

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

Escalations of a more tactical nature will be handled between the AT&T Engagement Manager and the appropriate SPOC serving as an escalation point.

#### Security Incidents

If, in the course of the assessment, a critical cybersecurity incident is suspected, the Assessor and/or Engineer will immediately perform an initial review of the suspected incident and provide all relevant information and recommended next steps to County authorities immediately. AT&T will also be notified of the Incident and all relevant details to help support the Customer in forming an immediate action plan.

If the details of the security incident provide a potential threat or impact to an organization outside of the County, then CyberDefenses and AT&T will be required to notify the Texas Secretary of State and potentially additional authorities, as described in the **Confidentiality** Section of this document.

#### **9. Initiation of Work**

AT&T's ability to provide resources will be based on:

- AT&T's acceptance of the customer request
- The customer's approval of the request
- The availability of resources at the time of request

AT&T requires up to four (4) business weeks after the approved SPP is received to provide resources to the Customer. The start of any specific resource under this SPP must be mutually agreed to by AT&T and the Customer.

#### **10. Schedule and Expected Duration**

Within one week of receipt of the Request for Solution (RFS), AT&T (or CyberDefenses) will contact the Customer to confirm the scheduled timeline and the target dates for the Site Visit.

If the Customer can support it, the ESA Kick-off Meeting will be schedule within 10 working days of receipt of order.

The ESA Site Visit will occur at a time mutually agreed upon between AT&T and the Customer. Once the Site Visit has occurred and all relevant information collected by AT&T, the ESA Deliverables will be provided to the Customer within 30 working days.

#### **11. Confidentiality**

The artifacts collected and the deliverables of the Election Security Assessment (ESA) are considered confidential to the County, unless a specific incident is discovered that has a direct impact on organizations or individuals outside of the County.

AT&T will generate the ESA Scorecard and the ESA Report and they may be reviewed for quality or correctness by AT&T. The results of any specific County will not be delivered to the Texas Department of Information Resources (DIR) or the Texas Secretary of State (SoS). The ESA deliverables are accepted from Public Information Requests because these documents specifically include information regarding security vulnerabilities (Texas Government Code 552.139).

If a security incident is discovered during the assessment that has an impact on individuals or organizations outside of the County, then AT&T is required to notify the Secretary of State's office and/or other appropriate authorities, depending on the details of the incident.

If AT&T identifies child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110, in conducting the activities described in this SPP, AT&T shall report such to the Customer's Executive Director or highest-level executive and an appropriate law enforcement agency and shall provide the law enforcement agency with access to the offending material. If AT&T identifies information that it perceives as a serious threat to human life or safety in conducting the activities described in this SPP, AT&T shall report such threat to an appropriate law enforcement agency and the Customer's Executive Director or highest-level executive.

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 5 © 2018 AT&T Intellectual Property. All rights reserved.

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

Aggregated results will be delivered to the SoS once a sufficient number of counties have been evaluated that will allow for a reasonable level of anonymity. Any information that might help to identify a specific County will be withheld to protect the anonymity of any specific County's results.

## 12. Acceptance Criteria

Upon receipt of the ESA Scorecard and the ESA Report and any other deliverable required under this SPP, the Customer will have five working days to request clarification and/or updates. Where needed, updates or clarifications will be provided within five business days or as quickly as possible. The Customer will be given five working days from the receipt of each respective update or clarification to request additional updates or clarification until the Customer is satisfied that the deliverable complies with the standards in this SPP. If the Customer receives the deliverables and does not respond with either acceptance or requests for updates for a period of five (5) working days, then the deliverables will be considered accepted by the Customer.

If the Customer and AT&T reach a point where AT&T cannot agree to provide additional updates or clarification, and the Customer is not satisfied that the deliverable complies with the standards in this SPP, the Customer shall utilize the Escalation Process contemplated in Section 8 of this SPP, and, if that does not result in a deliverable which the Customer believes is compliant with this SPP, the matter shall be referred by the Customer to DIR and resolved by DIR and AT&T pursuant to the dispute resolution procedures set forth in Article 19 of the Master Services Agreement between DIR and AT&T, DIR-MSS-SCP-001.

Each County choosing to participate in the ESA program will execute, among other things, a separate Inter-local contract ("ILC") with DIR; however, any provisions in each respective ILC (including, but not necessarily limited to, portions of Sections V, VI, and VII of each respective ILC) do not apply to the ESA Program to the extent they conflict with this SPP and the addendum to the Inter-agency Contract, DIR-SS-IAC0031, between SoS and DIR ("IAC") relating to the ESA Program. In addition, any provisions in the IAC (including, but not necessarily limited to, portions of Sections V, VI, and VII of the IAC) do not apply to the ESA Program to the extent they conflict with the addendum to the IAC and this SPP.

Once updates or clarifications are provided to the Customer's satisfaction or the deliverable is otherwise considered to be accepted following the aforementioned dispute resolution process, then the review process is considered completed and final. DIR and/or AT&T shall notify SoS that the review process is complete, and DIR may invoice SoS for the services provided to the Customer. No invoice shall be issued by DIR, and no payment shall be made by SoS, for a Customer, unless and until the current documentation workflow for that Customer, as referenced in Amendment 1 to the IAC, is substantively followed and the ESA Program services are considered to be accepted by that Customer in accordance with this section.

## 13. Resource Management

AT&T reserves the right to assign resources based on AT&T's understanding of the technical requirements and AT&T resource availability. The Customer agrees that all AT&T contractors are acceptable for this project.

AT&T will follow the Customer's policies when working at the Customer's facilities so long as such policies do not violate applicable state or federal law. This includes but is not limited to issues such as dress code, workplace conduct and security.

## 14. Risks

AT&T has identified the following potential risks in being able to complete this engagement. If any of these risks are in danger of occurring, AT&T shall invoke the Escalation Process. If any of these risks do occur, the parties agree to resolve the situation via the Change Order Process. Notwithstanding the foregoing, neither of the parties is bound to use the Change Order Process in the event of a material breach by the other party.

- Uncooperative Customer personnel or other entities (e.g. they won't provide information, provide incorrect or incomplete information, hinder progress of AT&T resources, etc.).
- Inability to travel due to government action (such as grounding of airlines).
- Delays in accessing network devices, systems, locations, documentation and people who are vital during the engagement.
- Delays in receiving Customer IP address ranges and/or URLs that are vital during the information collection phase of this project.
- The receipt of inaccurate information regarding the design and configuration as provided by the Customer or its third-party resources.
- Prolonged network outages that limit the access to in-scope devices.

### CONFIDENTIAL INFORMATION

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 6 © 2018 AT&T Intellectual Property. All rights reserved.

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

- The active shunning of AT&T's security testing IP addresses by the Customer or its third-party resources.

Should any of these risks occur and cannot be resolved within the duration window of the ESA, then the relevant sections of the ESA deliverables will reflect that some information was not available and the associated Risk Level, Concerns and Recommendations will reflect that not all information was provided.

#### 15. Change Order Process

The parties agree that this SPP may be amended by a Change Order Form prepared by AT&T and signed by both parties for one or more of the following reasons:

- The occurrence of any of the Risks.
- The invalidation of any of the Assumptions.
- Failure of the Customer to meet its Customer Responsibilities.
- Changes in the Description of Work or Deliverables requested by the Customer and agreed to by AT&T.
- The occurrence of any other event or the discovery of any other information that affects AT&T's ability to perform the engagement as specified herein.
- Any other mutually agreeable reason.

The remedy to any of the above may include changes to: the composition of the engagement team, duration and/or pricing.

The Customer will obtain the necessary approvals, signatures and, if required, a purchase order for any additional costs. The Customer will return the signed form to AT&T who will countersign the form, distribute it to the appropriate parties.

Whenever there is a conflict between the terms of a fully executed Change Order Form and those in this SPP, or a previous fully executed Change Order Form, the terms of the most recent fully executed Change Order Form shall prevail.

#### 16. Engagement Contacts

##### AT&T Consulting

Election Security Assessment Services Manager  
NAME: Daniel Weiske  
PHONE: (720) 481-7918  
EMAIL: daniel.weiske@att.com

ESA Program Manager  
NAME: Maria Acosta  
PHONE:  
EMAIL: elections@cyberdefenses.com

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 7 © 2018 AT&T Intellectual Property. All rights reserved.

#### 17. Appendix A: Election Security Assessment Service Details

The following sections outline the specific activities that will be included within the Election Security Assessment service.

The Customer workflow process is designed to facilitate the collection of **Artifacts**. An artifact is any piece of information that helps the Assessor to determine the current state of the organization. An artifact can be information that is obtained from a Customer through observation, verbally or through provided documents. An artifact can also be the result of technical scans that reveal information about specific systems or technology. For the purposes of categorization, AT&T will be working to obtain the following types of Artifacts throughout the ESA.

