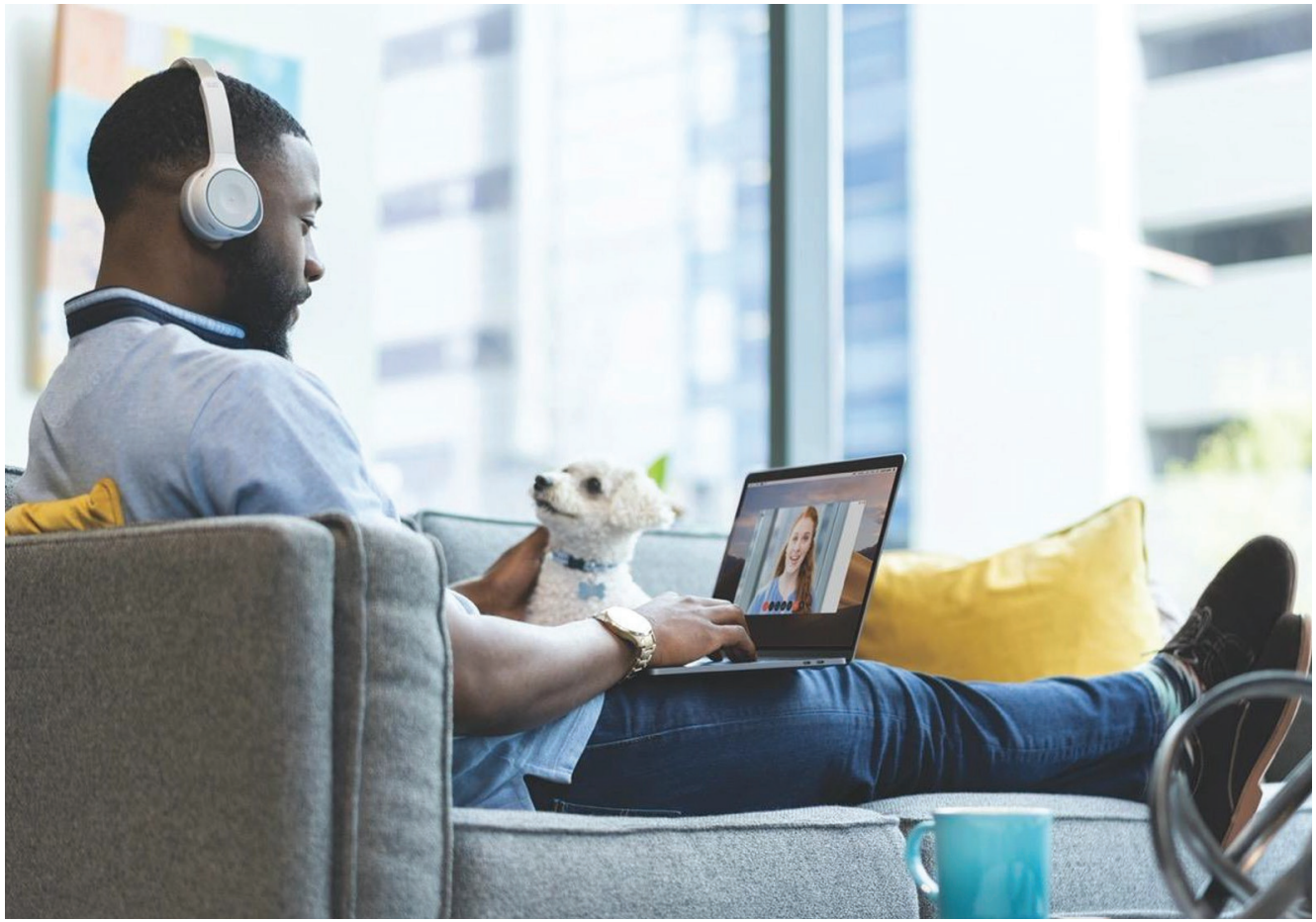
WHY TPx

Managed IT Service Enhance your IT support for security, performance and peace of mind. MSx Managed IT Services give you the support you need for your critical IT systems, including managed security, networks and backups, without the cost and hassle of doing it in-house.

