STATEMENT OF WORK

Security Consulting Solutions

PREPARED FOR

County of Webb

Secureworks®

Release Date

12/14/2021

4.3

Engagement

Table of Contents

This Statement of Work ("**SOW**") is entered into by and between **SecureWorks, Inc.**, with its principal place of business located at **One Concourse Parkway, Suite 500, Atlanta, GA 30328** ("**Secureworks**"), and **County of Webb**, with its principal place of business located at **1110 Victoria St suite 402**, **Laredo**, **TX 78040-4428** ("**Customer**"), as of the SOW Effective Date, which is defined as the latest date in the signature blocks below unless otherwise provided in the SOW Term section herein ("**SOW Effective Date**"). Secureworks and Customer are hereafter referred to collectively as the "parties," and each, a "party." This SOW is governed by and subject to the terms and conditions of: (a) the separately signed agreement executed by the parties that expressly authorizes Customer to order the services described herein from Secureworks, or (b) the Secureworks Customer Relationship Agreement available at https://www.secureworks.com/cra-us (the "**CRA**"), which is incorporated by reference in its entirety herein. Capitalized terms not defined herein shall have the meaning ascribed to them in the CRA.

1 Scope

Under this SOW, Secureworks will provide Customer with the **Emergency Incident Response** service ("**Service**") as such Service is described in detail below.

1.1 Emergency Incident Response Services

Secureworks will provide EIR that can be conducted remotely or on-site. The activities conducted can include but are not limited to the following:

- Incident support and coordination
- Digital media handling guidance and support
- Deployment support for host-based, network-based, and log analysis technologies
- Network analysis services
- Incident response and digital forensic analysis of online and offline infrastructure and datasets from customer's on-premises and cloud assets
- Malware analysis and reverse engineering
- Containment planning guidance
- Periodic Engagement Status Updates, in accordance with the mutually agreed-upon communication plan for each Engagement
- Engagement-specific Deliverables, in accordance with the mutually agreed-upon deliverables for each Engagement

Note: Each Customer-approved request for EIR is referred to as an Engagement.

Customer agrees to the purchased hours as set forth in Service Fees and Expenses section below ("**Committed Hours**").

The work provided by Secureworks described within this SOW will be delivered according to Customer-provided information located in Appendix 1: Additional Scoping Detail.

1.1.1 Digital Forensic Analysis

As part of EIR, Secureworks may acquire and analyze a variety of formats for forensic analysis of digital media and artifacts to assess compromise activity, including but not limited to the following:

- Disk images
- Memory images
- Mobile devices

- Network packet captures
- Plain text log files

1.1.2 Malware Analysis and Reverse Engineering

As part of EIR, Secureworks may perform static, dynamic, and reverse engineering analysis to assist in understanding the function of Customer-supplied files.

Secureworks will provide analysis results, to include cyber threat intelligence based on correlation across Secureworks datasets and will advise on mitigation actions to reduce the impact of the sample on Customer's infrastructure.

1.1.3 Periodic Engagement Status Updates

Periodic Engagement Status Updates, which may be verbal or written, will be provided to Customer during the Engagement and may include the following:

- Summary of completed activities
- Issues requiring attention
- Planning for the next work effort period

The work provided by Secureworks described within this SOW will be delivered according to Customer-provided information located in Additional Scoping Detail Appendix.

1.2 Out of Scope

Secureworks reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein
- Are beyond the capability of Secureworks to deliver within the contracted service levels
- Might violate legal or regulatory requirements

2 Service Delivery

2.1 Delivery Coordination

Secureworks will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes the following:

- Develop delivery timeline with Customer and with Secureworks personnel
- Work with Customer to identify and address issues or concerns that impact service delivery
- Periodic, high-level updates on progress
- Confirm delivery and procure project sign-off

2.2 Scheduling

Upon scoping and identifying the nature of the cyber incident, Secureworks personnel will be scheduled in a manner that is appropriate for Customer's response objectives, specified sense of urgency, and applicable laws or ordinances, and an appropriate timeline for working on the cyber incident will be determined.

2.3 Consulting Services Delivery

The Service(s) will be delivered remotely from a secure location and/or at Customer site(s) depending upon agreement between Customer and Secureworks or as defined in the SOW.

Customer's primary location:

County of Webb

1110 Victoria St suite 402

Laredo, TX 78040-4428

Secureworks solely reserves the right to refuse to travel to locations deemed unsafe by Secureworks or locations that would require a forced intellectual property transfer by Secureworks. Secureworks solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Secureworks. Customer will be notified at the time that Services are requested if Secureworks refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Secureworks travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Secureworks restrict travel to any location, Secureworks may at its election (i) deliver the Services remotely or (ii) postpone the Services until travel is permitted. If neither option (i) nor (ii) in the preceding sentence is feasible, Secureworks may terminate the affected Services and provide Customer with a refund of any unused, prepaid fees.