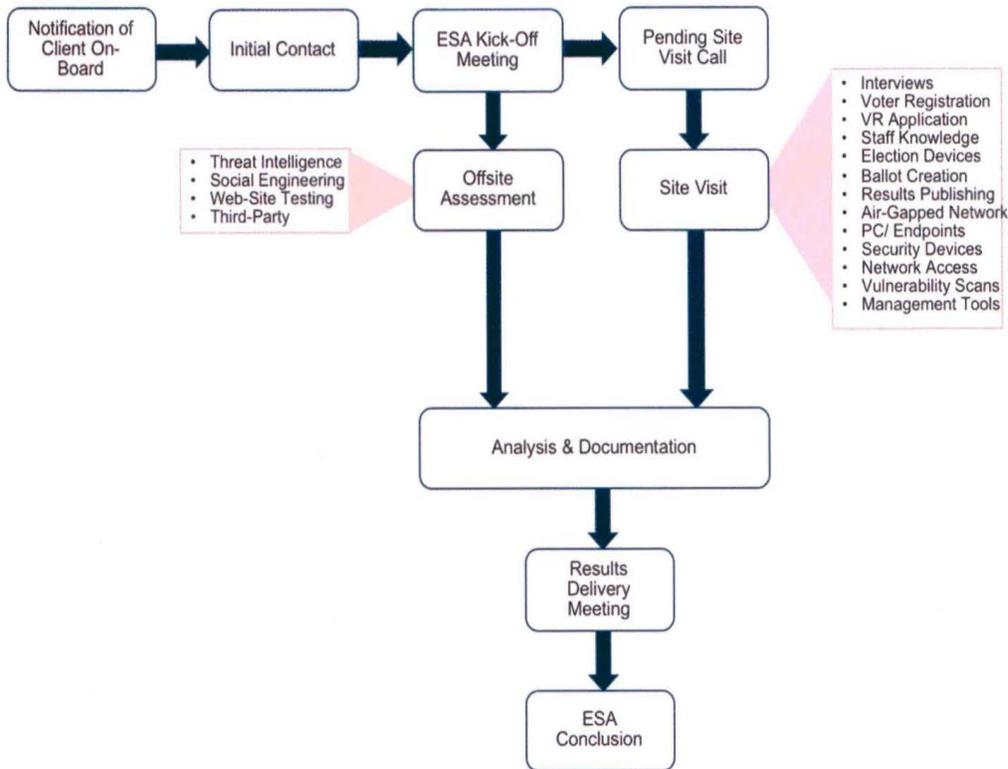
- **Provided Artifacts:** These artifacts represent information that is stored and needs to be collected from the Customer. Common examples are written policies & procedures, org charts, lists of product vendors, email addresses, domains and IP address ranges. Where possible, if the Customer can collect and deliver the Provided Artifacts, then the Site Visit can be shortened. If it is not reasonable, then the Assessor will work with the Customer staff to collect the Provided Artifacts during the site visit.
- **Interview Artifacts:** These artifacts represent information that is not collected in documents and needs to be verbally gathered by the Assessor. Interview Artifacts will typically be gathered in-person, though could be performed via conference call, if necessary. Interview Artifacts will typically be gathered in the form of notes taken by the interviewer. In some cases, Interview Artifacts are gathered by having the Engineer or Assessor review the activities of an individual that is executing specific policies.
- **Scanned Artifacts:** Scanned Artifacts will be collected through the use of technology, such as vulnerability or malware scanning tools, and the inspection of systems or networks.
- **Intelligence Artifacts:** Intelligence Artifacts are gathered through investigation of the internet, darknet and/or individuals that are outside the elections organization. Examples of intelligence artifacts might be information that is being sold on the darknet that relates to the Customer, such as stolen usernames/passwords.

All of the following steps in this workflow will facilitate Artifact collection. The Artifacts are then reviewed and analyzed to provide the resulting reports.

The figure below describes the expected Customer interaction workflow for the ESA. Each stage in the workflow is described in more detail in the following sections.

#### CONFIDENTIAL INFORMATION

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 8 © 2018 AT&T Intellectual Property. All rights reserved.



ESA Workflow

Initial Contact

Within three working days, the Program Manager will make Initial Contact with the Primary point of contact by phone, if possible, and provide them with the necessary steps to set up the Election Security Assessment Kick-Off Meeting to accomplish the following objectives:

- Confirm the key roles that will participate in the entire ESA process and Kick-Off meeting
- Identify the time of the Election Security Assessment Kick-off meeting to occur within two weeks, unless the Customer requests a later date and time
- Describe a very high-level outline of the site visit activities, contributions needed from the Customer and expectations to help prepare the Customer for the assessment
- Begin the process to identify a tentative date for the ESA Site Visit.

Election Security Assessment Kick-off Meeting

The Election Security Assessment Kick-off meeting is a critical event in the ESA process and requires that one representative from each important role be present. The meeting will be delayed until a time when all critical roles can participate, assuming that they exist within the Customer's organization. The three critical roles are:

- Administrator of Election
- Administrator of Voter Registration
- IT staff (County or Election)

The following roles will participate from the assessment team. Additional team members from DIR and AT&T may also contribute, dependent upon the Customer's specific requirements.

- Program Manager
- Lead Assessor

**CONFIDENTIAL INFORMATION**

This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.  
 Version 1.0 Page 9 © 2018 AT&T Intellectual Property. All rights reserved.

**AT&T Tracking Number: DMND0004894**  
**WO Number: DMND0004894**

The following activities will occur on the ESA Kick-off meeting. The ESA Kick-Off will typically be held as a conference call, though could be scheduled as an onsite meeting if requested by the Customer.

- Introduction of all team members
- Short overview of the ESA Process and expectations of participants
- Review of the Site Visit planned activities and confirmation of the following details:
  - AT&T will require access to:
    - All required systems, even if they are in storage.
    - The required samples of devices (such as DREs, Pollbooks, scanners, etc) and to the workspace where devices are prepared.
    - Networks and Domains to perform required tasks
    - Air-gapped networks
  - Customer team will be present and available for interviews, including
    - Administrator of Election
    - Administrator of Voter Registration
    - County and Elections IT Staff
    - Staff members that are familiar with the use of:
      - Election Management System
      - Electronic poll book or paper poll book generation
      - Ballot creation system
      - Vote capture devices
      - Vote tabulation
      - Results Publication
      - Current security practices

The Customer will be notified that social engineering efforts will begin immediately and may continue until the final report is delivered. The Customer will be requested to identify any calendar time-blocks where such efforts would be inappropriate or may slow or impact the elections process.

A contact will be identified to coordinate scheduling of vulnerability testing efforts of external websites.

Discussion of required Provided Artifacts and whether the Customer is able to provide any in advance. If the Customer is able to support the collection of the Provided Artifacts in advance, then access to the ESA secure portal will be granted.

#### Pending Site Visit Call

As the ESA Site Visit date approaches, the Program Manager will schedule a call to occur approximately two weeks before the visit. This call will include at least the Primary Point of contact but may also include the other organizational leaders. In this call, the Program Manager will review the plan for the site visit and re-confirm the dates and availability of required resources.

#### Site Visit

Every ESA will include a Site Visit that will involve one to four cybersecurity experts visiting the County and all relevant sites, depending on the size of the elections operation. Once on-site the following activities will be performed by the Assessor(s) and/or Engineer.

The visiting ESA team will utilize a digital camera to collect relevant photographic evidence of the facility and any visually identified artifacts.

#### *Interview Process*

The purpose of the Interview Process is to explore the Customer's elections processes and cybersecurity operations. Interviews with Elections and Voter Registration leadership are used to establish the governance, oversight, and management of risk as it relates to elections cybersecurity. Interviews with County Information Technology personnel are used to explore the IT functions provided to the elections department and how County technology services relate to cybersecurity capabilities. Interviews will also include security personnel in counties that have staff dedicated to the areas of cybersecurity.

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 10 © 2018 AT&T Intellectual Property. All rights reserved.

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

#### *Voter Registration System*

In Texas, voter registration is managed with a centralized application, TEAM. TEAM supports two common models of Voter Registration (VR), Online and Offline. For each of the models, users of the Customer's VR system will be asked to demonstrate common activities.

#### *VR Application Storage*

Texas law requires that each Customer store the original registration application submitted by a voter, according to specific retention requirements. The ESA Assessor will review the storage process and confirm that proper access controls and encryption levels are used throughout the transmission and storage of the application. If applications are stored in paper format, the practices for collecting and processing applications from digital sources will be inspected.

#### *Staff Security Knowledge*

The ESA team will hold short interviews with one to three staff members to assess general knowledge of security principals and to understand the level of security knowledge of the elections staff. Staff will also be asked to describe the staff and volunteer training process, specifically as it relates to the security of the election.

#### *Election Devices*

A sample of every device that is used as a part of the election process will be evaluated for proper security controls. Prior to arrival, the ESA team will request access to at least two of each type of the following devices that might be used at the Customer:

- Digital-Recording Equipment (DRE)
- Scanners (both Precinct and Central)
- Ballot Marker
- Computers that are specifically used at polling locations, commonly pollbook software
- Computers that are specifically used on a non-internet connected networks
- Tablets or Phones that are specifically used at polling locations

#### *Ballot Creation Process & Tools*

The Elections leadership (and/or staff members) will be requested to walk the ESA Assessor through the procedures and practices involved in the creation, verification, distribution and usage of Ballots. This will include the management and programming of the ballots throughout the early voting process and election day. Every point where the ballot is digitally stored or transmitted will be considered for security and verified by the Engineer, if possible.

For cases where external software programs or contract vendors are used for ballot programming, the external company will be requested to respond to a third-party risk assessment.

#### *Results Publication Process & Tools*

The Elections leadership (or a delegate) will be requested to walk the ESA Assessor through the procedures and practices involved in collecting the result of an election from the tabulation system and posting the results to the Secretary of State or to any of the Customer's publication mechanisms (such as websites).

#### *Non-Connected Network & System*

The ESA team will perform a limited penetration test on any air-gapped network that is used within the elections process. This effort will confirm that the air-gapped network is configured correctly and that network access is completely disabled. A monitoring device will be deployed on the air-gapped network to confirm that no external traffic is probing the controlled network. Systems on the air-gapped network will be manually inspected to insure proper configuration and security measures are in place.

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 11 © 2018 AT&T Intellectual Property. All rights reserved.

*General Computer / Endpoints*

Every computer that is involved in the elections process and generally available during the Site Visit will be accessed and tools will be executed to determine the following:

- Is endpoint security software present and configured properly?
- Is malware or suspicious software present?

Remotely executed tools will be used to evaluate security of the devices, executed remotely whenever possible (using Admin access over a domain). If remote access is not available, the Engineer will briefly access each computer to run the required scans and perform the appropriate manual inspection. This process creates Scanned Artifacts that contribute to the overall analysis effort.

*Security Devices*

The Assessment Engineer will work with the County or Election IT staff to identify all security devices (firewalls, URL filters, behavioral detection, etc) and review their configuration and logs to understand the full network protection provided to the elections network. In some cases, the devices will be employed only at the Customer network access points and they will still be evaluated for proper protection configuration and usage.

*Internet Connected Election Network*

The Engineer will work closely with the IT Staff (County or Elections) to determine the optimal placement for network analysis tools within the environment. These tools will optimally be placed at a network ingress/egress point. If network access point cannot be monitored, the tools can be placed in front of key servers.

The Engineer will provide the necessary monitoring appliance and required network tap(s) to allow visibility without interrupting network traffic. The appliance will deploy IDS and Behavioral detection technologies for a period of at least 24 hours and record the results.

*Network Access*

The ESA team will work with the County IT staff to identify each area where devices may be added to the network. These ingress/egress points are often defined as links to the internet, as network access ports or the wi-fi network. The Engineer will evaluate each of those points for proper physical and network access controls, dependent upon the technologies used.