Managed Connectivity Can your Internet connection support HD voice and video without sacrificing quality or reliability? The answer is a resounding yes when you're a TPx customer. TPx offers multiple connectivity options to help you find your ideal combination of speed, flexibility, and cost to meet your increasing internet needs.

Customized Planning and Implementation We have the tools and support to deliver professional services including Solutions Architects for customized planning, a dedicated project manager assigned to you and training resources to get you and your team up and running and collaborating.

Experience and Support TPx is the nation's leading managed services provider with over two decades managing networks. We offer superb reliability, back by a 100% SLA and 24/7/365 access to experienced support professionals.



SEAT OPTIONS

We know one size does not fit all. With five UCx seat options, enjoy the choice of a mix of user configurations tailored to the unique needs of each employee, while improving overall product adoption and managing costs.

Voice	**Business** *(add…)*	**Pro** *(add…)*	**Elite** *(add…)*	**Call Center** *(add…)*
Enterprise VoIP calling	Softphone	Personal room (100 capacity)	Personal room (1000 cap.)	Inbound ACD
Individual/group calling features	Instant messaging & presence	Desktop sharing	Meeting recording	Inbound queues
	Direct & group messaging	Application sharing	Remote desktop control	Outbound call center
	Spaces & Teams		Presenter controls	Reporting calling features
	Host 25-person Space mtgs		Recording transcription	
	Screen & file sharing			

TPx®

TPX.COM

Cybersecurity Gap Assessment

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Any successful security strategy must be disciplined, thorough, and quantifiable. With an ever-expanding network perimeter, a continuously evolving threat landscape, users demanding access to a myriad of services (both internal and external), and increased scrutiny on risk, privacy, and compliance, a structured approach to organizational security is more important than ever.

TPX's Cybersecurity Gap Assessment enables customers to evaluate their security posture in a methodical way, comparing it against industry standards and best practices, to generate a prioritized list of actions to lower organization risk while maximizing the impact of their limited security budgets.

Get answers to these questions…

- Do I use the best information security practices to protect my business and control my risks?
- Are my systems and data vulnerable to ransomware and other security threats?
- Am I protected against unauthorized access?
- If I do suffer a data breach, am I prepared to recover as quickly, safely, and cost-effectively as possible?
- What most important weaknesses should I fix first?
- What are the efforts needed to improve my current level of protection?

Our Cybersecurity Gap Assessment is founded on common industry standards such as NIST 800-171 as well as current best practices.

Overview

TPx's Cybersecurity Gap Assessment is founded on industry standards such as NIST 800-171 and current best practices. The assessment is divided into two main components:

- **Security Strategy** TPx will assess the security policies, standards and procedures as well as the security management processes, and roles and responsibilities related to your information security.
- **Operational Security** TPx will assess the technical security measures implemented within your network infrastructure.

Your information security posture is assessed based on a set of categorizations (e.g. access controls and network protections). The categorizations covered during the gap assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for your organization.

Gap Assessment Activities

The main objective of the gap assessment is to assess the security maturity of your organization and prioritize security risks for your leadership team. The areas of focus can range from information security governance to cybersecurity infrastructure and capabilities.

Information Security Organization Accountability Information security accountability and compliance, including strategic roles and responsibilities and information security policy

Human Resource Security Management Human resource security management, including information security in hiring, awareness, education and training, and change and termination

Identity and Access Management User access management and password policies

Information Security Incident Management Information security incident management preparation, identification and assessment, response and continuity, and testing

Change Management Change management including planning, building, testing, and implementation

Network Segmentation, Isolation and Protection Network security architecture including segmentation, isolation, firewalls, and threat management

Security Services Core security services including onboarding/offboarding, account and access management, and backup services

Server and Workstations Security Endpoint security including access controls, technical vulnerability management and protections

Email Service Security Email security including architecture, access controls, technical vulnerability management and protections

Reporting

Upon completion, TPx will provide two reports: an Executive Summary and a detailed Best Practices report. They speak to two different levels of resources: the leadership and the security practitioner. A detailed recommendations report will be provided and validated with your personnel in order to present the results and observations related to your security posture. In addition, you will receive recommendations for your top three priorities based on your business, your sensitive data, your exposure landscape, and the CIS top twenty controls.

