# PROFESSIONAL SERVICES AGREEMENT BETWEEN
# THE CITY OF DORAL
# AND
# CLARIUM MANAGED SERVICES
# FOR
# SECURITY OPERATION CENTER REMOTE MONITORING

**THIS AGREEMENT**, dated as of the 15 day of August, 2019, is made between **SUNSHINE COMPUTERS AND SOFTWARE INC. D/B/A/CLARIUM MANAGED SERVICES** a Florida corporation, (hereinafter the "Consultant"), and the **CITY OF DORAL, FLORIDA,** a Florida municipal corporation, (hereinafter the "City").

**WHEREAS,** the Consultant and City, through mutual negotiation, have agreed upon a scope of services, schedule, and fee for a three-year (3) remote monitoring of security devices and services that form part or whole of City of Doral eco-system (the "Project"); and

**WHEREAS,** the City desires to engage the Consultant to perform the services specified below.

**NOW, THEREFORE,** in consideration of the mutual covenants and conditions contained herein, the Consultant and the City agree as follows.

1. **Scope of Services/Deliverables.**

1.1 The Consultant shall furnish professional services to the City as set forth in the Scope of Services.

1.2 The "Scope of Services" includes a Project Schedule for the Project which includes a breakdown of tasks, timeline and deliverables to the City which is attached and incorporated as Exhibit "A".

2. **Term/Commencement Date.**

2.1 This Agreement shall become effective upon execution by both parties and shall remain in effect through December 31, 2021, unless earlier terminated in accordance with Paragraph 8. The City Manager may extend the term of this Agreement up to an additional 180 days by written notice to the Consultant.

2.2 Consultant agrees that time is of the essence and Consultant shall complete each deliverable for the Project within the timeframes set forth in the Project Schedule, unless extended by the City Manager.

3. **Compensation and Payment.**

3.1 The Consultant shall be compensated in the following manner:

The City shall pay Provider One Time Costs for Phase 1 Support (Palo Alto Networks) of $17,129.76. Also Phase 3 monthly recurring costs of $4,900.00 fixed for 36-month term (as set forth in EXHIBIT A Proposal attached hereto and made a part hereof).

3.2 The City shall pay Consultant in accordance with the Florida Prompt Payment Act.

3.3 If a dispute should occur regarding an invoice submitted, the City Manager may withhold payment of the disputed amount and may pay to the Consultant the undisputed portion of the invoice. Upon written request of the Finance Director, the Consultant shall provide written documentation to justify the invoice. Any compensation disputes shall be decided by the City Manager whose decision shall be final.

4. **SubConsultants.**

4.1 The Consultant shall be responsible for all payments to any sub-Consultants and shall maintain responsibility for all work related to the Project.

4.2 Any sub-Consultants used on the Project must have the prior written approval of the City Manager or his designee.

5. **City's Responsibilities.**

5.1 Furnish to Consultant, at the Consultant's written request, all available maps, plans, existing studies, reports and other data pertinent to the services to be provided by Consultant, in possession of the City.

5.2 Arrange for access to and make all provisions for Consultant to enter upon real property as required for Consultant to perform services as may be requested in writing by the Consultant (if applicable).

6. **Consultant's Responsibilities.**

6.1 The Consultant shall exercise the same degree of care, skill and diligence in the performance of the Project as is ordinarily provided by a professional under similar circumstances. If at any time during the term of this

Agreement or within one year from the completion of the Project, it is determined that the Consultant's deliverables are incorrect, defective or fail to conform to the Scope of Services of the Project, upon writteh notification from the City Manager, the Consultant shall at Consultants sole expense, immediately correct the work. The City in no way assumes or shares any responsibility or liability of the Consultant or Sub Consultant under this agreement.

7. **Conflict of Interest.**

7.1 To avoid any conflict of interest or any appearance thereof, Consultant shall not, for the term of this Agreement, represent any private sector entities (developers, corporations, real estate investors, etc.), with regard to any City related matter.

8. **Termination.**

8.1 The City Manager without cause may terminate this Agreement upon thirty (30) days written notice to the Consultant. The City Manager may immediately terminate this Agreement if is as an alleged, and confirmed by the City Manager in his/her sole discretion, that a Consultant has or may have violated Federal, State, or local laws. In the event that Consultant has failed to perform in accordance with this Agreement or to take reasonable direction by the City Manager in furtherance of this Agreement ("Act of Default"), the City Manager shall provide Consultant with notice of an Act of Default and a fifteen (15) day period within opportunity to cure same. Should Consultant fail to cure an Act of Default with the corresponding cure period of same, the City Manager may terminate this Agreement immediately.

8.2 Upon receipt of the City's written notice of termination, Consultant shall stop work on the Project.

8.3 In the event of termination by the City, the Consultant shall be paid for all work accepted by the City Manager up to the date of termination, provided that the Consultant has first complied with the provisions of Paragraph 8.4.

8.4 The Consultant shall transfer all books, records, reports, working drafts, documents, maps, and data pertaining to the Project to the City, in a hard copy and electronic format specified by the City within 14 days from the date of the written notice of termination or the date of expiration of this Agreement, subject to receipt of Final payment per 8.3.

9. **Insurance.**

9.1 The Consultant shall secure and maintain throughout the duration of this Agreement insurance of such type and in such amounts as required by Exhibit A. The insurance carrier shall be qualified to do business in the State of Florida and have agents upon whom service of process may be made in the State of Florida.

9.2 Certificates of Insurance shall be provided to the City at the time of execution of this Agreement and certified copies provided if requested. Each policy certificate shall be endorsed with a provision that not less than thirty (30) calendar days' written notice shall be provided to the City before any policy or coverage is cancelled or restricted, or in accordance to policy provisions. The City further reserves the right to solicit additional coverage, or require higher limits of liability as needed, and depending on the nature of scope, or level of exposure.

10. **Nondiscrimination.**

10.1 During the term of this Agreement, Consultant shall not discriminate against any of its employees or applicants for employment because of their race, color, religion, sex, or national origin, and to abide by all Federal and State laws regarding nondiscrimination

11. **Attorneys' Fees and Waiver of Jury Trial.**

11.1 In the event of any litigation arising out of this Agreement, each party shall be responsible for their attorneys' fees and costs, including the fees and expenses of any paralegals, law clerks and legal assistants, and including fees and expenses charged for representation at both the trial and appellate levels.

11.2 In the event of any litigation arising out of this Agreement, each party hereby knowingly, irrevocably, voluntarily and intentionally waives its right to trial by jury.

12. **Indemnification.**

12.1 Consultant shall defend, indemnify, and hold harmless the City, its officers, agents and employees, from and against any and all demands, claims, losses, suits, liabilities, causes of action, judgment or damages, arising out of, related to, or any way connected with Consultant's performance or non-performance of any provision of this Agreement including, but not limited to, liabilities arising from contracts between the Consultant and third parties made pursuant to this Agreement. Consultant shall reimburse the City for all its expenses including reasonable attorneys' fees and costs incurred in and about the defense of any such claim or investigation and for any judgment or damages arising out of, related to, or in any way connected with Consultant's performance or non-performance of this Agreement. This section shall be interpreted and construed in a manner to comply with any applicable Florida Statutes, including without limitation Sections 725.06 and 725.08, Fla. Stat., if applicable.

12.2 The provisions of this section shall survive termination of this Agreement.

12.3 Ten dollars ($10) of the payments made by the City constitute separate, distinct, and independent consideration for the granting of this indemnification, the receipt and sufficiency of which is voluntary and knowingly acknowledged by the Consultant.