The networking plan in use for polls and early voting will also be analyzed and evaluated, if possible.

*Vulnerability Detection*

The ESA team will deploy a network appliance that will be used to perform a vulnerability scan of each computer or supporting information technology devices that are associated with the election and/or voter registration process and are network accessible.

*Management Tools*

Products (devices or applications) that are used to support the general management of the election process will be identified and visually inspected to determine the security capability and current usage of those devices. In most cases, these products will include the County or elections organization's email system, file servers and any collaboration and/or distributed program management tools.

*Maintenance and Remote Support*

The ESA team will evaluate any vendor maintenance capabilities and remote support mechanisms for information technology devices and elections functions to ensure that access is appropriately limited to authorized personnel, properly protected to ensure that unauthorized access is prohibited, and established with audit trails and attribution to identify remote access and associated maintenance activities.

The ESA team will look for records that establish authorized vendors and corresponding personnel as well as inspect the methods used for equipment maintenance and remote support. Maintenance and remote access interfaces will have a limited test conducted to verify protections are effective.

**CONFIDENTIAL INFORMATION**

#### Off-Site Assessment Activity

Off-site Assessment activity refers to Artifact collection that does not require the assessment team to be at the Customer site. The activities will occur at a time that is convenient for the assessment team, but before the final analysis is complete and delivered to the Customer. Whenever direct interactions are required with the Customer (or Customer systems), the Program Manager will schedule the activity with the Customer.

#### *Threat Intelligence*

As soon as the Customer is able to provide confirmation of their IP Address ranges and internet domains (Provided Artifacts), AT&T will schedule the Intelligence Sub-Assessment. This effort will engage expert cybersecurity analysts in the effort of scanning the internet and darknet (criminal elements of the internet) for any of the following:

- Hacker communication that may impact the County or election
- Activity on the darknet that may indicate that information has been stolen from the Customer or a Customer's partner
- Collection of all Intelligence Artifacts on the darknet that can be associated with the Customer. For example, stolen accounts (from other companies/orgs) that may provide clues on how to access the Customer resources
- Attacker activity that may focus on the Customer's specific region

The Threat Intelligence Assessment does not require any interaction from the Customer and will not directly impact their ongoing activities. If a critical security incident is discovered, the Customer will be notified immediately. All discovered Intelligence Artifacts will be considered in the generation of the final ESA Scorecard and ESA Report.

#### *Social Engineering*

The ESA Team will undergo efforts to use social engineering in attempts to determine whether the staff uses common security principals when responding to requests for sensitive voter or elections information. Social Engineering attempts will include (but is not limited to) sending of phishing email and phone calls from individuals pretending to request protected information. Social Engineering phone calls to the Customer's staff will be recorded.

The results of the Social Engineering efforts are cataloged and treated as Scanned Artifacts.

Through the acceptance of this document, the Customer is acknowledging that the AT&T staff will contact the elections staff, pretending to be individuals that they are not, and attempt to retrieve information that should not be provided by Customer staff. Any information that is collected through these efforts will be treated confidentially.

#### *External Web-site Vulnerability Testing*

Each external website used by the Customer for any specific elections purpose will be evaluated to determine if it is currently compromised, if there are any indicators of past compromises and whether current application vulnerabilities make it susceptible to attack.

Web application vulnerability scans and analysis will be used. Limited efforts to penetrate existing security controls will be used to ensure that basic security constructs are in place. This test does not intend to provide a full cybersecurity penetration test of the application, though the Customer's processes will be evaluated to ensure that annual security assessments of all external interfaces are included.

#### *Third-party Risk Assessments*

Each outsourced and third-party vendor provided product that a Customer uses as a critical element of the elections infrastructure will be identified and the ESA Team will engage with the vendor to perform a risk assessment of that application. In some cases the ESA Team may require assistance from the Customer to obtain responses to the assessment request. The Risk Assessment will present the vendor with a focused questionnaire that will assess the vendors adherence to NIST CSF principals and industry best practices. Whenever possible, the risk assessment will be performed prior to the site visit so that any specific configuration practices might be evaluated.

#### Analysis and Documentation

Following the collection of the Artifacts, the AT&T team will be able to perform analysis and generate the findings and deliverables. The analysis effort happens continuously throughout the collection process but is primarily focused on the period of time following the Site Visit until the final deliverables are presented.

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 13 © 2018 AT&T Intellectual Property. All rights reserved.

#### *Cybersecurity Capability*

The ESA will evaluate the Customer's ability to perform activities within the NIST CSF functions and the level of maturity for ongoing cybersecurity operations. Using Provided Artifacts that include reports, procedure documents, and other outputs that are related to each of the associated activities, assessors will use the information to focus interview questions for sessions with key personnel during the on-site visit. Assessors will measure the maturity of capabilities using a capability/maturity scale. Capabilities are also validated using the Scanned Artifacts produced during the technical testing where possible.

The analysis is then compiled and scored using the ESA methodology to provide the capability scorecard summary and key recommendations for high risk areas where maturity is lacking or performing at low levels.

#### *Findings and Recommendations*

Through the analysis argument, each Artifact will be reviewed by ESA Analysts and a set of findings (concerns) will be documented. Each finding will be assigned a recommendation to address the concern with an appropriate level of maturity, given the current security level of the Customer.

Findings will be presented in the ESA Scorecard and ESA Report across the entire organization and also broken down across each of the eight areas of elections focus:

- Elections Management
- Election Team Support
- Voter Registration
- Pollbook / Voter Check-in
- Ballot Creation & Distribution
- Vote Capture (Paper or DRE)
- Vote Tabulation (Manual and/or Automated)
- Election Results Publishing (locally and to SoS)

#### *Risk Assessment*

ESA Analysts will process all findings and assign each a value to determine the impact that issue may have on the Customer and the overall probability that the issue may happen. Based upon these values each concern is assigned a risk level:

- Critical
- High
- Medium
- Low

Each area of the election (described above) is provided a Risk Level and the entire organization is assigned an overall Risk Level. These results are reported in both the ESA Scorecard and Report.

#### Delivery of Results

As the analysis effort is nearing completion, the Program Manager will contact the Primary Point of Contact for the Customer and schedule the Delivery of Results meeting. This meeting will typically be held as a conference call to review the ESA Scorecard and some of the key findings. This meeting will represent the first time the Customer has seen the results.

In this meeting, the ESA Lead Assessor will review the structure of the results and each of the key findings and discuss recommendations for improvements. The Customer will be provided with access to a secure portal to download the delivered reports and will be advised on mechanisms to protect the contents of the deliverables. A member of the sales team will also be available to discuss next steps, should the Customer wish to engage in resolving the concerns with the same team.

The Customer will be advised that they have five working days to review the results and request clarification and/or updates.

#### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 14 © 2018 AT&T Intellectual Property. All rights reserved.

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

## 18. Appendix B: Definitions

### Customer Roles:

**Administrator of Elections** - A general term that refers to a County employ that has the responsibility of managing the elections process.

**Administrator of Voter Registration** - A general term that refers to a County employ that has the responsibility of managing the voter registration efforts for the County.

**County IT Staff** - Many counties provide IT services for the election organization. The County IT Staff provides host, network and/or applications support across a large number of County departments, often including Elections.

**Election IT Staff** - Many elections organizations retain IT staff to directly support the technology requirements of the election infrastructure.

### Assessment Roles

**Assessor** – A cybersecurity risk assessment expert that has the role of collecting Provided Artifacts and Interview Artifacts.

**Engineer** – A technical cybersecurity expert that has the role of working with the Customer's technology to collect Scanned Artifacts and the ESA.

**Lead Assessor** – The lead of the ESA Team who will serve as the primary liaison throughout the Site Visit and through the ESA process. In most cases, there is only a single Assessor, who also serves as the Lead Assessor.

**Program Manager** – Manages the schedule and the process of delivering the ESA to the Customer. The Program Manager serves as a point of contact for the Customer and coordinates all aspect of providing the service.

**Sales** – Members of the AT&T Sales team members will a serve top help inform each Customer about the assessment and facilitating the sign-up process

### Terminology

**Artifact** - Piece of data or indicator of activity that contributes information to the ESA process and is used to help assess the risk and security preparedness of each Customer.

**County** - This term refers to the government responsible for managing the business of a specific County.

**Customer** - This general term is used to refer to the organization that is undergoing the assessment. In the case of the Election Security Assessment, the Customer is typically the County's election organization(s).

**Cyber Security Framework (CSF)** – A CSF consists of standards, guidelines, and best practices to manage cybersecurity-related risk.

**Darknet** – The darknet represents a small portion of the internet that is not accessible via normal internet search and access methods. Adversaries use this hidden area of the internet to communicate and coordinate activity that might be considered criminal and often to sell or trade information that is gathered through criminal activities

**Intelligence Artifact** – Piece of data or literature that was generated through research that was performed outside of the Customer's staff or systems.

**Inter-Local Contract (ILC)** – The ILC is a legal document that must be executed between the County and the Texas Department of Information Resources (DIR) that provides the legal framework in which the ESA will be provided.

**Interview Artifact** – Piece of data or literature that was generated through discussion or communication with an individual within the Customer.

**NIST CSF** – The NIST Cyber Security Framework is a CSF that is authored by the National Institute of Standards and Technology that provides a basic framework managed cybersecurity-related risk.

**Vulnerability Testing** – The technical effort of evaluating a specific system or network to identify known issues with the software or hardware that may allow an adversary to access that system.

**Phish** – To request confidential information under false pretenses, usually done via the Internet (email), phone or social media.

**Provided Artifact** – Piece of data or indicator (artifact) provided by the customer.

**Scanned Artifact** – Data found via scanning with assessment tools or through manual inspection of technology.

**Scan** - A test of capabilities, usually aimed to find areas of vulnerability or to define capability.

### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 15 © 2018 AT&T Intellectual Property. All rights reserved.

AT&T Tracking Number: DMND0004894  
WO Number: DMND0004894

**Security Incident** – The determination by a security analyst that an investigated Security Alert meets the criteria of the defined Security Incident classification policy and which generates notification to the Customer.

**Social Engineering** - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

**Vulnerability** - A weakness that can be exploited by an adversary that wishes to access systems or technology that they would otherwise not have access to.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*  
Version 1.0 Page 16 © 2018 AT&T Intellectual Property. All rights reserved.