43% of attacks are aimed at small and medium-sized businesses, but only 14% are prepared to defend themselves.

Accenture 2019 Cost of Cybercrime report

Network Security Assessment
Service Description

Overview

The objective of this Service Description is to provide an overview of the Network Security Assessment activities that are performed under the Service. This framework establishes the purpose, content, and scope of the activities to be performed. Schedule, cost, and other logistics for the Service are contained in a separate Statement of Work document.

Traditional network management has evolved in recent years to the point where it cannot be approached without considering the associated security ramifications. Any attempt to treat security as an "add-on" to network design and operations in today's hyperconnected world is destined to create more problems than it solves. To avoid this, TPx incorporates security considerations throughout its Network Assessment Service, yielding a comprehensive Network Security Assessment that results in actionable recommendations for a robust, high-performing, and secure networking environment.

TPx has defined a network security assessment to assess a Customer's environment per industry standard controls. During the assessment TPx will examine the Customer's strategic and tactical network configuration within a distilled scope that focuses on areas of cybersecurity that have the highest likelihood of incidents and breaches for the Customer's business sector. TPx's methodology is founded on industry standards such as ISO 27001, ISO 27033, CIS "Top Twenty" and current best practices. TPx's network security assessment is designed to evaluate an organization's network, the security posture and functional capabilities.

The assessment will be divided into three phases, covering the following:

- Documentation & Visualization of the existing network environment
- Security Strategy
- Operational Function & Hygiene

Phase 1: Documentation & Visualization

TPx will be inventorying and cataloging the existing network assets and architecture:

Physical Inventory

- Hardware Inventory Spreadsheet
  – Physical Hardware Inventory – Serial Numbers if Possible *review for accuracy
- Layer 1-2 Diagrams/Documentation *will create during the engagement if doesn't exist
  – Physical interconnectivity (including wireless)
- Layer 3 Diagrams/Documentation
  – Routing Connectivity, Gateway Management, Summarization, Route Entrances/Exits *review for accuracy
- Rack Elevation Diagrams/Documentation
  – Physical Rack Diagrams *review for accuracy
- Environmental Capabilities
  – Power, cooling, and cable management *review for accuracy

Design and Architecture Review

- Network Overview Architecture
  – Review for Modularity, scalability, and capabilities
- Traffic Flow
  – Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud

- Services and OLA's
  – High Availability, OLA/SLA if defined
- MPLS/VPN Service
  – Remote Office and Client Access Capabilities
- QOS Standards
  – Deployment methods, OLA's
- Layer 3 Routing
  – Dynamic, optimized, secure
- Layer 2 Optimization
  – Spanning-tree security/optimization, distributed Layer 2

Phase 2: Security Strategy

TPx will be assessing the network policies, standards and procedures as well as all the security management processes, and roles and responsibilities related to the network.

Network Infrastructure Security

- Misconfiguration or Design flaws
  – Firewall Design Review
- Weak authentication or encryption protocols
  – VPN, Wireless, any 802.1x authentication methods
- Centralized Authentication, Authorization, and Accounting
  – AAA Review
- Attack Awareness (IPS/IDS)
  – IPS/IDS design and Log review *if applicable
- Control Plane Policing/Security
  – Infrastructure Device Access, CoPP
- Rogue DHCP/Client Detection
  – Rogue detection both wired and wireless
- Infrastructure Physical Security
  – Cameras, locks, restricted physical access

Performance Monitoring and Analysis

- Netflow Capabilities
  – Bandwidth Planning Capabilities
- Client Experience Capabilities
  – L4-L7 Visibility – Baseline Capabilities
- Packet Capture Capabilities
  – Packet Capture Capabilities

Phase 3: Operational Function & Hygiene

TPx will be assessing the technical measures implemented at Customer's network infrastructure.