13. **Notices/Authorized Representatives.**

13.1 Any notices required by this Agreement shall be in writing and shall be deemed to have been properly given if transmitted by hand-delivery, by registered or certified mail with postage prepaid return receipt requested, or by a private postal service, addressed to the parties (or their successors) at the following addresses:

For the City:

Albert P. Childress
City Manager
City of Doral, Florida
8401 NW 53rd Terrace
Doral, Florida 33166

With a Copy to:

Luis Figueredo, Esq.
City Attorney
8401 NW 53rd Ter
Doral, FL 33166

For The Consultant:

Clarium Managed Services, LLC
Rob Vazquez
President and CSO
2244 NW 114 Avenue
Miami, FL 33172

14. **Governing Law.**

14.1 This Agreement shall be construed in accordance with and governed by the laws of the State of Florida. Exclusive venue for any litigation arising out of this Agreement shall be in Miami-Dade County, Florida.

15. **Entire Agreement/Modification/Amendment.**

15.1 This writing contains the entire Agreement of the parties and supersedes any prior oral or written representations. No representations were made or relied upon by either party, other than those that are expressly set forth herein.

15.2 No agent, employee, or other representative of either party is empowered to modify or amend the terms of this Agreement, unless executed with the same formality as this document.

16. **Ownership and Access to Records and Audits.**

16.1 Pursuant to Section 119.0701, Florida Statutes, Consultant shall, in addition to other contractual requirement provided bylaw, comply with public records laws, specifically to:

(a) Keep and maintain public records that ordinarily and necessarily would be required by the City in order to perform the service;

(b) Provide the public with access to public records on the same terms and conditions that the City would provide the records and at a cost that does not exceed the cost provided in this chapter or as otherwise provided by law;

(c) Ensure that the public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law; and

(d) Meet all requirements for retaining public records and transfer, at no cost, to the City all public records in possession of the Consultant upon termination of the contract and destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. All records stored electronically must be provided to the City in a format that is compatible with the information technology systems of the public agency.

16.2 All records, books, documents, maps, data, deliverables, papers and financial information (the "Records") that result from the Consultant providing services to the City under this Agreement shall be the property of the City.

16.3 The City Manager or his designee shall, during the term of this Agreement and for a period of one (1) year from the date of termination of this Agreement, have reasonable access to and the right to examine and audit any Records of the Consultant involving transactions related to this Agreement.

16.4 The City may cancel this Agreement for refusal by the Consultant to allow reasonable access by the City Manager or his designee to any Records pertaining to work performed under this Agreement that are subject to the provisions of Chapter 119, Florida Statutes.

## 17. Nonassignability.

17.1 This Agreement shall not be assignable by Consultant unless such assignment is first approved by the City Manager. The City is relying upon the apparent qualifications and personal expertise of the Consultant, and such firm's familiarity with the City's area, circumstances and desires.

## 18. Severability.

18.1 If any term or provision of this Agreement shall to any extent be held invalid or unenforceable, the remainder of this Agreement shall not be affected thereby, and each remaining term and provision of this Agreement shall be valid and be enforceable to the fullest extent permitted by law.

## 19. Independent Consultant.

19.1 The Consultant and its employees, volunteers and agents shall be and remain independent Consultants and not agents or employees of the City with respect to all of the acts and services performed by and under the terms of this Agreement. This Agreement shall not in any way be construed to create a partnership, association or any other kind of joint undertaking, enterprise or venture between the parties.

## 20. Compliance with Laws.

20.1 The Consultant shall comply with all applicable laws, ordinances, rules, regulations, and lawful orders of public authorities relating to the Project.

## 21. Waiver

21.1 The failure of either party to this Agreement to object to or to take affirmative action with respect to any conduct of the other which is in violation of the terms of this Agreement shall not be construed as a waiver of the violation or breach, or of any future violation, breach or wrongful conduct.

## 22. Survival of Provisions

22.1 Any terms or conditions of either this Agreement that require acts beyond the date of the term of the Agreement, shall survive termination of the Agreement, shall remain in full force and effect unless and until the terms or conditions are completed and shall be fully enforceable by either party.

## 23. Prohibition of Contingency Fees.

23.1 The Consultant warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for the Consultant, to solicit or secure this Agreement, and that it has not paid or agreed to pay any person(s), company, corporation, individual or firm, other than a bona fide employee working solely for the Consultant, any fee, commission, percentage, gift, or any other consideration, contingent upon or resulting from the award or making of this Agreement.

## 24. Counterparts

24.1 This Agreement may be executed in several counterparts, each of which shall be deemed an original and such counterpart shall constitute one and the same instrument.

**IN WITNESS WHEREOF**, the parties execute this Agreement on the respective dates under each signature: The City, signing by and through its City Manager, attested to by its City Clerk, duly authorized to execute same and by Consultant and through its representative, who has been duly authorized to execute same.

Attest:

____________________________
Connie Diaz, City Clerk

**CITY OF DORAL**

By: ____________________________
Albert P. Childress, City Manager
Date: Aug. 28, 2019

Approved As To Form and Legal Sufficiency for the Use
And Reliance of the City of Doral Only:

____________________________
Luis Figueredo, ESQ
City Attorney

**CLARIUM MANAGED SERVICES, LLC**
**("CONSULTANT")**

By: ____________________________
Rob Vazquez
President and CSO

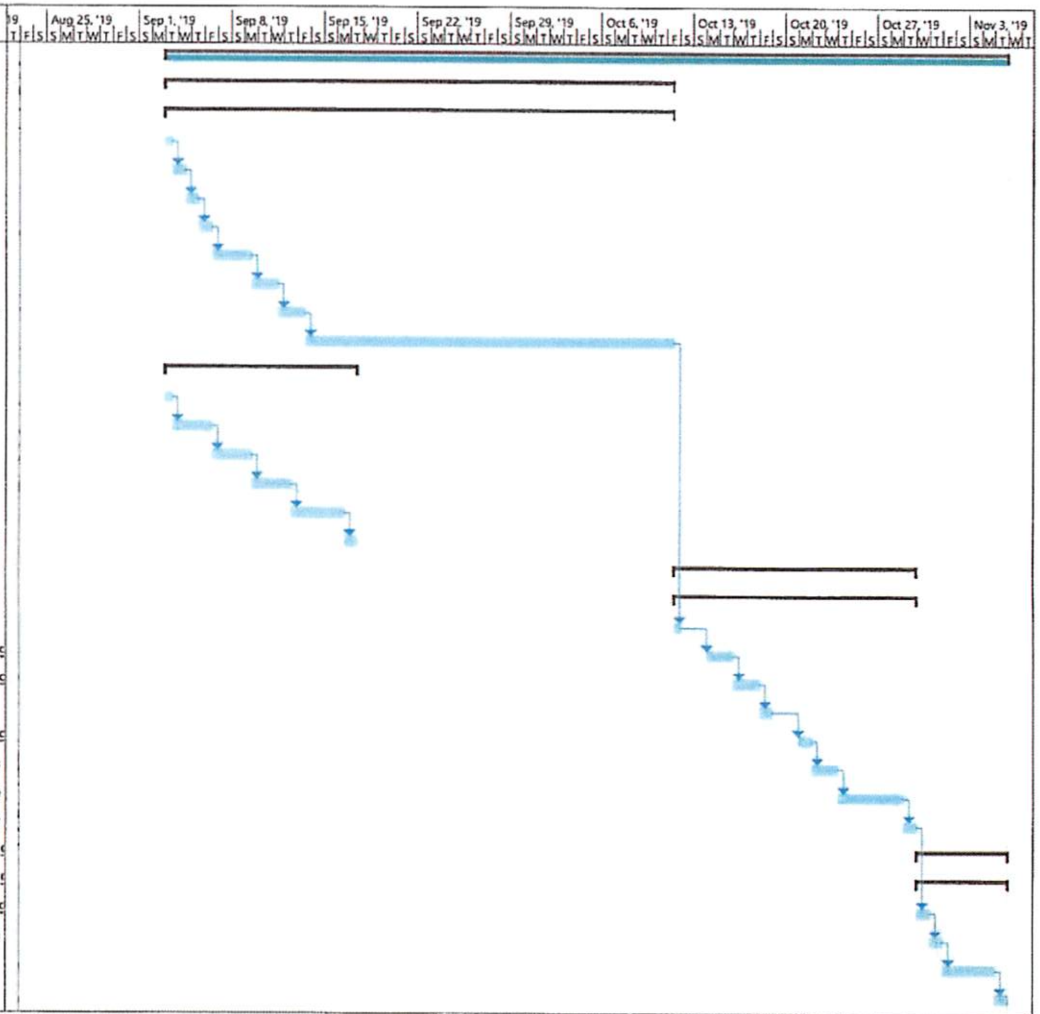
Date: 8/27/19

# SCOPE OF SERVICES

SEE EXHIBIT "A" ATTACHED

Scope of Service - City of DORAL

| ID | Task Mode | Task Name | Duration | Start |
|---|---|---|---|---|
| 1 | | **City of Doral High Level Project Plan** | **46 days** | **Tue 9/3/19** |
| 2 | | **Phase 1** | **28.5 days** | **Tue 9/3/19** |
| 3 | | **Palo Alto Networks Traps Ugrade 4.2 to 6.0 Cloud** | **28.5 days** | **Tue 9/3/19** |
| 4 | | Project Kickoff & Requirements Session | 0.5 days | Tue 9/3/19 |
| 5 | | Deployment Planning and TMS Instance Activation | 1 day | Tue 9/3/19 |
| 6 | | Review Current ESM configuration | 1 day | Wed 9/4/19 |
| 7 | | Migrate Profiles to TMS | 1 day | Thu 9/5/19 |
| 8 | | Upgrade Pilot Group Agents | 1 day | Fri 9/6/19 |
| 9 | | Optimize Policies & Rules | 2 days | Mon 9/9/19 |
| 10 | | Verification of Policies & Rules | 2 days | Wed 9/11/19 |
| 11 | | Production Go-Live Upgrade ESM agents to TMS | 20 days | Fri 9/13/19 |
| 12 | | **Palo Alto Networks NGFW Update and Best Practice Review (E** | **10.5 days** | **Tue 9/3/19** |
| 13 | | Project Kickoff & Requirements Session | 0.5 days | Tue 9/3/19 |
| 14 | | Conduct BPA on Existing Devices | 3 days | Tue 9/3/19 |
| 15 | | Review BPA with City and Determine In-Scope Fixes | 1 day | Fri 9/6/19 |
| 16 | | Optimize Policies & Rules | 3 days | Mon 9/9/19 |
| 17 | | Verification of Policies & Rules | 2 days | Thu 9/12/19 |
| 18 | | Production Go-Live | 1 day | Mon 9/16/19 |
| 19 | | **Phase 2** | **12.5 days** | **Fri 10/11/19** |
| 20 | | **Final Design and POC Presentation** | **12.5 days** | **Fri 10/11/19** |
| 21 | | Project Kickoff & Requirements Session | 0.5 days | Fri 10/11/19 |
| 22 | | Complete Draft Dashboard Visualization | 2 days | Mon 10/14/1 |
| 23 | | Establish all Baseline Log Sources | 2 days | Wed 10/16/1 |
| 24 | | Test /Reset Log Sources and Access | 1 day | Fri 10/18/19 |
| 25 | | Ensure Proper ACLs are enabled/allowed | 1 day | Mon 10/21/1 |
| 26 | | Configure and Test Universal Forwarder | 2 days | Tue 10/22/19 |
| 27 | | Develop Final Design | 3 days | Thu 10/24/19 |
| 28 | | Present Proposed Dashboards for City Approval | 1 day | Tue 10/29/19 |
| 29 | | **Phase 3** | **5 days** | **Wed 10/30/1** |
| 30 | | **Dashboard Production** | **5 days** | **Wed 10/30/1** |
| 31 | | Complete Final Checklist for all Log and Manufacturer Source | 1 day | Wed 10/30/1 |
| 32 | | Establish Assigned Personnel and SLA's for City Event Routing | 1 day | Thu 10/31/19 |
| 33 | | Conduct End to End Event Simulation | 2 days | Fri 11/1/19 |
| 34 | | Present Final Dashboard and SLA for City Approval | 1 day | Tue 11/5/19 |



Project: City of Doral Project Pla
Date: Fri 8/23/19

Task, Split, Milestone ◇, Summary, Project Summary, Inactive Task, Inactive Milestone, Inactive Summary, Manual Task, Duration-only, Manual Summary Rollup, Manual Summary, Start-only [, Finish-only ], External Tasks, External Milestone ◇, Deadline, Progress, Manual Progress

Approved 8/23/19

# SCOPE OF SERVICES

SEE EXHIBIT "A" ATTACHED

# Professional Security Support Proposal

**Prepared by:**
Rob Vazquez
Clarium Managed Services

**Prepared for:**
Gladys Gonzalez
City of Doral

# About Us

Clarium is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology.

Clarium has served clients of various sizes from global enterprises to SME's and across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 25 of the leading security product manufacturers.

Clarium's trademarked SecureVault is the solution for most middle market organizations that are grappling with the complexity and cost of securing their digital assets. Clarium augments, and if necessary can replace the security component of your information technology resources at a fraction of the cost.

Our product fulfillment is completely custom tailored around our customers' requirements. Clarium's strong national distribution network can facilitate custom logistics to meet the most aggressive timelines and geographies. Complimented by a staff of top level systems engineers and architects, every bundled product or service we maintain has been certified and stress tested before reaching any customers environment.

# Minority Business Enterprise

CLARIUM IS A STATE OF FLORIDA CERTIFIED, DADE COUNTY MINORITY OWNED ENTERPRISE

NMSDC
National Minority Supplier
Development Council

THIS CERTIFIES THAT

## Sunshine Computers & Software, Inc.

dba Clarium Managed Services

* Nationally certified by the: **FLORIDA STATE MINORITY SUPPLIER DEVELOPMENT COUNCIL**

*NAICS Code(s): 423850

* Description of their product/services as defined by the North American Industry Classification System (NAICS)

10/01/2018
**Issued Date**

FL04238
**Certificate Number**

10/01/2019
**Expiration Date**

Adrienne Trimble

**Beatrice Louissaint, President & CEO**

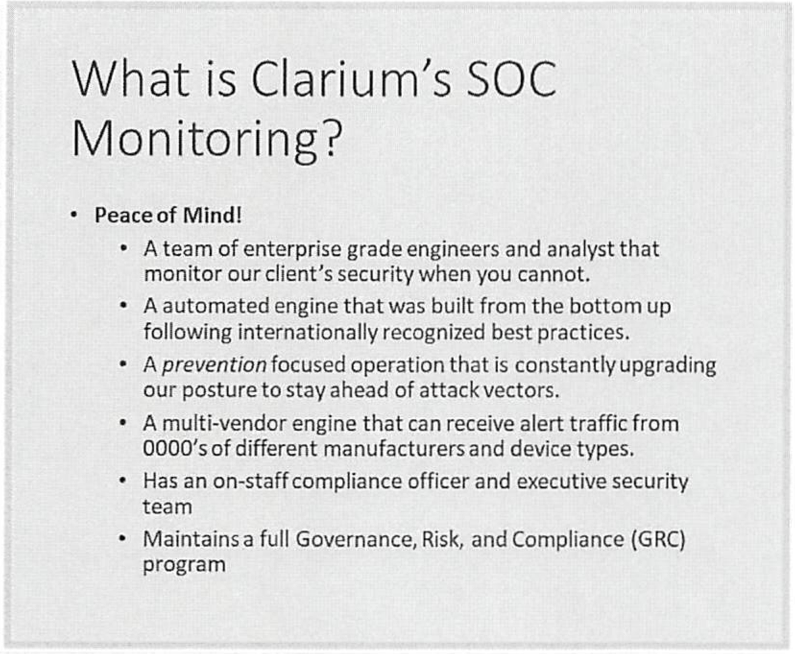
By using your password (NMSDC issued only), authorized users may log into NMSDC Central to view the entire profile: http://nmsdc.org

Certify, Develop, Connect, Advocate.