COPY

#35



Office of the Governor  
Public Safety Office –CEO/Law Enforcement Certifications and Assurances Form

|   |                  |
|---|------------------|
| Entity Name: Val Verde County                             | Date: 02/06/2019 |
| Agency/Department Name: Val Verde County Sheriff's Office |                  |
| Name of Chief Executive Officer: Lewis G. Owens           |                  |
| Name of Head of Law Enforcement Agency: Jose F. Martinez  |                  |

Certification Required by CEO and Head of Law Enforcement Agency

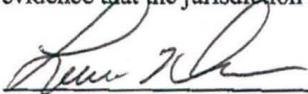
In our respective capacities as chief executive officer of Val Verde County ("Grantee") and as head of Val Verde County Sheriff's Office ("Agency"), we hereby each certify that Grantee and Agency participate fully, and will continue to participate fully from the date of this certification until the later of August 31, 2021 or the end of the grant project period, in all aspects of the programs and procedures utilized by the U.S. Department of Homeland Security ("DHS") to: (1) notify DHS of all information requested by DHS related to illegal aliens in Agency's custody; and (2) detain such illegal aliens in accordance with requests by DHS.

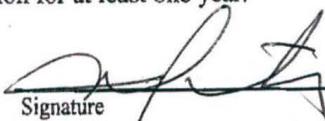
We further certify that Grantee and Agency do not have, and will continue not to have until the later of August 31, 2021 or the end of the grant project period, any policy, procedure, or agreement (written or unwritten) that in any way limits or impedes Agency's receipt or DHS's issuance of detainer requests, or in any way limits or restricts Grantee's and Agency's full participation in all aspects of the programs and procedures utilized by DHS to: (1) notify DHS of all information requested by DHS related to illegal aliens in Agency's custody; and (2) detain such illegal aliens in accordance with requests by DHS.

Additionally, we certify that neither Grantee nor Agency have in effect, purport to have in effect, or are subject to or bound by any law, rule, policy, or practice (written or unwritten) that would: (1) require or authorize the public disclosure of federal law enforcement information in order to conceal, harbor, or shield from detection fugitives from justice or aliens illegally in the United States; or (2) impede federal officers from exercising authority under 8 U.S.C. § 1226(a), § 1226(c), § 1231(a), § 1357(a), § 1366(1), or § 1366(3).

Lastly, we certify that Grantee and Agency will comply with all provisions, policies, and penalties found in Chapter 752, Subchapter C of the Texas Government Code.

We acknowledge that failure to comply with this certification may result in OOG, in its sole discretion, terminating any grant made by OOG to Grantee, and that Grantee must return all funds received from OOG for any grant terminated under this certification. We further acknowledge that Grantee will remain ineligible for OOG funding until it provides satisfactory evidence that the jurisdiction has complied with this certification for at least one year.

  
Signature  
Chief Executive Officer for Grantee

  
Signature  
Head of Agency

COPY #36

COMMISSIONERS' COURT  
OF VAL VERDE COUNTY, TEXAS

**RESOLUTION**

**RESOLUTION IN SUPPORT OF FY 2018 OPERATION  
STONEGARDEN (VAL VERDE COUNTY)**

**WHEREAS**, the Val Verde County Commissioners' Court finds it in the best interest of the citizens of Val Verde County to apply and accept the 2018 Operation Stonegarden (Val Verde County) grant;

**WHEREAS**, Val Verde County Commissioners' Court understands that there is no matching fund requirements for the said project;

**WHEREAS**, the Val Verde County Commissioners' Court agrees that in the event of loss or misuse of the Office of the Governor funds, Val Verde County assures that the funds will be returned to the Office of the Governor in full;

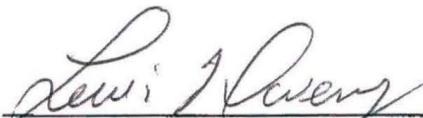
**WHEREAS**, the Val Verde County Commissioners' Court designates Val Verde County as the grantee's Authorized Official and Sheriff as the Grant Performance Officer. The Authorized Official is given the power to review, sign, and accept all grant documents on behalf of Val Verde County; and,

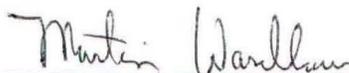
**WHEREAS**, the Val Verde County Commissioners' Court designates County Auditor as the grantee's Financial Officer.

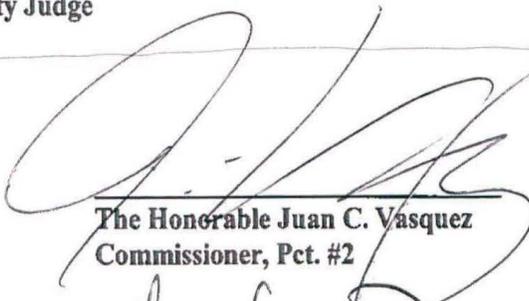
#36

**NOW THEREFORE, BE IT RESOLVED**, that the Commissioners' Court of the County of Val Verde approves submission and acceptance of grant application of the 2018 Operation Stonegarden (Val Verde County), award.

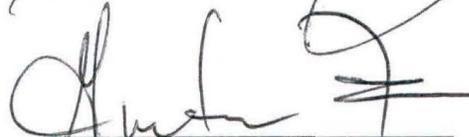
**PASSED, ADOPTED, APPROVED and FILED** on this the 6th day of Feb A.D. 2019.

  
The Honorable Lewis G. Owens  
County Judge

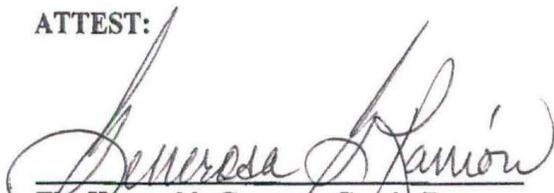
  
The Honorable Martin Wardlaw  
Commissioner, Pct. #1

  
The Honorable Juan C. Vasquez  
Commissioner, Pct. #2

  
The Honorable Robert Beau Nettleton  
Commissioner, Pct. #3

  
The Honorable Gustavo Flores  
Commissioner, Pct. #4

ATTEST:

  
The Honorable Generosa Gracia-Ramon  
County Clerk



#37

**COMMISSIONERS' COURT  
OF VAL VERDE COUNTY, TEXAS**

**RESOLUTION**

**RESOLUTION IN SUPPORT OF LOCAL BORDER  
SECURITY PROGRAM (LBSP) 2019 #2995205**

---

**WHEREAS**, the Val Verde County Commissioners' Court finds it in the best interest of the citizens of Val Verde County to apply and accept the Local Border Security Program (LBSP) 2019 #2995205 grant;

**WHEREAS**, Val Verde County Commissioners' Court understands that there is no matching fund requirements for the said project;

**WHEREAS**, the Val Verde County Commissioners' Court agrees that in the event of loss or misuse of the Office of the Governor funds, Val Verde County assures that the funds will be returned to the Office of the Governor in full;

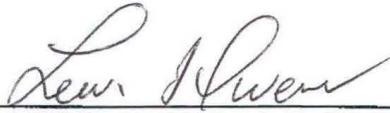
**WHEREAS**, the Val Verde County Commissioners' Court designates Val Verde County Judge as the grantee's Authorized Official and Sheriff as the Grant Performance Officer. The Authorized Official is given the power to review, sign, and accept all grant documents on behalf of Val Verde County; and,

**WHEREAS**, the Val Verde County Commissioners' Court designates County Auditor as the grantee's Financial Officer.

COPY #37

NOW THEREFORE, BE IT RESOLVED, that the Commissioners' Court of the County of Val Verde approves submission and acceptance of grant application Local Border Security Program (LBSP) 2019 #2995205, award.

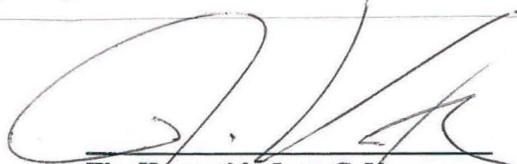
PASSED, ADOPTED, APPROVED and FILED on this the 6th day of February, 2019.



The Honorable Lewis G. Owens  
County Judge



The Honorable Martin Wardlaw  
Commissioner, Pct. #1



The Honorable Juan C. Vasquez  
Commissioner, Pct. #2

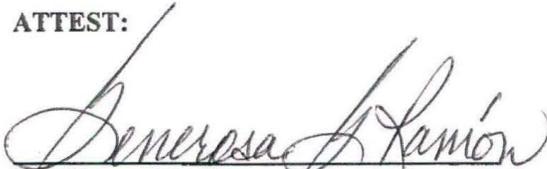


The Honorable Robert Beau Nettleton  
Commissioner, Pct. #3



The Honorable Gustavo Flores  
Commissioner, Pct. #4

ATTEST:



The Honorable Generosa Gracia-Ramon  
County Clerk



#38



December 4, 2018

Sheriff Joe Martinez  
Val Verde County Sheriff's Office  
PO Drawer 1201  
Del Rio, TX 78841-1201

Dear Sheriff Martinez:

Grant number G18SS0008A has been increased and now totals \$264,872.00.

The original of Modification 2 is enclosed. If you accept this Modification, sign the Modification and return a copy to the Assistance Center in Miami. Keep the original Modification for your file.

All terms and conditions of the original award apply to the Modification. If you have any questions pertaining to this grant award, please contact Jayme Delano at (202) 395-6794.