Infrastructure Monitoring and Management

- Central Monitoring/Alerting Capabilities
  – Management Platform utilization/capabilities
- Syslog Capabilities
  – Controls, retention, management
- Host End Monitoring/Management
  – Host detection/monitoring
- Software Management (networking)
  – Deployment processes for upgrades/patches
- Configuration validation capabilities
  – Lab Environment
- EoL/EoS hardware and licensing
  – Process for Lifecycle and licensing compliance

Configuration Management

- Centralized Configuration Backup
  – Configuration backups
- Centralized Configuration Automation
  – Configuration change capabilities
- Configuration Change Management Workflow
  – Change Control Management

Controls and Methodology

The expertise of the security team relies upon leading information security practices. Our approach is aligned with the most recent versions of international standards, such as:

- ISO 27001:2013 Information security management requirements
  http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- ISO 27002:2013 Organizational standards and best management practices related to information security
  https://www.iso.org/standard/54533.html
- ISO 27033:2015 Information technology – Security techniques – Network security (sections 1- 7)
  https://www.iso.org/standard/63461.html
- CIS "Top Twenty Controls", Center for Internet Security
  https://www.cisecurity.org/controls/cis-controls-list/

Posture and Profile

The approach for the cybersecurity assessment is to evaluate the Customer's information security posture and profile.

Posture refers to the organization's current capability to protect information and manage associated risks

Profile refers to the minimum target of capability, to protect information and manage associated risks, which an organization should aim to achieve. It is recommended that the organization selects a target profile that is reflective of its security objectives; that is, selecting a target posture (e.g. 'Defined', 'Managed', etc.) for each of the assessed categorizations.

The information security profile accounts for several factors such as an organization's attributes (e.g. size and type of organization compared to similar organizations), business and risk context (e.g. value of critical information assets and expected capabilities/motivations of threat actors) and other relevant variables (e.g. legal, regulatory and service level requirements).

Categories

The organization's information security posture is assessed based on a set of categorizations (e.g. access controls and network protections). The categorizations covered for the gap assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for the organization.

Rating

Information security ratings are evaluated according to the information security approach adopted by the organization. This includes selected controls or solutions, deployment strategy, metrics, system monitoring, organizational plans, and so forth. The ratings are organized into six categories: None, Minimal, Developing, Documented, Managed and Maintaining. Maintaining is the highest rating, which would indicate that an organization is postured for continuous improvement in the rated category. The full list of categories is as follows:

- *Maintaining (5)* Managed information security whereby generated metrics are applied to the performance evaluation and continuous improvement of information security.
- *Managed (4)* Defined information security established that generates relevant, measurable and useful metrics.
- *Documented (3)* Well-established information security requirements, practices, controls and documentation that translate into consistent repeatable and predictable results.
- *Developing (2)* Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.
- *Minimal (1)* Early reactive information security requirements, practices, inadequately controlled and/or documented.
- *None (0)* No information security requirements, practices, controls or documentation.

Workplan

Scope

The main objective of this effort is to assess the Customer's infrastructure adherence to industry standards of ISO 27033. TPx will review the organization through interviews, policy review, validation and investigation of process to provide a prioritized list of risks to the organization. TPx will review the data traversing the network and review the network architecture to the minimally documented schema. TPx will provide a report with business priorities based on the sensitive data of the organization and the operational risk to business sustainability. Based on the findings, TPx will issue an executive summary that makes a statement of the Customer's network security posture. TPx will also detail the results of each best practice assessed, the validation method and risk level to the business. From TPx's report, Customer can build a network architecture program set on controls with the greatest benefit to the security posture and assure that the Customer's limited resources are utilized most effectively.

TPx expects the work to consist of three (3) weeks of effort. The bulk of the assessment will incorporate inventorying the network architecture and hygiene through resource interviews, request of information from the Customer's current MSP (if applicable), review of extant policies (and processes where policies don't exist), and review of system configuration, logs, system playbooks and processes in operations. Additional data may be collected using networking tools to review the type of traffic traversing the network and recommendations to QoS (Quality of Service). Additional effort will be to inventory the wireless network and perform a heatmap/wireless saturation assessment of the physical environment. There may be additional data collation to enable report generation in the form of an Executive Summary, Detailed Statement of Best Practice, wireless network mapping and a graphical depiction of the Customer's network security state by category. Please note, the wireless network mapping is highly dependent on the Customer having physical schematics of the building reviewed. Without the availability of pre-existing documents, TPx will make a best effort to recreate the building layout.