* MBEs certified by an Affiliate of the National Minority Supplier Development Council, Inc.®

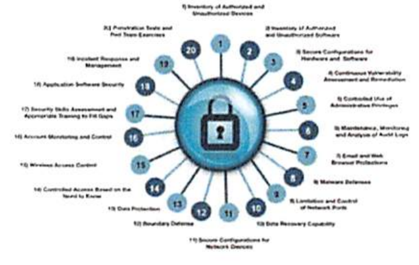
Solution Overview

## What is SOC Monitoring?



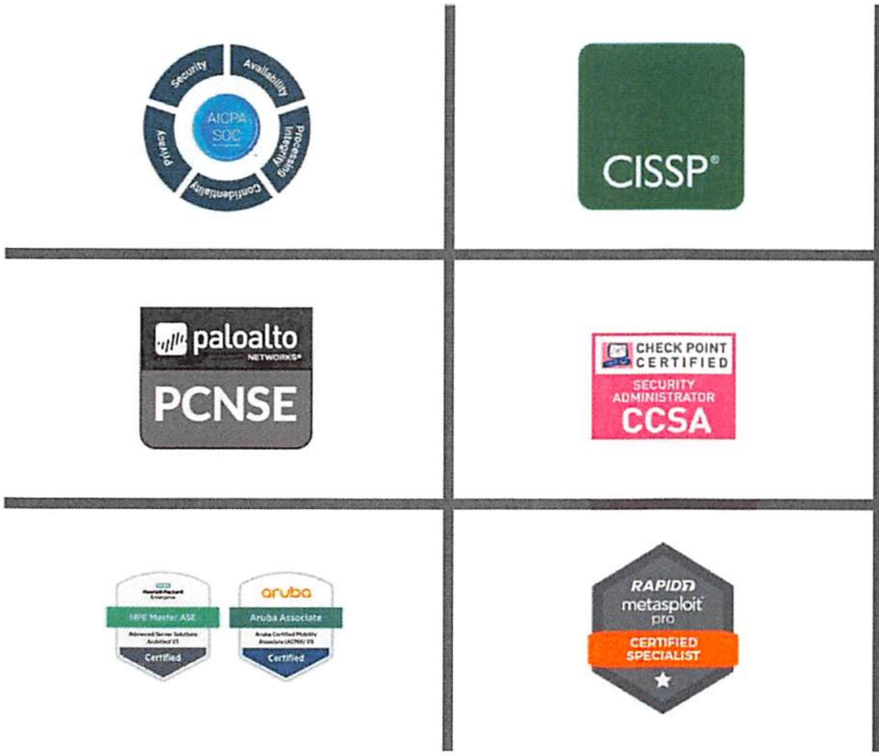
# What is Clarium's SOC Monitoring?

- **Peace of Mind!**
  - A team of enterprise grade engineers and analyst that monitor our client's security when you cannot.
  - A automated engine that was built from the bottom up following internationally recognized best practices.
  - A *prevention* focused operation that is constantly upgrading our posture to stay ahead of attack vectors.
  - A multi-vendor engine that can receive alert traffic from 0000's of different manufacturers and device types.
  - Has an on-staff compliance officer and executive security team
  - Maintains a full Governance, Risk, and Compliance (GRC) program


1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

Security
Availability
Processing Integrity
Confidentiality
Privacy
AICPA
SOC

## Our Credentials



Our Credentials...Clarium personnel spend >200 hours per annum in training!

The most skilled and credentialed cybersecurity workforce in the State of Florida.

**Engagement Length:** 36 Months

**Target Launch Date:** 8/12/2019

# Business Rationale

The City of Doral has requested a proposal from a Palo Alto Networks Certified Managed Security Services Partner (MSSP) to provide security staff support and Security Operations Center monitoring (SOC) from our center in Miami, Florida. The proposed engagement is intended to provide the following vital support to the City:

1. Security Operations Center (SOC) vigilance of the City's Security Infrastructure including following escalation paths, incident response, and notification as deemed necessary by the City.
2. PANW Certified Engineering staff to provide day to day updating, patching, and physical response to any device or program included in-scope as defined herein, and required as part of a manufacturer service bulletin, critical response, machine response, or as indicated by the City.
3. Firewall /PANW Panorama Monitoring and Policy Management as required for the day to day successful operation and security of the City of Doral's perimeter and core digital assets.

It is the City's intention to also replace or discontinue their use of Splunk software products internally, hence generating a *cost avoidance* to the City's IT budget. The in-scope items in this proposal will make the license of this software *redundant*.

# In-Scope Items (General)

- Remote monitoring of security devices and services that form part or whole of the security eco-system at the City of Doral.
- 24/7 automated monitoring and threat prevention services from Clarium's Security Operations Center (SOC).
- Network security posture
- Running of any security reports per the City's schedule utilizing any supported platform such as:
  - Palo Alto Networks
  - Tenable
  - Splunk
  - Metasploit
  - Rapid 7

  Note: the use of any of these vulnerability or penetration testing tools will only be executed after a *program plan* is submitted to the City's CIO for approval. The plan will articulate what device, or area of concern is being tested, date, impact (if any), and desired result. The City is asked to be a part of these testing regimes to ensure that a healthy security posture is constantly maintained.

# In-Scope Items (Specific Requests)

The following specific items have been requested for special event monitoring by the City:

- Critical Hosts (Approximately 10 file server hosts)
- Intersections (19 VPN's)
- Wifi Access Points (100) General threat, health/welfare, performance metrics
- Next Generation Firewalls PA-3020's. (2) perimeter, (3) at City Hall
- Advanced Endpoint Monitoring using existing PANW Traps platform. Approximately (750) potential endpoints.

# Out of Scope Items

- Non-Cybersecurity related information technology devices, services, mechanisms, or data ***with the exception of*** the hardware and software that is used to protect these devices, services, mechanisms, or data.
- Management of day to day data back-up and restore routines unless Clarium has been alerted of a failure of these routines that needs security oversight.
- Design, implementation, or renewal of items not part of the current day to day cybersecurity ecosystem (with the exception of the Palo Alto Networks upgrade support in this proposal) at the City of Doral upon acceptance and execution of this proposal.

# Approach

Clarium is proposing to implement the services contained herein in three sequential phases as described below:

**Phase 1 : Palo Alto Networks Updating and Remediation Support**
Clarium would guide and facilitate the upgrades of the City's PANW software assets such as Traps and Panorama to the latest releases and patch levels including migration to the new Cortex cloud based services of these products. This activity is considered a *precursor* to the onboarding of SOC services to Clarium. A detailed plan will be co-developed with the City's IT department and submitted for approval by the CIO.

**Phase 2: Final Design and POC Presentation**
During Phase 1, Clarium will work in parallel to establish the final design for the monitored dashboard and Proof of Concept (POC) for approval by the CIO.

**Phase 3 : Dashboard Production**

Phase 3 deliverable will include the final turn-up to production of the remainder of in-scope assets to Clarium. It will also signal the commencement of all agreed reporting and escalation mechanisms with the City of Doral.

This proposal includes all the project management which is estimated at (80) hours to oversee all (3) phases of the program and is offered to the City as a complementary function of the onboarding.

# Service Level Objectives

Clarium is pleased to offer the City of Doral the following Service Level Objectives (SLO):

- Mean Time to Respond (1 Hour Maximum Threshold)
- Mean Time to Repair (4 Hour Maximum Threshold)
- Escalation of un-resolved Level 2 incidents to CSO (1 HR)
- Escalation of un-resolved Level 3 incidents to CSO (30 minutes)
- Escalation of un-resolved Level 2 incidents to CEO (2 HR)
- Escalation of un-resolved Level 3 incidents to CEO (1 HR)

Metering of our SLO will be captured in Clarium's automated or manual ticketing system and reported to the City as part of our routine reporting intervals every month.

# Single Pane of Glass (SOC Services)

Clarium's proposal to the City of Doral covers (2) keys areas of the City's cybersecurity area.