3 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder are dependent on Customer's compliance with these obligations.

- Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- For on-site activities, Customer will provide a suitable workspace for Secureworks personnel, and necessary access to systems, network, and devices.
- Replies to all requests are prompt and in accordance with the delivery dates established in the Scheduling phase.
- Customer-scheduled interruptions and maintenance intervals will allow adequate time for Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent any disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP).

4 Deliverable Components

Listed in the table below are the standard deliverables for the Service. Secureworks will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Report	Delivery Schedule	Delivery Method
	Status Updates	Mutually agreed upon	Mutually agreed upon

Service	Report	Delivery Schedule	Delivery Method
Emergency Incident Response	Final	Upon completion of Engagement	Mutually agreed upon

4.1 Engagement-specific Deliverables and Timing

Presentation of deliverables and findings compiled by Secureworks in the performance of the Service(s) (the "**Engagement-specific Deliverables**") are tailored to work performed, and to Customer's needs. Engagement-specific Deliverables Final Report may include the following:

- Executive summary, outlining key findings and recommendations
- Methods, detailed findings, narratives, and recommendations
- Attachments providing relevant details and supporting data

During the beginning phases of an Engagement, if a Final Report has been mutually agreed upon as an Engagement-specific Deliverable, then Secureworks will issue a Final Report draft to the Customer-designated point of contact within three (3) weeks of completing an Engagement. Customer shall then have three (3) weeks from Secureworks delivery of the Final Report draft to provide comments. Should Customer provide comments, the Final Report shall be deemed complete upon the earlier of the date which (1) Secureworks provides responses to these comments or (2) Secureworks delivers a revised Final Report. If no comments are received from Customer before the expiration of the review period, or upon Customer's written acceptance of the Report, the Final Report will be deemed complete and referred to as the "Completed Final Report."

5 Service Fees and Expenses

Until this SOW is fully executed by both parties, the fees proposed herein are only valid for 90 days from the date received.

5.1 Service Fees

Service Name	Committed Hours	Fee	Total Fee
Emergency Incident Response	44	472.50 USD	$20,790 USD

5.2 Billing Terms

- Service Fees for Committed Hours are 100% billable upon the SOW Effective Date
- Additional hourly fees for the Service are billable monthly in arrears as hours are consumed

5.2.1 Additional Hours

- Additional blocks of hours may be purchased in advance of or upon exhaustion of contracted hours at the contracted rate referenced in in the Services Fees Section via e-mail authorization from Customer.
- Requests for additional hours must be sent by e-mail from Customer to irservices@secureworks.com and Customer acknowledges and agrees that any such e-mail will be from a representative of Customer authorized to commit Customer to the purchase of the additional hours and is binding on Customer.

- Customer acknowledges and agrees that if Purchase Orders (P.O.s) are required for the transaction with Secureworks to extend the Committed Hours, an updated P.O. will be issued to Secureworks for the number of hours specified in the authorizing e-mail within seven (7) calendar days from the date of the acknowledged receipt of the email by Secureworks. If an updated P.O. is not received within seven (7) calendar days, then Secureworks may terminate the Engagement as applicable and, notwithstanding the foregoing, Customer acknowledges and agrees that it remains responsible for any additional work performed by Secureworks until such P.O. is received.

5.2.2 Committed Hours

- Customer may terminate an Engagement by providing 24-hour advance notice to stop all work against this SOW. Committed Hours will be forfeited if Engagement is terminated prior to exhaustion of those hours.
- Notice for termination of Engagement must be sent by email to irservices@secureworks.com
- Consumed hours will be calculated in quarter-hour increments.
- All Committed Hours are non-refundable and non-transferable for other Secureworks services. Any unused hours within a given year expire and are forfeited on the anniversary of SOW execution.

5.3 Expenses

Customer agrees to reimburse Secureworks for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include but are not limited to the following:

- Travel fees related to transportation, meals, and lodging to perform the Services, including travel to the Customer location(s)
- Digital media storage, Engagement-specific equipment, or licensing necessary for tailored digital forensic analysis work
- Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, if Secureworks and Customer agree that usage is necessary to complete the Engagement

6 SOW Term

The term of this SOW (the "**SOW Term**") shall commence upon the SOW Effective Date and terminate on the earlier to occur of one of the following: (i) the date which is one (1) year thereafter, or (ii) the completion of the Services.

7 Security Consulting Disclaimers

7.1 On-site Services

Notwithstanding Secureworks' employees' placement at Customer's location(s), Secureworks retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses.

7.2 Security Services

Should this SOW include security scanning, testing, assessment, forensics, or remediation Services ("**Security Services**"), Customer understands that Secureworks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Customer hereby authorizes Secureworks to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Customer from time to time) on network resources with the internet protocol ("**IP**") addresses identified by Customer. Secureworks shall perform the Security Services during a timeframe mutually agreed upon with Customer. The Security Services may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom-coded applications, but will exclude intentional and deliberate denial of service ("**DoS**") attacks. Furthermore, Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes Secureworks to provide any or all of the Security Services with respect to Customer's systems. Customer further acknowledges that it is Customer's responsibility to restore network computer systems to a secure configuration after Secureworks completes testing.