Project Management

TPx will initiate a kickoff meeting where TPx will present the controls for review, identify the key resources to review the controls and build out a schedule for the engagement to review and collect the information to assess the controls. During this meeting, TPx will also set a normal cadence for status and escalation points within the Customer in case the engagement stalls. TPx expects to incorporate eight (8) hours of project management and presenting results of the assessment and findings to the Customer.

Reporting

Upon completion of the assessment, TPx will provide two (2) reports to the Customer: an Executive Summary and a detailed Best Practice report. The reports will speak to two different levels of resources at the Customer: the leadership and the security practitioner.

A detailed recommendations report will be provided and validated with Customer personnel. The objective of this report is to present the results and observations related to Customer's network security posture. In addition, the Customer will receive recommendations by TPx for their top three (3) priorities based on their business, their sensitive data, their exposure landscape and the network state.

TPx will also provide an updated network diagram, wireless saturation for the primary location and recommendations for further documentation that either doesn't exist or which requires updating.

Ransomware Readiness Assessment

Ransomware has become the number one cybersecurity risk in the world. According to the U.S. Department of Justice, there have been an average of 4,000 ransomware attacks every day since 2016. Cybercriminals have turned malware and hacking into a robust, money-driven industry complete with commercial-grade exploit kits widely available to those who seek them. A haphazard approach to online security cannot keep up. New cyberthreats emerge every minute and businesses need to protect themselves against costly security incidents.

Ransomware is especially dangerous for small and medium businesses, many of whom do not have the resources to fend off these attacks. By partnering with TPx's cybersecurity experts, your business can quickly gain rich insights into where you have the most exposure in your business and how you can mitigate yourself against ransomware attacks. Our Ransomware Readiness Assessment can help you identify your organization's weaknesses, and ultimately help save your business money and reputation by giving you a stronger security posture.

Prepare and Respond

- Are my network entry points effectively secured?
- Are my systems properly patched against vulnerabilities?
- Do I have the visibility I need into who is on my network?
- Does my organization's staff know how to avoid security risks in email and other attack vectors?
- Does my backup strategy allow me to recover quickly and minimize downtime?
- Is my incident response plan detailed enough to enable my team to respond effectively in the event of an attack?

Quickly understand your exposure to ransomware attacks — and how to protect yourself. All in a matter of days.

Overview

TPx's Ransomware Readiness Assessment (RRA) is founded on industry standards developed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). This assessment focuses on the aspects of cybersecurity that have the highest value in defending your organization against ransomware attacks. As a subset of TPx's full-blown Security Program Gap Assessment, the RRA provides a cost-effective way for small and medium businesses to understand the risk of ransomware to their organization. It also provides an actionable roadmap that enables these organizations to quickly address their areas of highest exposure, to reduce their ransomware risk.

TPx will assess the security policies and practices surrounding the most common attack vectors that cybercriminals use in ransomware attacks: social engineering, email-based attacks, compromised credentials, and external-facing software vulnerabilities. Through the use of both administrative and technical controls, organizations can reduce their attack surface and encourage cybercriminals to move on to easier targets.

Defense is only part of the story, however. Risk can be reduced, but it can never be eliminated completely. To practice truly effective security, you must be well-prepared to act in the event of a breach. Time is critical during an attack, and it is imperative that your procedures & systems are thoroughly defined and tested. TPx will provide expert advice on the aspects of your incident response plan, your data backup and storage policies, and your ability to recover to a working state with a minimum of downtime and operational impact.

Readiness Assessment Activities

The assessment will focus on the following areas:

- Network Perimeter Monitoring
- Application Integrity and Allowlists
- Web Browser Management and DNS Filtering
- Phishing Prevention and Awareness
- Asset Management
- Risk Management
- Patch and Update Management
- User and Access Management
- Data Backups
- Incident Response
- Manual or Independent Operations

Through document review, interviews, and policy analysis, TPx will conduct a baseline review of your organization's exposure to ransomware and its effect on your business in the event of a successful attack.

Upon completion of the assessment, TPx will provide two reports: an Executive Summary and a prioritized list of specific actions you can take to reduce your exposure to ransomware attacks. In less than a week, you and your team will have the information you need to tighten your security and reduce the risks you face due to the most widespread method of cyberattacks today.