Sincerely,

*Michael K. Gottlieb*

Michael K. Gottlieb  
Associate Director

Enclosures

|  |   |  |             |
|--|---|--|-------------|
| <b>Executive Office of the President<br/>Office of National Drug Control Policy</b>  |   | <b>AWARD<br/>Grant</b>   | Page 1 of 1 |
| 1. Recipient Name and Address<br>Sheriff Joe Martinez<br>Val Verde County Sheriff's Office<br>PO Drawer 1201<br>Del Rio, TX 78841-1201 |   | 4. Award Number: G18SS0008A  |             |
|  |   | 5. Grant Period: From 01/01/2018 to 12/31/2019   |             |
| 2. Total Amount of the Federal Funds Obligated:<br>\$264,872   | 6. Federal Award Date:<br>12/4/2018                                 | 7. Action<br><br>Initial<br><input checked="" type="checkbox"/> Supplemental                             |             |
| 2A. Budget Approved by the Federal Awarding Agency \$264,872   | 8. Supplement Number 2  |  |             |
| 3. CFDA Name and Number:<br><i>High Intensity Drug Trafficking Areas Program - 95.001</i>  | 9. Previous Award Amount: \$259,872.00                              |  |             |
| 3A. Project Description<br><br><i>High Intensity Drug Trafficking Areas (HIDTA) Program</i>  | 10. Amount of Federal Funds Obligated by this Action:<br>\$5,000.00 |  |             |
|  | 11. Total Amount of Federal Award:<br>\$264,872.00                  |  |             |
| 12. The above grant is approved subject to such conditions or limitation as are set forth in the original Grant.                       |   |  |             |
| 13. Statutory Authority for Grant: Public Law:115-141  |   |  |             |
| <b>AGENCY APPROVAL</b>   |   | <b>RECIPIENT ACCEPTANCE</b>  |             |
| 14. Typed Name and Title of Approving Official<br>Michael K. Gottlieb<br>Associate Director<br>Office of National Drug Control Policy  |   | 15. Typed Name and Title of Authorized Official<br>Joe Martinez<br><br>Val Verde County Sheriff's Office |             |
| 16. Signature of Approving ONDCP Official<br><br><i>Michael K. Gottlieb</i>  |   | 17. Signature of Authorized Recipient/Date<br><br><i>[Signature]</i>                                     |             |
| <b>AGENCY USE ONLY</b>   |   |  |             |
| 18. Accounting Classification Code<br>DUNS: 611754136<br>EIN: 1746000673A2   |   | 19. HIDTA AWARD<br>OND1070DB1819XX      OND6113<br>OND2000000000      OC 410001<br>JID: 61486            |             |

# Initiative Cash by HIDTA

FY 2018

| HIDTA             | Agency Name   | Initiative                        | Cash              | Type          | Grant      |
|-------------------|---|-----------------------------------|-------------------|---------------|------------|
| SWB - South Texas | Val Verde County Sheriff's Office                       | Amistad Intelligence Center (AIC) | 126,218.00        | Intelligence  | G18SS0008A |
|                   |   | Del Rio HIDTA Task Force          | 69,317.00         | Investigation | G18SS0008A |
|                   |   | Eagle Pass HIDTA Task Force       | 69,337.00         | Investigation | G18SS0008A |
|                   | <b>Agency Total : Val Verde County Sheriff's Office</b> |                                   | <b>264,872.00</b> |               |            |
| <b>Total</b>      |   |                                   | <b>264,872.00</b> |               |            |

VOL. 53 PAGE 273

## Budget Detail

### 2018 - SWB - South Texas

Initiative - Amistad Intelligence Center (AIC)

Intelligence

Award Recipient - Val Verde County Sheriff's Office (G18SS0008A)

Resource Recipient - Val Verde Sheriff's Office

**Indirect Cost: 0.0%**

---

**Current Budget (net of reprogrammed funds) \$5,000.00**

| Travel              | Quantity | Amount            |
|---------------------|----------|-------------------|
| Travel              |          | \$5,000.00        |
| <b>Total Travel</b> |          | <b>\$5,000.00</b> |
| <b>Total Budget</b> |          | <b>\$5,000.00</b> |

#39

**COMMISSIONERS' COURT  
OF VAL VERDE COUNTY, TEXAS**

**RESOLUTION**

**RESOLUTION IN SUPPORT OF FY 2017 OPERATION  
STONEGARDEN (VAL VERDE COUNTY)**

**WHEREAS**, the Val Verde County Commissioners' Court finds it in the best interest of the citizens of Val Verde County to apply and accept the 2017 Operation Stonegarden (Val Verde County) grant;

**WHEREAS**, Val Verde County Commissioners' Court understands that there is no matching fund requirements for the said project;

**WHEREAS**, the Val Verde County Commissioners' Court agrees that in the event of loss or misuse of the Office of the Governor funds, Val Verde County assures that the funds will be returned to the Office of the Governor in full;

**WHEREAS**, the Val Verde County Commissioners' Court designates Val Verde County as the grantee's Authorized Official and Sheriff as the Grant Performance Officer. The Authorized Official is given the power to review, sign, and accept all grant documents on behalf of Val Verde County; and,

**WHEREAS**, the Val Verde County Commissioners' Court designates County Auditor as the grantee's Financial Officer.

COPY

#39

NOW THEREFORE, BE IT RESOLVED, that the Commissioners' Court of the County of Val Verde approves submission and acceptance of grant application of the 2017 Operation Stonegarden (Val Verde County), award.

PASSED, ADOPTED, APPROVED and FILED on this the 6th day of Feb A.D. 2019.

*Lewis G. Owens*  
The Honorable Lewis G. Owens  
County Judge

*Martin Wardlaw*  
The Honorable Martin Wardlaw  
Commissioner, Pct. #1

*Juan C. Vasquez*  
The Honorable Juan C. Vasquez  
Commissioner, Pct. #2

*Robert Beau Nettleton*  
The Honorable Robert Beau Nettleton  
Commissioner, Pct. #3

*Gustavo Flores*  
The Honorable Gustavo Flores  
Commissioner, Pct. #4

ATTEST:

*Generosa Gracia-Ramon*  
The Honorable Generosa Gracia-Ramon  
County Clerk



**COPY**

#39

**COMMISSIONERS' COURT  
OF VAL VERDE COUNTY, TEXAS**

**RESOLUTION**

**RESOLUTION IN SUPPORT OF LOCAL BORDER  
SECURITY PROGRAM (LBSP) 2019 #2995204**

**WHEREAS**, the Val Verde County Commissioners' Court finds it in the best interest of the citizens of Val Verde County to apply and accept the Local Border Security Program (LBSP) 2019 #2995204 grant;

**WHEREAS**, Val Verde County Commissioners' Court understands that there is no matching fund requirements for the said project;

**WHEREAS**, the Val Verde County Commissioners' Court agrees that in the event of loss or misuse of the Office of the Governor funds, Val Verde County assures that the funds will be returned to the Office of the Governor in full;

**WHEREAS**, the Val Verde County Commissioners' Court designates Val Verde County Judge as the grantee's Authorized Official and Sheriff as the Grant Performance Officer. The Authorized Official is given the power to review, sign, and accept all grant documents on behalf of Val Verde County; and,

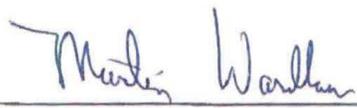
**WHEREAS**, the Val Verde County Commissioners' Court designates County Auditor as the grantee's Financial Officer.

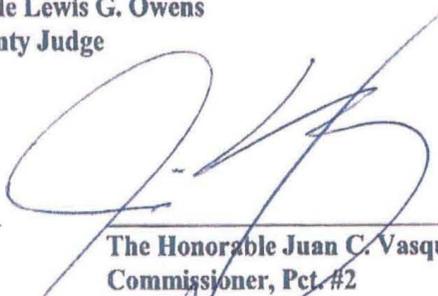
#39

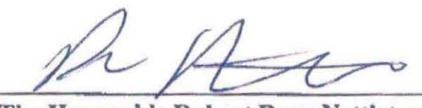
**NOW THEREFORE, BE IT RESOLVED**, that the Commissioners' Court of the County of Val Verde approves submission and acceptance of grant application Local Border Security Program (LBSP) 2019 #2995204, award.

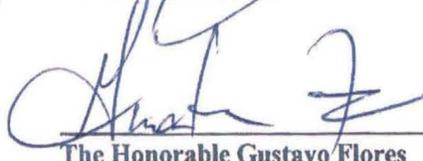
**PASSED, ADOPTED, APPROVED and FILED** on this the 6th day of February, 2019.

  
The Honorable Lewis G. Owens  
County Judge

  
The Honorable Martin Wardlaw  
Commissioner, Pct. #1

  
The Honorable Juan C. Vasquez  
Commissioner, Pct. #2

  
The Honorable Robert Beau Nettleton  
Commissioner, Pct. #3

  
The Honorable Gustavo Flores  
Commissioner, Pct. #4

ATTEST:  
  
The Honorable Generosa Gracia-Ramon  
County Clerk







January 11, 2019



TEXAS ASSOCIATION of COUNTIES

254 COUNTIES \* ONE VOICE

EST. 1969

Greetings, Healthy County Wellness Coordinator:

Thank you for coordinating the Texas Association of Counties Health and Employee Benefits Pool's Healthy County program in your county. Your visible support and commitment are vital to the success of the program.

This year, county employees earned Amazon e-gift cards as incentive prizes through program participation. Employees received a \$50 Amazon e-gift card on the Healthy County powered by Provant portal for completing three of four Healthy County challenges between Feb. 12 and Nov. 11

Additionally, the Pool acknowledges and rewards your county's support with *Employer Rewards*. Since each county is unique with different wellness goals, Healthy County provides funding that allows flexibility to implement health and wellness initiatives appropriate for your county. Healthy County encourages the county to use these funds to re-invest in workplace wellness initiatives.

Counties earned a percentage of the maximum allowed amount (see table below) based on the number of employees who earned the \$50 incentive. The maximum amount was based on the number of covered employees in your county and the percent who earned the \$50 incentive. A check for this amount is enclosed.

| Group Size        | Max Amount Available to Earn            |
|-------------------|---|
| 25 Lives or Less  | \$50x employee who earned the incentive |
| 26-50 Lives       | \$3,000                                 |
| 51-99 Lives       | \$5,000                                 |
| 100-199 Lives     | \$7,000                                 |
| 200 Lives or More | \$9,000                                 |

The *Employer Rewards* informational leaflet, which is enclosed, explains the *who, what, how and why's* of the *Employer Rewards* program, and provides recommendations on how these incentives can be used. Please share the *Employer Rewards* information with your county's Commissioners Court, wellness sponsor, and other wellness team members to determine the most effective plan of action for your county's *Employer Rewards*.

Please contact your Healthy County Wellness Consultant at (800) 456-5974 should you have questions.