7.3 Record Retention

Secureworks will retain a copy of the Customer Reports in accordance with Secureworks' record retention policy. Unless Customer gives Secureworks written notice to the contrary prior thereto and subject to the provisions of the CRA and DPA, all Customer Data will be deleted within 30 days from issuance of the final Customer Report unless Secureworks is legally required to retain such Customer Data for a longer period. Notwithstanding the foregoing, Secureworks shall be entitled to retain Customer Data as necessary to comply with any legal, regulatory, judicial, audit, or internal compliance requirements.

7.4 Compliance Services

Should this SOW include compliance testing or assessment or other similar compliance advisory Services ("**Compliance Services**"), Customer understands that, although Secureworks' Compliance Services may discuss or relate to legal issues, Secureworks does not provide legal advice or services, none of such Compliance Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Secureworks in connection with any Compliance Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

7.5 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after the completed Engagement, Secureworks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Secureworks in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Secureworks any special requirements for Secureworks to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Secureworks will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Secureworks will provide a confirmation letter to Customer addressing completion and scope of these post-Engagement activities, in Secureworks' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Secureworks shall, in its sole discretion, dispose of the Engagement Media on or after the Engagement conclusion and only maintain a copy of the completed Engagement-specific Deliverables.

7.6 Legal Proceedings

If Customer knows or has reason to believe that Secureworks or its employees performing Services under this SOW have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Secureworks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks for (a) its employees' time spent as to such response at the hourly fee reflected in this SOW, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Secureworks as to the Services or this SOW.

7.7 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of an Engagement, within thirty (30) days following the date of the Completed Final Report (the "**Thirty Day Period**"), Customer shall uninstall any and all copies of the software agent used for the Engagement. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Secureworks' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Secureworks from the software agent. Customer will uninstall the software agent as described in this SOW.

This SOW is agreed to by the parties. Any terms and conditions attached to a purchase order submitted by Customer in connection with this SOW are null and void.

SecureWorks, Inc.		County of Webb	
By:	.....	By:	.....
Printed:	.....	Printed:	.....
Title:	.....	Title:	.....
Date:	.....	Date:	.....

Billing Contact Information – This is where your invoicing will be emailed

Contact Name		**Phone/Fax#**	
Role		**Billing Portal Y/N**	
Email		**If yes, what Portal Provider**	
V4.3			

Secureworks Sales Team Contact

Account Executive	Brian Herman
Email	bherman@secureworks.com
Phone	561-703-7567
Sales Engineer	

Appendix 1: Additional Scoping Detail

8 Emergency Incident Response Scoping Details

The information below was provided by Customer to derive scope and pricing described within this SOW. Secureworks will deliver the services described herein according to this information. Significant changes to the Customer environment that exceed this information may result in scope changes and additional fees, as documented through a Change Order. Customer and Secureworks agree to follow the Change Control guidelines as indicated in the CRA

Additional Scoping Detail:

1) Engagement Codename: TBD
2) Engagement Contact Information:

County of Webb	
Engagement Address	Remote
Point of Contact Name	Gus Ornelas
Point of Contact Email Address	gornelas@webbcountytx.gov
Point of Contact Primary Telephone Number	956-523-4893
Point of Contact Secondary Telephone Number	m956-326-0545

3) Incident Management Services Scope of Work:
   - Forensic analysis of the following systems/evidence:
     - Deploy up to 2,000 Red Cloak Windows endpoints to identify and timeline threat activity
     - Triage analysis of two (2) Exchange servers to timeline threat activity
4) Incident Management Services Deliverables:
   - Daily email updates on status of analysis
   - Final report within 3 weeks of completion of analysis
5) Incident Management Services Billable Retainer Hours Estimate*:
   - 44-60
6) Customer Responsibilities:
   - Deploy up to 2,000 Red Cloak endpoint agents
   - Respond to escalations and requests for additional context
   - Provide permission to use F-Response for Exchange server triage data retrieval

* The Retained Hours necessary for the completion of an Engagement may vary depending on the Customer requests and the complexity of the circumstances for such Service chosen.

7) Remote Digital Forensic Analysis Engagement Milestones:

Milestone	**Timeframe for Completion**	**Responsible Party**
Evidence Collection and Transport	Within 1-3 business days of engagement kickoff.	Customer Technical Point of Contact
Evidence Examination	Within 1-2 business days of receipt of evidence.	SecureWorks Incident Response Practice
Digital Forensic Analysis	Iterative analysis of submitted items will be completed in support of engagement scope and objectives.	SecureWorks Incident Response Practice
Reporting	Recurring status reports during analysis and final engagement report delivered within three (3) weeks from completion of analysis.	SecureWorks Incident Response Practice