There were 65,000 successful ransomware attacks in 2020 — one every 8 minutes

Recorded Future

Wireless Security Assessment
Service Description

Overview

The objective of this Service Description is to provide an overview of the Wireless Security Assessment activities that are performed under the Service. This framework establishes the purpose, content, and scope of the activities to be performed. Schedule, cost, and other logistics for the Service are contained in a separate Statement of Work document.

Wireless technology has introduced a number of complications and additional security risk into traditional network management. BYOD, signal jacking, the proliferation of public Wi-Fi and most recently, expanded work-from-home has made securing the corporate network much more challenging. Securing the wireless component of your organization's network requires well-documented policies as well as strong technical controls. To help your organization achieve this, TPx offers a comprehensive Wireless Security Assessment that results in actionable recommendations for a robust, high-performing, and secure wireless environment.

TPx has defined a wireless security assessment to assess a Customer's environment per industry standard controls. During the assessment TPx will examine the Customer's strategic and tactical wireless network configuration within a distilled scope that focuses on areas of cybersecurity that have the highest likelihood of incidents and breaches for the Customer's business sector. TPx's methodology is founded on industry standards such as ISO 27001, ISO 27033, NIST 800-153, CIS "Top Twenty" and current best practices. TPx's wireless security assessment is designed to evaluate an organization's wireless infrastructure and configuration, the security posture, and functional capabilities. The assessment will be divided into three phases, covering the following:

- Documentation & Visualization of the existing wireless network environment
- Security Strategy
- Operational Function & Hygiene

Phase 1: Documentation & Visualization

TPx will inventory and catalog the existing wireless network assets and architecture.

Physical Inventory

- Hardware Inventory Spreadsheet
  Physical hardware inventory — serial numbers if possible
- Layer 1-2 Diagrams/Documentation
  Physical interconnectivity
- Layer 3 Diagrams/Documentation
  Routing connectivity, gateway management, summarization, route entrances/exits

The approach for the assessment is to evaluate Customer's current exposure to threats through a vulnerability scan, and also the Customer's ability to improve its' future exposure through an effective vulnerability management program.

Design and Architecture Review

- Network Overview Architecture
  Review for modularity, scalability, and capabilities
- Layer 3 Routing
  Dynamic, optimized, secure
- Layer 2 Optimization
  Spanning-tree security/optimization, distributed Layer 2

Phase 2: Security Strategy

TPx will assess the network policies, standards and procedures as well as all the security management processes, and roles and responsibilities related to the wireless network.

Network Infrastructure Security

- Weak wireless authentication or encryption protocols
- Centralized authentication, authorization, and accounting
  AAA review
- Rogue DHCP/client detection
  Rogue detection on wireless
- Validate network access (ingress and egress) to the WAN via port scan

Performance Monitoring and Analysis

- Recommend improved hygiene and integration with MSS/SOC
- Review acceptable usage policies and ensure WAN enforces policy details
- Validate performance on WAN and off WAN
- Validate performance via different network protocols
- WAN heat map available (as scoped)

Phase 3: Operational Function & Hygiene

TPx will assess the network policies, standards and procedures as well as all the security management processes, and roles and responsibilities related to the wireless network.

Infrastructure Monitoring and Management

- Central monitoring/alerting capabilities
  Management Platform utilization/capabilities
- Syslog Capabilities
  Controls, retention, management
- Software Management (networking)
  Deployment processes for upgrades/patches
- Wireless configuration validation capabilities
  Lab Environment

Wireless Configuration Management

- Centralized configuration backup
  Configuration backups
- Centralized configuration Automation
  Configuration change capabilities
- Configuration change management workflow
  Change control management

Controls and Methodology

The expertise of the security team relies upon leading information security practices. Our approach is aligned with the most recent versions of international standards, such as:

- ISO 27001:2013 Information security management requirements
  http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- ISO 27002:2013 Organizational standards and best management practices related to information security
  https://www.iso.org/standard/54533.html
- ISO 27033:2015 Information technology – Security techniques – Network security (sections 1- 7)
  https://www.iso.org/standard/63461.html
- NIST Special Publication 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)
  https://csrc.nist.gov/publications/detail/sp/800-153/final
- CIS "Top Twenty Controls", Center for Internet Security
  https://www.cisecurity.org/controls/cis-controls-list/

Posture and Profile

The approach for the wireless security assessment is to evaluate an organization's wireless network security posture and profile.