In appreciation,  
Healthy County Wellness Team

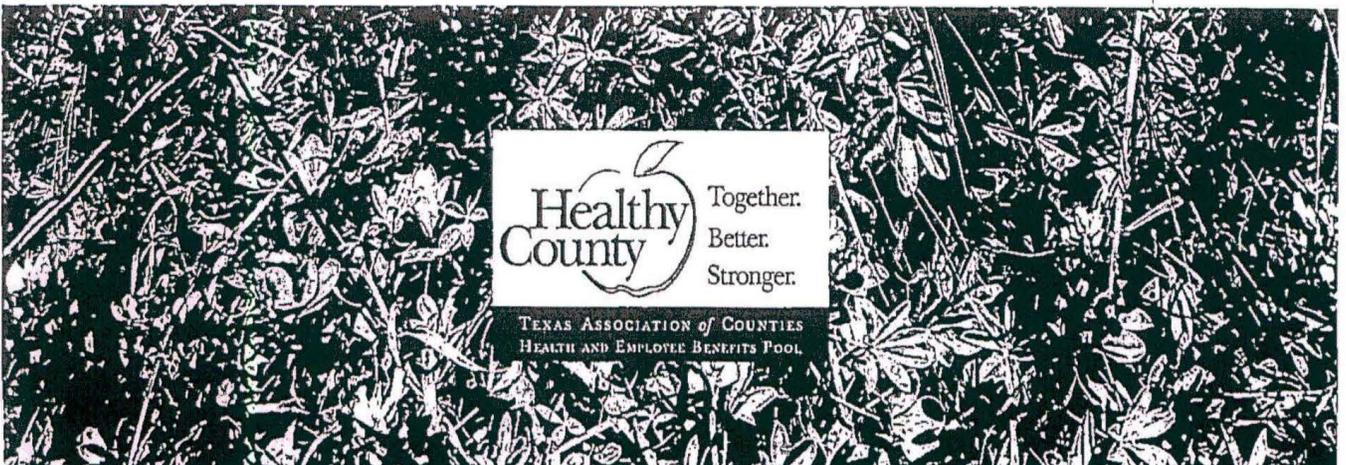
(512) 478-8753 • (800) 456-5974 • (512) 478-8481 FAX • www.county.org • 1210 San Antonio, Austin, TX 78701 • P.O. Box 2131, Austin, TX 78768-2131

Susan M. Redford, Executive Director



# HEALTHY COUNTY

## 2018 Employer Rewards



## Healthy County 2018 Employer Rewards

The mission of Healthy County, the Texas Association of Counties Health and Employee Benefits Pool wellness program, is to optimize the health and well-being of its members.

### What is the Healthy County Employer Rewards program?

A successful wellness program requires effort and support at the local level. The Healthy County Employer Rewards program honors participating members for their efforts and success in helping employees enroll and complete various Healthy County programs. The Texas Association of Counties Health and Employee Benefits Pool grants eligible employers funds based on the amount their employees earn in incentive prizes through program participation. A member county may use the Pool's funds for future health and wellness initiatives.

### Who is eligible to receive employer rewards?

An Employer is eligible to receive a reward if they:

- Are a member of the Pool (ASO groups are not eligible);
- Designate a wellness coordinator and wellness sponsor

### How do members earn employer rewards?

Members earn rewards based on their employees' participation in Healthy County activities. For 2018, employees are eligible to receive a \$50 Amazon gift card by completing three out of the four Healthy County challenges.

Counties will earn a percentage of the maximum allowed amount (see table below) based on the number of employees who earned the \$50 Amazon gift card. The maximum amount will be based on the number of covered employees.

| Group Size               | Max Amount Available to Earn            |
|--------------------------|---|
| Under less than 25 Lives | \$50x employee who earned the incentive |
| 26-50 Lives              | \$3,000                                 |
| 50-99 Lives              | \$5,000                                 |
| 100-199 Lives            | \$7,000                                 |
| Over 200 Lives           | \$9,000                                 |

**Example:** County A has 100 employees. 28 percent of their employees earn the \$50 incentive. The county will earn \$1,960 (28 percent of \$7,000) in Employer Rewards for 2017 participation.

### Why is the Pool doing this?

The Pool's intention is to provide members with resources to build a positive, healthy and safe work environment and to encourage employees to engage in healthier behaviors.

The Pool's members, including elected officials and employees of Texas counties, represent one of our state's most valuable assets - public servants to all Texas citizens. When officials and employees are healthy, they are better able to provide quality service, manage stress appropriately, experience fewer lost workdays and model healthy behaviors for their families and the community. Healthy employees also save taxpayers' money due to lower health care costs and workers' compensation costs, as well as a reduced rate of absenteeism. The Pool's ultimate goals are to reduce health care costs and make better use of taxpayers' dollars by improving the quality of your employees' health.

### How can a member use the Healthy County employer rewards?

The Pool recommends reward funds be applied toward the member's wellness program and:

- be health related;
- be available to all employees; and
- promote ongoing attention to health initiatives that provide lasting benefits.

### Ideas for how to use Employer Rewards:

- **To provide healthy evidence-based worksite and safety programs.** Trainings can arm individuals with new knowledge about their own health and safety. Examples include: flu, pneumonia and adult vaccinations; biometric screening for cholesterol, triglycerides, blood glucose and blood pressure; learning lunches or educational programs (like those provided by Agrilife Extension Agents such as Do Well Be Well with Diabetes and Step Up & Scale Down); and ergonomic training.
- **To support the people who are responsible for coordinating county health initiatives, building infrastructure and promoting employee wellness.** Health initiatives are more effective when the person assigned to promote the program is provided with time and resources necessary to meet identified objectives.

## Healthy County 2018 Employer Rewards

Examples include: county officials allowing time and budgeting financial resources for the Healthy County wellness coordinator to roll out programs and organize wellness initiatives.

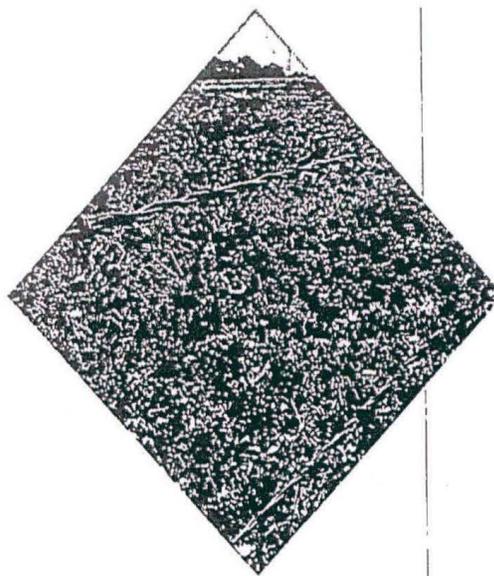
- **To prepare and implement safety, health and wellness policies.** Policies that reinforce healthy lifestyle efforts encourage a healthy worksite culture. Examples include: smoke free policies, clean-air maintenance plan; allowing a flextime schedule to encourage exercise during lunch; and creating a media library for employees to check-out educational DVDs on various health and safety topics such as stress management, the risks of obesity, balancing work and home life, co-worker dynamics, and the importance of physical exercise, etc.
- **To improve environmental working conditions.** Health and productivity are increased by identifying ways to improve the employees' physical work environment and implementing changes. Examples include: installing hands-free fixtures (faucets, flushers, soap and paper towel dispensers) in restrooms and kitchens to slow down the spread of infections; purchasing a kiosk computer to provide Internet access for those without a work or home computer; conducting a worksite wellness audit; developing walking routes and trails near the worksite; installing bike racks or creating a bike storage area; installing slip-resistant flooring and guardrails; providing shower and changing facilities; setting up motivational signs; and adding rubber treading to stairs or carpet to encourage stair climbing at the worksite.
- **To purchase fitness equipment.** The purchase of fitness equipment for a county owned and operated fitness center is permitted. Or the purchase (or subsidize) of physical activity tracking devices, such as a Fitbit or Garmin for employees. Funds may also be used to purchase equipment, such as the Fitbit or Garmin scale.
- **To improve the nutritional value of food products available to elected officials and county employees.** Healthier food choices during the work day equal healthier adults.

Examples include: purchasing (or subsidizing) a healthy snack machine with items such as fat-free milk, fruits, low-calorie snacks and caffeine-free beverages; and hosting a Farmer's Market during peak growing seasons.

- **To encourage participation and sustain employee engagement in health and wellness activities.** The purchase of incentives is permitted, subject to restrictions in state and federal law.

*Health Insurance Portability and Accountability Act (HIPAA) Wellness Program Rules:*

- Classify wellness programs as either participatory or health-contingent, with different rules for each;
- Classify health-contingent wellness programs as either activity-based or outcome-based, with different rules for each; and
- Set out five requirements for health-contingent wellness programs:
  - Includes annual opportunity to qualify for reward;
  - Sets limits on amount of award based on cost of employee-only coverage;
  - Requires program be reasonably designed to promote health or prevent disease;
  - Requires program include a reasonable alternative method for earning a reward be provided for employees who are otherwise unable to meet the requirements to earn an award; and
  - Calls for notice of availability of reasonable alternative in all program materials.





VAL VERDE COUNTY  
HUMAN RESOURCES DEPT

MEMORANDUM

#42

To: Lewis G. Owens Jr., County Judge  
From: Juanita Barrera, HR Director  
Date: January 30, 2019  
Subject: **AGENDA ITEMS FOR FEBRUARY 2019**

Listed below are several personnel matters which need to be part of the upcoming February agenda for HR reporting period from January 19, 2019 through February 5, 2019.

- A. Sergio Gonzalez, County Court At Law Judge, requesting to stop the issuance of checks to Tom Garcia, Assistant Court Coordinator, effective January 11, 2019. Mr. Garcia transferred to County Judges Office.
- B. Joe Frank Martinez, requesting the issuance of checks to Adrian Valdez, Deputy Sheriff, with a salary of \$34,986.00, effective January 22, 2019. Mr. Valdez is replacing Pedro Garcia who was promoted.
- C. Hilda Lopez, JP Pct. 4, requesting to stop the issuance of checks to Ruth Weeks, Deputy Clerk, effective January 30, 2019. Ms. Weeks has resigned.



## Cascos & Associates, PC

Certified Public Accountants  
Audit/Accounting/Tax/Consulting

COPY

#44

January 18, 2019

Honorable Lewis Owens  
County Judge  
400 Pecan Street  
Del Rio, Texas 78740

The following represents our understanding of the services we will provide to Val Verde County.