## Area 1: Supporting and Updating of the Palo Alto Networks Infrastructure

The City has indicated a desire to have their current Palo Alto Networks security devices and software monitored by a third party. This will deliver greater threat visibility to the City and escalation in the event of any threats.

In order to accomplish this objective, the City needs to refresh their current Palo Alto Networks infrastructure to the latest software release levels including movement of management from their current on-premise console for Traps, to the new cloud based Management Console. This will additionally facilitate more robust data coming to the proposed Security Operations Center (SOC) directly from the Palo Alto Cortex environment.

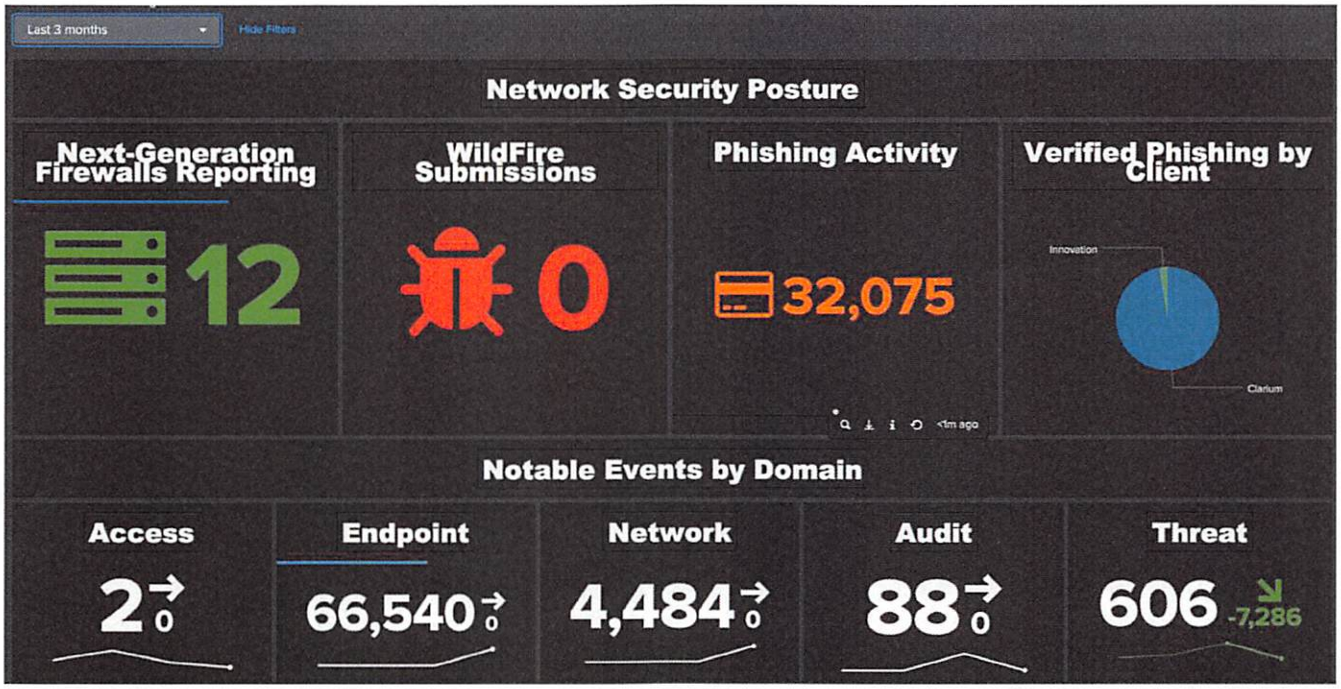
Additional benefits include several new and vital security features the City is currently not leveraging based on the older versions of the software and devices being utilized. The City has support contracts in place and only require design and operations support to complete the updating from Clarium.

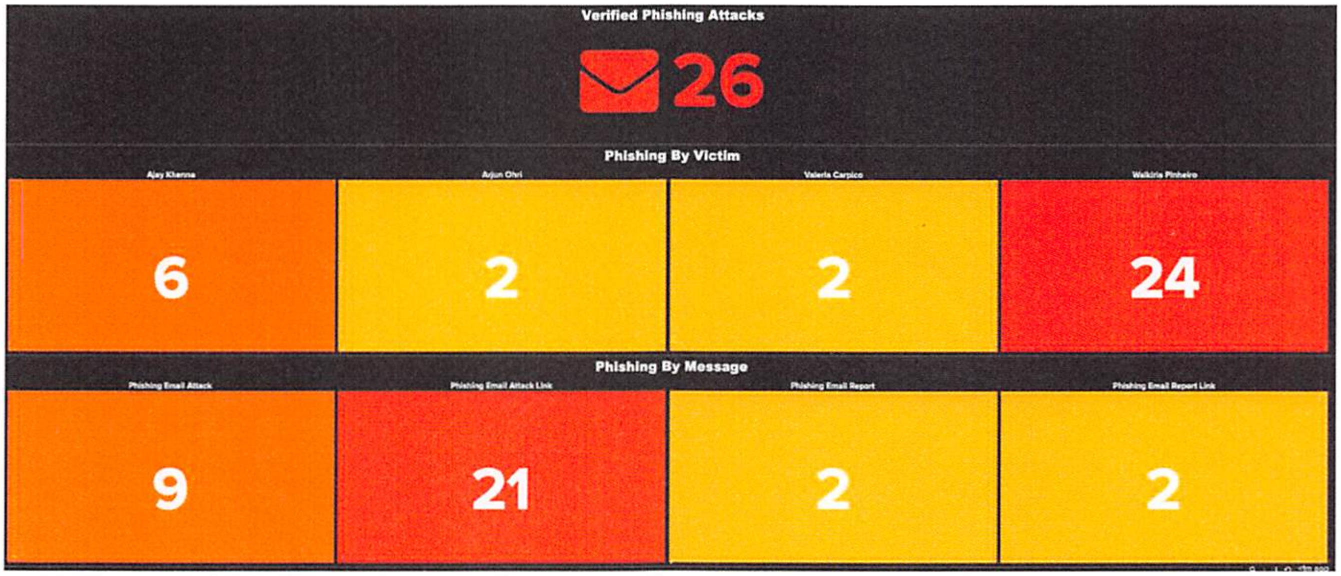
## Area 2: SOC Monitoring via Splunk Dashboarding

Clarium will design, build, and capture under our rapid deployment model, a *Single Pane of Glass Dashboard* where we would include up to (8) critical *elements* in a single dashboard that will be monitored for the City of Doral. The *elements* to be included would be documented and agreed as part of the initial discovery meeting. Elements are typically items such as # of Firewalls Reporting, Traps Activity by User /Asset, or Suspicious Threat Activity. Clarium is including up to *5GB of Splunk consumption per day as part of this service.

The following is a depiction of a basic dashboard for day to day monitoring. The final dashboard for the City of Doral will encompass the *elements* included in the in-scope discussion of this proposal.

*Please see note regarding Splunk consumption in the cost section of this document.





Verified Phishing Attacks

26

Phishing By Victim

| Ajay Khanna | Arjun Ohri | Valeria Carpico | Walkiria Pinheiro |
|---|---|---|---|
| 6 | 2 | 2 | 24 |

Phishing By Message

| Phishing Email Attack | Phishing Email Attack Link | Phishing Email Report | Phishing Email Report Link |
|---|---|---|---|
| 9 | 21 | 2 | 2 |

# Pre-requisites (What does Clarium Require from the City?)

Clarium would hold a (4) hour on-site discovery workshop to determine the items that need to be initiated or completed prior to the commencement or execution of our rapid deployment services. Such as the SOC dashboard services illustrated previously.

Clarium is specifically suited to complete this service provisioning sooner than our competitors given our confidential knowledge of the City of Doral's security eco-system from our completion of the Security Assessment in the Fall of 2018.