Posture refers to the organization's current ability to transfer, maintain and protect data within the wireless network.

Profile refers to the minimum target of capability required to protect information and manage associated risks, which an organization should aim to achieve. It is recommended that the organization selects a target profile that is reflective of its security objectives; that is, selecting a target posture (e.g. 'Defined', 'Managed', etc.) for each of the assessed categorizations.

The information security profile accounts for several factors such as an organization's attributes (e.g., size and type of organization compared to similar organizations), business and risk context (e.g., value of critical information assets and expected capabilities/motivations of threat actors) and other relevant variables (e.g., legal, regulatory and service-level requirements).

Categories

The organization's information security posture is assessed based on a set of categorizations (e.g., access controls and network protections). The categorizations covered for the assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for the organization.

Rating

Information security ratings are evaluated according to the information security approach adopted by the organization. This includes selected controls or solutions, deployment strategy, metrics, system monitoring, organizational plans, and so forth. The ratings are organized into six categories: None, Minimal, Developing, Documented, Managed and Maintaining. Maintaining is the highest rating, which would indicate that an organization is postured for continuous improvement in the rated category. The full list of categories is as follows:

- *Maintaining (5)* Managed information security whereby generated metrics are applied to the performance evaluation and continuous improvement of information security.

- *Managed (4)* Defined information security established that generates relevant, measurable and useful metrics.
- *Documented (3)* Well-established information security requirements, practices, controls and documentation that translate into consistent repeatable and predictable results.
- *Developing (2)* Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.
- *Minimal (1)* Early reactive information security requirements, practices, inadequately controlled and/or documented.
- *None (0)* No information security requirements, practices, controls or documentation.

Workplan

Scope

The main objective of this effort is to assess Customer's wireless infrastructure adherence to industry standards of ISO 27033. TPx will review the organization through interviews, policy review, and investigation and validation of process to provide a prioritized list of risks to the organization. TPx will review the data traversing the network and review the wireless network architecture to the minimally documented schema. TPx will provide a report with business priorities based on the sensitive data of the organization and the operational risk to business sustainability. Based on the findings, TPx will issue an executive summary that makes a statement of the Customer's wireless network security posture. TPx will also detail the results of each best practice assessed, the validation method and risk level to the business. From TPx's report, the Customer can build a wireless network architecture program based on controls with the greatest benefit to the security posture and assure that their limited resources are utilized most effectively.

TPx expects the work to consist of two (2) weeks of effort. The bulk of the assessment will incorporate inventorying the wireless network architecture and hygiene through resource interviews, review of existing policies (and processes where policies don't exist), and review of system configuration, logs, and processes in operations. Additional effort will be to perform a heatmap/wireless saturation assessment of the physical environment (as scoped with the Customer at the outset of the engagement). There may be additional data collation to enable report generation in the form of an Executive Summary, Detailed Statement of Best Practice, wireless network mapping and a graphical depiction of Customer's wireless network security state by category. Please note, the wireless network mapping is highly dependent on the Customer having physical schematics of the building reviewed. Without the availability of pre-existing documents, TPx will make a best effort to recreate the building layout.

Project Management

TPx will initiate a kickoff meeting where TPx will present the controls for review, identify the key resources to review the controls, and build out a schedule for the engagement to review and collect the information to assess the controls. The primary location for the wireless saturation test will also be identified. During this meeting, TPx will set a normal cadence for status and escalation points within the Customer in case the engagement stalls. TPx expects to incorporate eight (8) hours for project management and presentation of the assessment results to Customer.

Reporting

Upon completion of the assessment, TPx will provide two (2) reports to Customer: an Executive Summary and a detailed Best Practice report. The reports will speak to two different levels of resources at the Customer: the leadership and the security practitioner.

A detailed recommendations report will be provided and validated with Customer personnel. The objective of this report is to present the results and observations related to the Customer's wireless network security posture. In addition, the Customer will receive recommendations by TPx for their top three (3) priorities based on their business, their sensitive data, their exposure landscape and the wireless network state.

TPx will also provide an updated wireless network diagram, wireless saturation for the primary location (as scoped) and recommendations for further documentation that either doesn't exist or which requires updating.