You have requested that we audit the financial statements of the governmental activities, each major fund, and the aggregate remaining fund information of Val Verde County, as of September 30, 2018, and for the year then ended, and the related notes to the financial statements, which collectively comprise Val Verde County's basic financial statements as listed in the table of contents.

In addition, we will audit the entity's compliance over major federal and state award programs for the period ended September 30, 2018. We are pleased to confirm our acceptance and our understanding of this audit engagement by means of this letter. Our audits will be conducted with the objectives of our expressing an opinion on each opinion unit and an opinion on compliance regarding the entity's major federal and state award programs.

Accounting principles generally accepted in the United States of America (U.S. GAAP), as promulgated by the Governmental Accounting Standards Board (GASB) require that management's discussion and analysis, budgetary comparison information, and pension related information be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the GASB, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. As part of our engagement, we will apply certain limited procedures to the required supplementary information (RSI) in accordance with auditing standards generally accepted in the United States of America (U.S. GAAS). These limited procedures will consist primarily of inquiries of management regarding their methods of measurement and presentation, and comparing the information for consistency with management's responses to our inquiries. We will not express an opinion or provide any form of assurance on the RSI. The following RSI is required by U.S. GAAP. This RSI will be subjected to certain limited procedures but will not be audited:

- Management's Discussion and Analysis
- Budgetary Comparison Information
- Schedules of Changes in Net Pension & OPEB Liability

Supplementary information other than RSI will accompany Val Verde County's basic financial statements. We will subject the following supplementary information to the auditing procedures applied in our audit of the basic financial statements and perform certain additional procedures, including comparing and reconciling the supplementary information to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and additional procedures in accordance with U.S. GAAS. We intend to provide an opinion on the following supplementary information in relation to the financial statements as a whole:

- Combining Statements and Schedules

---

765 East 7th Street / Brownsville, Texas 78520  
Phone (956) 544-7778 Fax (956) 544-8465  
Email: ccascos@cascoscpa.com

#44

Also, the document we submit to you will include the following other additional information that will not be subjected to the auditing procedures applied in our audit of the financial statements:

- Introductory Section
- Statistical Section

#### **Schedule of Expenditures of Federal Awards**

We will subject the schedule of expenditures of federal and state awards to the auditing procedures applied in our audit of the basic financial statements and certain additional procedures, including comparing and reconciling the schedule to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and additional procedures in accordance with auditing standards generally accepted in the United States of America. We intend to provide an opinion on whether the schedule of expenditures of federal and state awards is presented fairly in all material respects in relation to the financial statements as a whole.

#### **Data Collection Form**

Prior to the completion of our engagement, we will complete the sections of the Data Collection Form that are our responsibility. The form will summarize our audit findings, amounts and conclusions. It is management's responsibility to submit a reporting package including financial statements, schedule of expenditure of federal awards, summary schedule of prior audit findings and corrective action plan along with the Data Collection Form to the federal audit clearinghouse. The financial reporting package must be text searchable, unencrypted, and unlocked. Otherwise, the reporting package will not be accepted by the federal audit clearinghouse. We will assist you in the electronic submission and certification. You may request from us copies of our report for you to include with the reporting package submitted to pass-through entities.

The Data Collection Form is required to be submitted within the earlier of 30 days after receipt of our auditors' reports or nine months after the end of the audit period, unless specifically waived by a federal cognizant or oversight agency for audits. Data Collection Forms submitted untimely are one of the factors in assessing programs at a higher risk.

#### **Audit of the Financial Statements**

We will conduct our audit in accordance with U.S. GAAS, the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States of America; the audit requirements of Title 2 U.S. Code of Federal Regulations (CFR) Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance); and the State of Texas' Uniform Grant Management Standards (UGMS). Those standards and the Uniform Guidance require that we plan and perform the audit to obtain reasonable assurance about whether the basic financial statements are free from material misstatement. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to error, fraudulent financial reporting, misappropriation of assets, or violations of laws, governmental regulations, grant agreements, or contractual agreements.

An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements. If appropriate, our procedures will therefore include tests of documentary evidence that support the transactions recorded in the accounts, tests of the physical existence of inventories, and direct confirmation of cash, investments, and certain other assets and liabilities by correspondence with creditors and financial institutions. As part of our audit process, we will request written representations from your attorneys, and they may bill you for responding. At the conclusion of our audit, we will also request certain written representations from you about the financial statements and related matters.

#44

Because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk that some material misstatements or noncompliance (whether caused by errors, fraudulent financial reporting, misappropriation of assets, detected abuse, or violations of laws or governmental regulations) may not be detected exists, even though the audit is properly planned and performed in accordance with U.S. GAAS and *Government Auditing Standards* of the Comptroller General of the United States of America. Please note that the determination of abuse is subjective, and *Government Auditing Standards* does not require auditors to detect abuse.

In making our risk assessments, we consider internal control relevant to the entity's preparation and fair presentation of the basic financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. However, we will communicate to you in writing concerning any significant deficiencies or material weaknesses in internal control relevant to the audit of the financial statements that we have identified during the audit. Our responsibility as auditors is, of course, limited to the period covered by our audit and does not extend to any other periods.

We will issue a written report upon completion of our audit of Val Verde County's basic financial statements. Our report will be addressed to the governing body of Val Verde County. We cannot provide assurance that unmodified opinions will be expressed. Circumstances may arise in which it is necessary for us to modify our opinions, add an emphasis-of-matter or other-matter paragraph(s), or withdraw from the engagement. If our opinions on the basic financial statements are other than unmodified, we will discuss the reasons with you in advance. If, for any reason, we are unable to complete the audit or are unable to form or have not formed opinions, we may decline to express opinions or to issue a report as a result of this engagement.

In accordance with the requirements of *Government Auditing Standards*, we will also issue a written report describing the scope of our testing over internal control over financial reporting and over compliance with laws, regulations, and provisions of grants and contracts, including the results of that testing. However, providing an opinion on internal control and compliance over financial reporting will not be an objective of the audit and, therefore, no such opinion will be expressed.

#### **Audit of Major Program Compliance**

Our audit of Val Verde County's major federal and state award program(s) compliance will be conducted in accordance with the requirements of the Single Audit Act, as amended; and the Uniform Guidance and UGMS, and will include tests of accounting records, a determination of major programs in accordance with the Uniform Guidance, UGMS, and other procedures we consider necessary to enable us to express such an opinion on major federal and state award program compliance and to render the required reports. We cannot provide assurance that an unmodified opinion on compliance will be expressed. Circumstances may arise in which it is necessary for us to modify our opinion or withdraw from the engagement.

The Uniform Guidance and UGMS requires that we also plan and perform the audit to obtain reasonable assurance about whether the entity has complied with applicable laws and regulations and the provisions of contracts and grant agreements applicable to major federal and state award programs. Our procedures will consist of determining major federal and state programs and performing the applicable procedures described in the U.S. Office of Management and Budget (OMB) Compliance Supplement UGMS for the types of compliance requirements that could have a direct and material effect on each of the entity's major programs. The purpose of those procedures will be to express an opinion on the entity's compliance with requirements applicable to each of its major programs in our report on compliance issued pursuant to the Uniform Guidance and UGMS.

Also, as required by the Uniform Guidance and UGMS, we will perform tests of controls to evaluate the effectiveness of the design and operation of controls that we consider relevant to preventing or detecting material noncompliance with compliance requirements applicable to each of the entity's major federal and state award programs. However, our tests will be less in scope than would be necessary to render an opinion on these controls and, accordingly, no opinion will be expressed in our report.

#44

We will issue a report on compliance that will include an opinion or disclaimer of opinion regarding the entity's major federal and state award programs, and a report on internal controls over compliance that will report any significant deficiencies and material weaknesses identified; however, such report will not express an opinion on internal control.

#### **Management's Responsibilities**

Our audit will be conducted on the basis that management and, when appropriate, those charged with governance acknowledge and understand that they have responsibility:

1. For the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America;
2. For the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of the basic financial statements that are free from material misstatement, whether due to error, fraudulent financial reporting, misappropriation of assets, or violations of laws, governmental regulations, grant agreements, or contractual agreements;
3. For identifying, in its accounts, all federal and state awards received and expended during the period and the federal and state programs under which they were received, including federal and state awards and funding increments received prior to December 26, 2014 (if any), and those received in accordance with the Uniform Guidance and UGMS (generally received after December 26, 2014);
4. For maintaining records that adequately identify the source and application of funds for federally and state funded activities;
5. For preparing the schedule of expenditures of federal and state awards (including notes and noncash assistance received) in accordance with the Uniform Guidance and UGMS requirements;
6. For the design, implementation, and maintenance of internal control over federal and state awards;
7. For establishing and maintaining effective internal control over federal and state awards that provides reasonable assurance that the nonfederal entity is managing federal and state awards in compliance with federal and state statutes, regulations, and the terms and conditions of the federal and state awards;
8. For identifying and ensuring that the entity complies with federal and state statutes, regulations, and the terms and conditions of federal and state award programs and implementing systems designed to achieve compliance with applicable federal and state statutes, regulations, and the terms and conditions of federal and state award programs;
9. For disclosing accurately, currently, and completely the financial results of each federal and state award in accordance with the requirements of the award;
10. For identifying and providing report copies of previous audits, attestation engagements, or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented;
11. For taking prompt action when instances of noncompliance are identified;
12. For addressing the findings and recommendations of auditors, for establishing and maintaining a process to track the status of such findings and recommendations and taking corrective action on reported audit findings from prior periods and preparing a summary schedule of prior audit findings;
13. For following up and taking corrective action on current year audit findings and preparing a corrective action plan for such findings;
14. For submitting the reporting package and data collection form to the appropriate parties;

#44

15. For making the auditor aware of any significant contractor relationships where the contractor is responsible for program compliance;
16. To provide us with:
  - a. Access to all information of which management is aware that is relevant to the preparation and fair presentation of the basic financial statements, and relevant to federal and state award programs, such as records, documentation, and other matters;
  - b. Additional information that we may request from management for the purpose of the audit; and
  - c. Unrestricted access to persons within the entity from whom we determine it necessary to obtain audit evidence.
17. For including the auditor's report in any document containing basic financial statements that indicates that such basic financial statements have been audited by the entity's auditor;
18. For adjusting the basic financial statements to correct material misstatements and confirming to us in the management representation letter that the effects of any uncorrected misstatements aggregated by us during the current engagement and pertaining to the current year period(s) under audit are immaterial, both individually and in the aggregate, to the basic financial statements as a whole;
19. For acceptance of nonattest services, including identifying the proper party to oversee nonattest work;
20. For maintaining adequate records, selecting and applying accounting principles, and safeguarding assets;
21. For informing us of any known or suspected fraud affecting the entity involving management, employees with significant role in internal control and others where fraud could have a material effect on compliance;
22. For the accuracy and completeness of all information provided;
23. For taking reasonable measures to safeguard protected personally identifiable and other sensitive information; and
24. For confirming your understanding of your responsibilities as defined in this letter to us in your management representation letter.