In general, Clarium requires sufficient credentialed and leveled access to in-scope systems for up to (3) assigned engineers to conduct the services as contained herein. They are:

- **Sahr Lebbie, Sr. Splunk Architect**
- **John Maki, PCNSE**
- **German Gobel, PANW Certified Traps Professional**

These engineers will report to the City as required, and will be available to the City remotely, and on-site (as required) through the direction and supervision of Clarium's Security Operations Director, Paul Tippin.

Paul Tippin will also serve as the technical engagement manager and liaison between Clarium and the City of Doral.

The following particular access and pre-requisites are required to the City of Doral's systems.

- **Documentation** / Schematics / Drawings illustrating the full TCP/IP network schema for the City of Doral inclusive of Security Devices.
- **Hardware (To be provided by the City of Doral), Clarium configured.**
    - **Centos/RHEL VMs (Splunk Universal Forwarder (count based on log sources)**
    - 2CPU (dedicated)
    - 4GB RAM (dedicated)
    - Disk Space TBD (based on log volume)
    - **Centos/RHEL/Windows VM (Syslog Aggregator (R-syslog/Kiwi Syslog/Syslog-NG)**
    - 1 CPU (dedicated)
    - 4 GB RAM (dedicated)
    - Disk Space TBD (based on log volume)
- **Software**
    - Splunk Universal Forwarder
    - Syslog Aggregator(R-syslog/Syslog-NG/Kiwi-Syslog)
    - Based on environment
- **Items that the City needs to provide:**
    - Log Sources *(that need to be collected)*
        - Syslog/WinEvent
        - Application Logs
        - Firewall Logs
        - Endpoint Logs
        - Database Logs
        - Networking Devices (IDS/IPS/NetFlow)
        - Email Logs
        - Custom Logs (RFID/GPS Data/CDR/etc.)
- **Hosts *(that need to be monitored)***
    - List of Servers
- **Environments *(that need to be monitored)***
    - Production Environment
    - Staging Environment
    - Development Environment
    - Cloud Space (AWS/Azure)

    - On-Premise
    - Infrastructure
- Ensure Proper ACLs are enabled/allowed
- Disable/Modify all AVs that may natively stop the Splunk Agents/processes from running
- Read access to any relevant SYSLOG logging forwarders as required for the provision of this service to the City of Doral.

# Cybersecurity Personnel Job Descriptions per Schedule 70

### HACS Cybersecurity Engineers

**HACS Cybersecurity Engineer Level 5** - Leads and/or supports authorized security/penetration testing on enterprise network assets, incident response activities including collection and correlation of incident data for mitigation and remediation, cyber hunt activities, threat and vulnerability assessments, analysis and evaluation of Computer Network Defense policies and configurations, and evaluation for compliance with regulations and enterprise directives.. Possesses in-depth knowledge of principles, concepts, and techniques appropriate to the development, operation of systems, and procedures dealing with real-time security monitoring, response, containment, investigation, and remediation; identification of flaws and weaknesses in the systems; prioritization of security resources; information security/assurance; resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services. Interprets requirements, performs highly-complex analyses, and resolves complex problems related to security testing principles, tools, and techniques; general attack stages; and identification of systemic security issues. Develops advanced technological ideas and guides their development into a final product. May act as advisor to customers on advanced technical research studies and applications. Education and Experience: 14 years with Bachelor's or 12 Years w/ Master's, or 9 years with PhD.

**HACS Cybersecurity Engineer Level 4** - Conducts and/or supports authorized security/penetration testing on enterprise network assets, incident response activities including collection and correlation of incident data for mitigation and remediation, cyber hunt activities, threat and vulnerability assessments, analysis and evaluation of Computer Network Defense policies and configurations, and evaluation for compliance with regulations and enterprise directives. Responsibilities may include solving engineering requirements relating to the development, operation of systems, and procedures dealing with real-time security monitoring, response, containment, investigation, and remediation; identification of flaws and weaknesses in the systems; prioritization of security resources; information security/assurance; resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services. Determines program objectives and requirements and develops standards and guides related to security testing principles, tools, and techniques; general attack stages; and identification of systemic security issues. Guides the successful completion of major programs and may function in a project leadership role. Education and Experience: 9 years with Bachelor's or 7 years with Masters, or 4 years with PhD.

**HACS Cybersecurity Engineer Level 3 -** Conducts and/or supports authorized security/penetration testing on enterprise network assets, incident response activities including collection and correlation of incident data for mitigation and remediation, cyber hunt activities, threat and vulnerability assessments, and analysis and evaluation of Computer Network Defense policies and configurations. Responsibilities may require developing new or improved techniques and procedures relating to the development, operation of systems, and procedures dealing with real-time security monitoring, response, containment, investigation, and remediation; identification of flaws and weaknesses in the systems; prioritization of security resources; information security/assurance; resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services.,. Provides analysis on a wide range of requirements related to security testing principles, tools, and techniques; general attack stages; and identification of systemic security issues. Contributes to the completion of specific programs and projects with frequent customer contacts. Education and Experience: 5 years with Bachelor's or 3 Years with Master's, or experience in lieu of degree.

**HACS Cybersecurity Engineer Level 2 -** Conducts and/or supports authorized security/penetration testing on enterprise network assets, incident response activities including collection and correlation of incident data for mitigation and remediation, cyber hunt activities, threat and vulnerability assessments, and analysis and evaluation of Computer Network Defense policies and configurations. Responsibilities may support research and assignments relating to the development, operation of systems, and procedures dealing with real-time security monitoring, response, containment, investigation, and remediation; identification of flaws and weaknesses in the systems; prioritization of security resources; information security/assurance;

resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services. Follows established procedures and contributes to the completion of milestones associated with specific projects and security testing principles, tools, and techniques; general attack stages; and identification of systemic security issues. Education and Experience: 2 years with Bachelor's Degree, or experience in lieu of degree.

**HACS Cybersecurity Engineer Level 1** - Supports authorized security/penetration testing on enterprise network assets, incident response activities including collection and correlation of incident data for mitigation and remediation, cyber hunt activities, threat and vulnerability assessments, and analysis and evaluation of Computer Network Defense policies and configurations. May develop and recommend solutions to technical requirements as assigned relating to the development, operation of systems, and procedures dealing with engineering support relating to real-time security monitoring, response, containment, investigation, and remediation; identification of flaws and weaknesses in the systems; prioritization of security resources; information security/assurance; resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services. Follows technical and process guidance and instructions, contributing to the completion of assigned technical fields related to security testing principles, tools, and techniques; general attack stages; and identification of systemic security issues. Education and Experience: 0 Years of experience with Bachelor's.

## HACS Cybersecurity Analyst HACS

**Cybersecurity Analyst Level 5** - Provides and leads cross-functional efforts for: planning; analyzing; designing; developing; documenting; test, training, and exercise (TT&E); operating; measuring/reporting; and/or administering cybersecurity systems, processes and procedures, support infrastructure, capabilities, and programs. Defines and interprets strategic requirements, analyzes and provides guidance, and executes cyber mission tasks including analysis support to penetration testing, incident response activities, cyber hunt activities, and risk and vulnerability assessments. Develops and leads projects, including defining scope, objectives, and methods. Develops advanced technological ideas and guides their development into a final product. May act as advisor to program leadership and customers on advanced concepts for system lifecycle management/engineering and mission assurance. Education and Experience: 14 years with Bachelor's or 12 Years w/ Master's, or 9 years with PhD.

**HACS Cybersecurity Analyst Level 4** - Provides for: planning; analyzing; designing; developing; documenting; test, training, and exercise (TT&E); operating; measuring/reporting; and/or administering cybersecurity systems, processes and procedures, support infrastructure, capabilities, and programs. Defines and interprets strategic requirements, analyzes and provides guidance, and executes cyber mission tasks including analysis support to penetration testing, incident response activities, cyber hunt activities, and risk and vulnerability assessments. Often works as part of cross-functional teams. Develops and leads projects, including defining scope, objectives, and methods. Develops advanced technological ideas and guides their development into a final product/deliverable. Meets program objectives and requirements and develops standards and guides. Supports the successful completion of programs and may function in a project/task lead role. Education and Experience: 9 years with Bachelor's or 7 years with Masters, or 4 years with PhD.