Network Vulnerability & Penetration Scanning

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Proactively maintaining and protecting a computing network requires continuous effort. Vendors are continually releasing patches and updates, access and permissions requirements are always evolving, and most importantly, the threat landscape is continuously expanding and becoming more dangerous. Preparing ahead of time for the inevitable attack by thinking like a hacker and understanding the way they will attack is critical and leaves you and your organization better protected against hackers and malware than a "just-in-time" approach.

Regular Vulnerability and Penetration Scanning are two of the best tools you can use to understand where your weaknesses are and how likely it is that a hacker will be able to exploit them.

Get answers to these questions…

- What vulnerabilities currently exist in my network? How do I know which ones pose the greatest threat?
- How do I best prioritize my patching and updating activities?
- Am I susceptible to attack from employees and others inside my organization?
- Based on my network infrastructure, are there threats that I do not need to worry about?
- How do I stay current on the threat landscape and defend my organization against emerging threats?

57% of data breaches are attributed to poor patch management. The average time to apply, test, and fully deploy a patch is 102 days.

Ponemon Institute

Overview

TPx's Vulnerability and Penetration Scanning Service (VPS) consists of two components: a Vulnerability Scan and a Penetration Scan. For further visibility into the strength of your overall Vulnerability Management Program, we also offer an optional Vulnerability Management Plan Review as part of this engagement.

The **Vulnerability Scan** evaluates devices that are connected to the network for the purpose of identifying vulnerabilities that may be present on those devices due to open ports, exposed services, lack of current patches, etc. The TPx Vulnerability Scan:

- Uses manually written signatures to detect known vulnerabilities
- Leads to discovery of new vulnerabilities or validates the presence (or remediation) of vulnerabilities that had been previously identified

The **Penetration Scan** shows how exploiting a vulnerability could result in a significant impact to the environment. By demonstrating this impact, it is possible to get organizations to reconsider the priority of remediating vulnerabilities that Vulnerability Scanners may have reported as non-urgent. The TPx Penetration Scan mirrors the behavior of bad actors by:

- Performing exploits against identified network vulnerabilities (shell file uploads, hash cracking, password dumping)
- Executing multiple authentication-based attacks (POP3, Telnet, SMB, AD, FTP)
- Conducting man-in-the-middle (MitM) attacks (SMB relay, DNS poisoning, ARP poisoning)
- Attempting privilege escalations on the network using AD group and share enumeration
- Impersonating users to find sensitive data

Regular Penetration Scanning is one of the best tools you can use to understand where your weaknesses are and how likely it is that a hacker will be able to exploit them and gain access to other systems and/or confidential information on the network.

Although both Vulnerability and Penetration scans can be run independently, there is tremendous added value in running them together. The additional discovered details can be used in strengthening the security posture of your business. The Vulnerability Scan looks for known vulnerabilities on the network but will not exploit them. In addition to testing each of the vulnerabilities that are found in the Vulnerability Scan (which lowers the number of false positives), the Penetration Scan probes various parts of the network, potentially uncovering unpublicized weaknesses and running further testing to discover the extent of those weaknesses.

During the optional **Vulnerability Management Plan Review**, we will evaluate your organization's security program through interviews, policy review, validation and investigation of processes to generate an assessment of your Vulnerability Management (VM) program. TPx will detail the results of the assessment of each aspect of the program, any deviation from best practice, and the resulting risk to the business.

Scheduling and Reporting

TPx can schedule a scan as frequently as needed and keep track of your risk profile in near real time. Our reports will show your trending data, allowing your team to see improvements from one month to the next.

The post-scan reports will speak to two distinct levels of resources: the security practitioner and the leadership. For the security practitioner, we'll deliver the results of the scans — annotated to highlight the most important findings — and recommend how to mitigate those vulnerabilities. An additional Best Practices report presents assessment results and observations related to your organization's current level of exposure.

TPx will also generate an executive-level document containing a summary of our findings. From our insights, you will be able to build or enhance a VM program based on controls with the greatest impact to your risk posture, ensuring that you utilize your limited resources most effectively.

74% of IT security pros believe their orgs would test systems more frequently if the penetration testing process was more efficient or required less management.

VentureBeat, Nov. 2021