With regard to the supplementary information referred to above, you acknowledge and understand your responsibility (a) for the preparation of the supplementary information in accordance with applicable criteria, (b) to provide us with the appropriate written representations regarding the supplementary information, (c) to include our report on the supplementary information in any document that contains the supplementary information and that indicates that we have reported on such supplementary information, and (d) to present the supplementary information with the audited basic financial statements, or if the supplementary information will not be presented with the audited basic financial statements, to make the audited basic financial statements readily available to the intended users of the supplementary information no later than the date of issuance by you of the supplementary information and our report thereon.

With respect to any nonattest services we perform, such as preparation, of financial statements and related note disclosures and the schedule of expenditures of federal awards. The entity's management is responsible for (a) making all management decisions and performing all management functions; (b) assigning a competent individual to oversee the services; (c) evaluating the adequacy of the services performed; (d) evaluating and accepting responsibility for the results of the services performed; and (e) establishing and maintaining internal controls, including monitoring ongoing activities. These nonaudit services do not constitute an audit under *Government Auditing Standards* and such services will not be conducted in accordance with *Government Auditing Standards*.

*Government Auditing Standards* require that we document an assessment of the skills, knowledge, and experience of management, should we participate in any form of preparation of the financial statements and related schedules or disclosures as these actions are deemed a non-audit service.

#44

As part of our audit process, we will request from management and, when appropriate, those charged with governance, written confirmation concerning representations made to us in connection with the audit.

We understand that your employees will prepare all confirmations we request and will locate any documents or invoices selected by us for testing.

If you intend to publish or otherwise reproduce the financial statements and make reference to our firm, you agree to provide us with printers' proofs or masters for our review and approval before printing. You also agree to provide us with a copy of the final reproduced material for our approval before it is distributed.

With regard to the electronic dissemination of audited financial statements, including financial statements published electronically on your website, you understand that electronic sites are a means to distribute information and, therefore, we are not required to read the information contained in these sites or to consider the consistency of other information in the electronic site with the original document.

#### **Provisions of Engagement Administration, Timing and Fees**

We will schedule the engagement based in part on deadlines, working condition, and the availability of your key personnel. We will plan the engagement based on the assumption that your personnel will cooperate and provide assistance by performing tasks such as preparing requested schedules, retrieving supporting documents, and preparing confirmations. If for whatever reason your personnel are unavailable to provide the necessary assistance in a timely manner, it may substantially increase the work we have to do to complete the engagement within the established deadlines, resulting in an increase in fees over our original fee estimate.

Mr. Carlos H. Cascos, CPA is the engagement partner for the audit services specified in this letter. His responsibilities include supervising Cascos & Associates, PC's services performed as part of this engagement and signing or authorizing another qualified firm representative to sign the audit report.

Our fees for these services will be at our standard hourly rates plus out-of-pocket costs (such as; report reproductions, word processing, postage, travel, copies, telephone, etc.) except that we agree that our gross fee, including expenses, will not exceed \$42,500. Our standard hourly rates vary according to the degree of responsibility involved and the experience level of the personnel assigned to your audit. Our invoices for these fees will be rendered each month as work progresses and are payable on presentation. In accordance with our firm policies, work may be suspended if your account becomes 30 days or more overdue and may not be resumed until your account is paid in full. If we elect to terminate our services for nonpayment, our engagement will be deemed to have been completed upon written notification of termination, even if we have not completed our report(s). You will be obligated to compensate us for all time expended and to reimburse us for all out-of-pocket costs through the date of termination. The above fee is based on anticipated cooperation from your personnel and the assumption that unexpected circumstances will not be encountered during the audit. If significant additional time is necessary, we will discuss it with you and arrive at a new fee estimate before we incur the additional cost.

#### **Other Matters**

During the course of the engagement, we may communicate with you or your personnel via fax or e-mail, and you should be aware that communication in those mediums contains a risk of misdirected or intercepted communications.

Our firm may transmit confidential information that you provided us to third parties in order to facilitate delivering our services to you. For example, such transmissions might include, but not be limited to investment information. We have obtained confidentiality agreements with all our service providers to maintain the confidentiality of your information and we will take reasonable precautions to determine that they have the appropriate procedures in place to prevent the unauthorized release of confidential information to others. We will remain responsible for the work provided by any third-party service providers used under this agreement. By your signature below, you consent to having confidential information transmitted to entities outside the firm. Please feel free to inquire if you would like additional information regarding the transmission of confidential information to entities outside the firm.

#44

The audit documentation for this engagement is the property of Cascos & Associates, PC and constitutes confidential information. However, we may be requested to make certain audit documentation available to state and federal agencies and the U.S. Government Accountability Office pursuant to authority given to it by law or regulation, or to peer reviewers. If requested, access to such audit documentation will be provided under the supervision of Cascos & Associates, PC's personnel. Furthermore, upon request, we may provide copies of selected audit documentation to these agencies and regulators. The regulators and agencies may intend, or decide, to distribute the copies of information contained therein to others, including other governmental agencies. We agree to retain our audit documentation or work papers for a period of at least five years from the date of our report.

Further, we will be available during the year to consult with you on financial management and accounting matters of a routine nature.

During the course of the audit, we may observe opportunities for economy in, or improved controls over, your operations. We will bring such matters to the attention of the appropriate level of management, either orally or in writing.

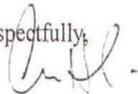
You agree to inform us of facts that may affect the financial statements of which you may become aware during the period from the date of the auditor's report to the date the financial statements are issued.

At the conclusion of our audit engagement, we will communicate to management and those charged with governance the following significant findings from the audit:

- Our view about the qualitative aspects of the entity's significant accounting practices;
- Significant difficulties, if any, encountered during the audit;
- Uncorrected misstatements, other than those we believe are trivial, if any;
- Disagreements with management, if any;
- Other findings or issues, if any, arising from the audit that are, in our professional judgment, significant and relevant to those charged with governance regarding their oversight of the financial reporting process;
- Material, corrected misstatements that were brought to the attention of management as a result of our audit procedures;
- Representations we requested from management;
- Management's consultations with other accountants, if any; and
- Significant issues, if any, arising from the audit that were discussed, or the subject of correspondence, with management.

Please sign and return the attached copy of this letter to indicate your acknowledgment of, and agreement with, the arrangements for our audit of the basic financial statements compliance over major federal and state award programs including our respective responsibilities.

We appreciate the opportunity to be your financial statement auditors and look forward to working with you and your staff.

Respectfully,  


Cascos & Associates, PC  
Brownsville, Texas

RESPONSE:

This letter correctly sets forth our understanding.

#44

Val Verde County

Acknowledged and agreed on behalf of Val Verde County by:

Name: Levin A. Owen

Title: County Judge Val Verde

Date: 2-6-19

#44

Form **W-9**  
(Rev. October 2018)  
Department of the Treasury  
Internal Revenue Service

### Request for Taxpayer Identification Number and Certification

Give Form to the  
requester. Do not  
send to the IRS.

Go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9) for instructions and the latest information.

Print or type  
See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.  
**Cascos & Associates, PC**

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

Individual/sole proprietor or single-member LLC

C Corporation

S Corporation

Partnership

Trust/estate

Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) **▶** \_\_\_\_\_

**Note:** Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

Other (see instructions) **▶** \_\_\_\_\_

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) \_\_\_\_\_

Exemption from FATCA reporting code (if any) \_\_\_\_\_

*(Applies to accounts maintained outside the U.S.)*

5 Address (number, street, and apt. or suite no.) See instructions.  
**765 E. 7th**

6 City, state, and ZIP code  
**Brownsville, TX 78520**

7 List account number(s) here (optional)

Requester's name and address (optional)

#### Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Social security number

\_\_\_\_\_

OR

Employer identification number

83-2842934

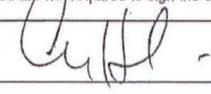
**Note:** If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

#### Part II Certification

- Under penalties of perjury, I certify that:
- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
  - I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
  - I am a U.S. citizen or other U.S. person (defined below); and
  - The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

**Certification instructions.** You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here

Signature of U.S. person **▶** 

Date **▶** **1/22/15**



PATTILLO, BROWN & HILL, L.L.P.  
CERTIFIED PUBLIC ACCOUNTANTS ■ BUSINESS CONSULTANTS

#44

January 14, 2019

Dear Sir or Madam:

Effective February 4, 2019, Pattillo, Brown Hill, LLP (Brownsville) will no longer be affiliated with Pattillo, Brown Hill, LLP (Waco). The PBH Brownsville office will change its firm name to Cascos & Associates, PC., (C&A) and thus all engagements currently with PBH Brownsville will be transferred and serviced by C&A. There will be no disruption in our scheduling or complying with our engagements that are currently planned.

This change will in no way affect the location, phone numbers, staff and quality service that PBH Brownsville has provided to all its clients over the last 23 years. Although C&A will continue servicing our South Texas clients, PBH (Waco) will continue to offer support to those clients that have used their services over the years, if and when necessary.

Should you have any questions, concerns or comments, please do not hesitate to contact me at 956.544.7778 or thru email at [ccascos@cascoscpa.com](mailto:ccascos@cascoscpa.com)

Sincerely,

Carlos H. Cascos, CPA

---

The new firm name and logo -



**Cascos & Associates, PC**  
Certified Public Accountants  
Audit/Accounting/Tax/Consulting

---

765 East 7th Street / Brownsville, Texas 78520  
Phone (956) 544-7778 Fax (956) 544-8465  
Email: [ccascos@cascoscpa.com](mailto:ccascos@cascoscpa.com)