**HACS Cybersecurity Analyst Level 3** - Provides for: planning; analyzing; designing; developing; documenting; test, training, and exercise (TT&E); operating; measuring/reporting; and/or administering cybersecurity systems, processes and procedures, support infrastructure, capabilities, and programs. Defines and interprets strategic requirements, analyzes and provides guidance, and executes cyber mission tasks including analysis support to penetration testing, incident response activities, cyber hunt activities, and risk and vulnerability assessments. Develops and leads projects, including defining scope, objectives, and methods. Develops advanced technological solutions and their implementation into a final product/deliverable. Meets program objectives and requirements and develops standards and guides. Contributes to the completion of specific cross-functional tasks and projects. Education and Experience: 5 years with Bachelor's or 3 Years with Master's, or experience in lieu of degree.

**HACS Cybersecurity Analyst Level 2** - Provides for: planning; analyzing; designing; developing; documenting; test, training, and exercise (TT&E); operating; measuring/reporting; and/or administering cybersecurity systems, processes and procedures, support infrastructure, capabilities, and programs. Defines and interprets strategic requirements, analyzes and provides guidance, and executes cyber mission tasks including analysis support to penetration testing, incident response activities, cyber hunt activities, and risk and vulnerability assessments. Develops and leads projects, including defining scope, objectives, and methods. Develops advanced technological solutions and their implementation into a final product/deliverable. Meets program objectives and requirements and develops standards and guides. Contributes to the completion of specific cross-functional tasks and projects. Follows established procedures and contributes to the completion of milestones associated with specific projects. 2 years with Bachelor's Degree, or experience in lieu of degree.

**HACS Cybersecurity Analyst Level 1 -** Provides for: planning; analyzing; designing; developing; documenting; test, training, and exercise (TT&E); operating; measuring/reporting; and/or administering cybersecurity systems, processes and procedures, support infrastructure, capabilities, and programs. Defines and interprets strategic requirements, analyzes and provides guidance, and executes cyber mission tasks including analysis support to penetration testing, incident response activities, cyber hunt activities, and risk and vulnerability assessments. Develops and leads projects, including defining scope, objectives, and methods. Develops advanced technological solutions and their implementation into a final product/deliverable. Meets program objectives and requirements and develops standards and guides. Contributes to the completion of specific cross-functional tasks and projects. Follows established procedures and contributes to the completion of milestones associated with specific projects. Education and Experience: 0 Years with Bachelor's.

**HACS Cybersecurity Subject Matter Expert Level 2 -** Responsible for daily operations of a team or work unit (direct supervision of the staff, assignment of work schedules, day-to-day workflow, and operating costs) relating to cybersecurity policy and configuration analysis and evaluation; development, implementation, and management of systems security solutions; authorized security testing; threat and vulnerability assessment; collection and correlation of incident data; mitigation and remediation support; resource management; cyber hunt activities; database planning and design; data/records management; systems analysis and design; network monitoring and analysis services; network services project management; application systems/software/database architecture, analysis, design, documentation, development, modification, and implementation; data recovery and digital chain of evidence support (computer-related evidence collection, processing, preservation, analysis, and presentation); reverse engineering; and other computer-related services. Responsibilities may include cost, schedule, and technical performance, and quality of a work package, subsystem, or related group of work packages on a large system development-type task or full responsibility for all aspects of team performance. Education and Experience: 5 years with Bachelor's or 3 years with Master's or substitution of experience in lieu of degree.

**IT Analyst Level 2 (IT-ANL02) -** Responsibilities may support research and assignments relating to the development, operation of systems, and procedures dealing with resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services. Follows established procedures and contributes to the completion of milestones associated with specific projects. Education and Experience: 2 years with Bachelor's or 0 years with Master's.

# Costing Table (On-Demand Hourly Personnel as Required) per GSA Schedule 70 guidance

Clarium is honoring and proposing to the City of Doral the same schedule currently used by the The General Services Administration (GSA)'s IT Schedule 70 for **Highly Adaptive Cybersecurity Services (HACS)** with the applicable Special Item Numbers (SINs). **Clarium is currently not on Schedule 70 for services, however we honor the same contract prices on the schedule plus provide additional incentives to State and Local Government (SLED) beyond those contracted by the GSA.*

The below rates are guaranteed to the City of Doral for the duration of the term of this proposed agreement. Clarium shall provide a Statement of Work (SOW) for approval upon acceptance of these terms by the City.

GSA Contract Rates Effective 27 January 2019 – 26 January 2020 illustrated Below

*This proposal is for the ongoing monitoring of the City's digital assets as indicated throughout this proposal. The City can at its discretion order management or on-demand services as required to maintain a healthy cybersecurity. This section illustrates the costs of those resources as offered to the City and locked in for the duration of the Term.*

| SKU | Description | Clarium Rate | City of Doral Rate |
|---|---|---|---|
| HACS-ENG05 | Cybersecurity Engineer Level 5 | $242.15 | $206.46 |
| HACS-ENG04 | Cybersecurity Engineer Level 4 | $198.58 | $169.30 |
| HACS-ENG03 | Cybersecurity Engineer Level 3 | $155.69 | $132.74 |
| HACS-ENG02 | Cybersecurity Engineer Level 2 | $117.92 | $100.53 |
| HACS-ENG01 | Cybersecurity Engineer Level 1 | $111.09 | $94.70 |
| HACS-ANL05 | Cyber Analyst Level 5 | $206.12 | $182.82 |
| HACS-ANL04 | Cyber Analyst Level 4 | $174.09 | $154.42 |
| HACS-ANL03 | Cyber Analyst Level 3 | $138.51 | $122.86 |
| HACS-ANL02 | Cyber Analyst Level 2 | $115.40 | $102.36 |

|  |  |  |  |
|---|---|---|---|
| HACS-ANL01 | Cyber Analyst Level 1 | $97.68 | $86.64 |
| HACS-SME02 | HACS Cybersecurity SME Level 2 | $233.30 | $198.90 |
| IT-ANL02 | IT Analyst Level 2 | $ 145.57 | $ 130.61 |

## Estimated One Time Costs - Phase 1 Support (Palo Alto Networks)

The following costs are support estimates to complete the upgrade of the following Palo Alto Networks vital security systems. Clarium will make all efforts to minimize the hours utilized in completing the upgrade. If the upgrade is anticipated to exceed these estimates, a request for additional support hours will be submitted to the City's CIO for approval before the additional work is performed. Any additional support hours will be billed at the rate illustrated in the contained cost scheduled, and in the subsequent request for approval. Should the support hours fall below these estimates only logged approved hours will be billed.

| Name | Price | QTY | Subtotal |
|---|---|---|---|
| Palo Alto Networks Traps Upgrade and Patching (650 EP's)<br>Cyber Analyst Level 4 | $154.42 | 48 | $7,412.16 |
| Palo Alto Networks Panorama Upgrade to Cloud and NGFW patching to Newest PAN/OS<br>Cybersecurity Engineer Level 4 | $169.30 | 48 | $8,126.40 |
| Palo Alto Networks Project Manager (Project Support Oversight)<br>HACS Cybersecurity SME Level 2 | $198.90 | 8 | $1,591.20 |

|  |  |
|---|---|
| Subtotal | **$17,129.76** |
| **Total** | **$17,129.76** |

## One Time Costs - Phase 2 Final Design and POC Presentation

| Name | Price | QTY | Discount | Subtotal |
|---|---|---|---|---|
| Dashboard Production<br>Design, Build, and Implement the primary dashboard with in-scope elements as contained in the scope of this proposal.<br>Cyber Analyst Level 4 | $154.42 | 80 | 100% | $0.00 |
| Dashboard POC Presentation<br>Prep and Presentation of the POC and Final Dashboard for Approval by the City<br>HACS Cybersecurity SME Level 2 | $198.90 | 16 | 100% | $0.00 |

|  |  |
|---|---|
| Subtotal | **$0.00** |
| **Total** | **$0.00** |

# Proposed Costs Phase 3 (Custom Dashboard) (Monthly Recurring -Fixed Term 36)

| Name | Price | QTY | Subtotal |
|---|---|---|---|
| SecureVault (Endpoint Reporting and SOC Monitoring)<br>Custom dashboard monitoring of key metrics with alert escalation paths as prescribed by the City of Doral | $2.50 | 650 | $1,625.00 |
| SecureVault (Server SOC Monitoring)<br>Custom dashboard monitoring of key metrics with alert escalation paths as prescribed by the City of Doral | $75.00 | 10 | $750.00 |
| SecureVault (City Intersections)<br>Custom dashboard monitoring of key metrics with alert escalation paths as prescribed by the City of Doral | $75.00 | 19 | $1,425.00 |
| Securevault (NGFW Monitoring and Escalation)<br>Custom dashboard monitoring of key metrics with alert escalation paths as prescribed by the City of Doral | $120.00 | 5 | $600.00 |
| Securevault (WIFI Access Points Monitoring and Escalation)<br>Custom dashboard monitoring of key metrics with alert escalation paths as prescribed by the City of Doral | $5.00 | 100 | $500.00 |
| Splunk ES Consumption (Logging)<br>Clarium is including (5 GB) of consumption measured per day for the above items. | $0.00 | 1 | $0.00 |
| | | Subtotal | **$4,900.00** |
| | | **Total** | **$4,900.00** |

## Splunk Logging Services Cost Disclaimer

Splunk ES Cost : Clarium is including (5 GB) of consumption measured per day for the in-scope items. Clarium will review the actual consumption (ingestion) of logs effectively (30) days after the final production dashboard is approved by the City of Doral. If the actual consumption exceeds (5GB) per day measured over that period, a true-up adjustment will be calculated for the City and submitted for approval. Clarium will use a competitive *cost plus* basis to derive a final consumption cost utilizing our MSSP bulk buying license with Splunk Corporation on behalf of the City of Doral. The City will be granted a further (60) days decide if they want to cut their consumption, or add the additional consumption (if any). The initial (90) days of consumption are guaranteed at the (5GB) included rate *regardless of consumption values*.

Clarium will utilize all means necessary to adjust non essential log items from utilizing vital consumption and indexing space. This is key in maximizing value because many items that can be ingested by Splunk *are not essential* to security and therefore waste resources and costs. Clarium's Splunk Architect will be directed to prune as much non-security indexing as possible to keep this cost to a minimum.

# Legal

Clarium would follow the existing, approved, and in-force vendor agreements already in place with the City of Doral.

## Data Responsibilities of Clarium

Clarium shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (MAY 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

Target project completion date : 9/30/2019

Acceptance of timeline initial here: R.V.

# Terms and Conditions

**Proposal Acceptance:**

Name: Gladys Gonzalez
Company: City of Doral

Signature:

Net 30 Terms are offered upon approval and form part of this proposal, or as stipulated in existing or superseding agreements with the City of Doral.

# RESOLUTION No. 19-163

**A RESOLUTION OF THE MAYOR AND THE CITY COUNCIL OF THE CITY OF DORAL, FLORIDA, WAIVING THE COMPETITIVE BID PROCESS PURSUANT TO SECTION 2-321 OF THE CITY'S CODE OF ORDINANCES, TO HAVE CLARIUM SECURITY OPERATION CENTER (SOC) THREE-YEAR REMOTE MONITORING OF SECURITY DEVICES AND SERVICES THAT FORM PART OF OR WHOLE OF THE SECURITY ECO-SYSTEM AT THE CITY OF DORAL; AUTHORIZING THE CITY MANAGER TO EXECUTE THE AGREEMENTS AND EXPEND BUDGETED FUNDS ON BEHALF OF THE CITY IN AN AMOUNT NOT TO EXCEED $73,800.00; PROVIDING FOR IMPLEMENTATION; AND PROVIDING FOR AN EFFECTIVE DATE**

**WHEREAS**, In 2018, the Information Technology Department worked with Clarium to conduct an information security audit. The assessment scope was to several key areas of the Center for Internet Security Top 20 Controls, (CIS 20); and

**WHEREAS**, These are internationally recognized controls that are constantly being reviewed for improvement, and used by many leading Fortune 1000 entities, along with Federal, State, and Local Government; and

**WHEREAS**, The controls we assessed specifically were CIS 6-18; which are critical in how an entity protects against, tracks, and documents potential security events. Clarium's audit provided a comprehensive risk analysis that took into account all the contributing factors including asset criticality, vulnerabilities, external threats, reachability, exploitability, and business; and

**WHEREAS**, The custom risk assessment proved the usefulness of the City's firewalls, security software and monitoring tools. However, considering the recent cyber-attacks aimed at government agencies proves that security infrastructure needs twenty-four hours seven days a week (24/7) vigilance including day to day successful operation and security of the City's perimeter and core digital; and

**WHEREAS**, The Information Technology Department respectfully recommends waiving competitive bidding and procurement requirements and authorizing the City Manager to have Clarium Security Operation Center (SOC) three-year (3) Year Remote Monitoring of security devices and services that form part of or whole of the security eco-system at the City of; and

**WHEREAS**, staff has recommended that the Mayor and City Council Members approve the purchase of twenty-four hours seven days a week (24/7) automated monitoring and threat prevention services from Clarium Security Operations Center in an amount not to exceed FY1819 **$58,800.00** for SOC monitoring and **$15,000** implementation.

**NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND CITY COUNCIL OF THE CITY OF DORAL, FLORIDA, AS FOLLOWS:**

**Section 1. Recitals.** The above recitals are confirmed, adopted, and incorporated herein and made a part hereof by this reference.

**Section 2. Waiver of Competitive Bid Process.** Pursuant to section 2-321 of the City Code of Ordinances, the competitive bid process as required by the Chapter 2 of the City Code is hereby waived for the purchase of Clarium Security Operation Center (SOC) three-year (3) Year Remote Monitoring of security devices and services that form part of or whole of the security eco-system at the City of Doral, because they are suited to complete this service provisioning sooner than our competitors given their confidential knowledge of the City of Doral's security eco-system from our completion of the Security Assessment in the Fall of 2018.

**Section 3.** **Approval of Goods and Services.** The procurement of Clarium Security Operation Center (SOC) three-year (3) Year Remote Monitoring of security devices and services, in the amount of FY1819 **$58,800.00** for SOC monitoring and **$15,000** implementation.

**Section 3.** **Authorization.** The City Manager is hereby authorized to execute such agreements and other contractual documents, subject to approval by the City Attorney as to form and legal sufficiency, as may be necessary to consummate the procurement of the good and services contemplated herein. The City Manager is further authorized to expend budgeted funds in furtherance hereof.

**Section 4.** **Implementation.** The City Manager and City Attorney are hereby authorized to take such further action as may be necessary to implement the purpose and provisions of this Resolution.

**Section 5.** **Effective Date.** This Resolution shall take effect immediately upon adoption.

The foregoing Resolution was offered by Vice Mayor Mariaca who moved its adoption. The motion was seconded by Councilmember Cabral and upon being put to a vote, the vote was as follows:

| | |
|---|---|
| Mayor Juan Carlos Bermudez | Yes |
| Vice Mayor Claudia Mariaca | Yes |
| Councilwoman Digna Cabral | Yes |
| Councilman Pete Cabrera | Yes |
| Councilwoman Christi Fraga | Yes |

PASSED AND ADOPTED this 13 day of August, 2019.

JUAN CARLOS BERMUDEZ, MAYOR

ATTEST:

CONNIE DIAZ, MMC
CITY CLERK

APPROVED AS TO FORM AND LEGAL SUFFICIENCY
FOR THE USE AND RELIANCE OF THE CITY OF DORAL ONLY:

LUIS FIGUEREDO, ESQ.
CITY ATTORNEY