FINANCE/PERSONNEL SUBCOMMITTEE AGENDA

SUBCOMMITTEE MEMBERS

LARRY McCALLON, MEMBER
JOHN TIMMER, MEMBER

October 26, 2021
5:45 p.m.
Upright Conference Room
Highland City Hall
27215 Base Line
Highland, California

SPECIAL NOTICE REGARDING COVID-19

This meeting is being held in person. Please be advised, facial coverings or masks are required to be worn in the Upright Conference Room. If you do not have a facial covering or mask, one will be provided to you.

Submission of Public Comments: To limit the number of persons in the Upright Conference Room, the public is encouraged to make public comments by email rather than in person. For those wishing to make public comments by email, please submit your comments by email to be read aloud at the meeting. Email comments must be submitted by 4:45 p.m. on October 26, 2021, to publiccomment@cityofhighland.org. If you are submitting a public comment pertaining to an item on the October 26, 2021 agenda, please identify the agenda item number in the subject line. All email comments shall be subject to the same rules as would otherwise govern speaker comments at a Council meeting. Members of the public will be permitted to make public comments in person.

CITY OF HIGHLAND MISSION STATEMENT

Highland is dedicated to the betterment of the individual, the family, the neighborhood, and the community. The City Council and the staff of Highland are dedicated to providing the quality of public facilities and services that its citizens are willing to fund and will do so as efficiently as possible.

Visit the City's Website at: www.cityofhighland.org

THE CITY OF HIGHLAND COMPLIES WITH THE AMERICANS WITH DISABILITIES ACT OF 1990. IF YOU REQUIRE SPECIAL ASSISTANCE TO PARTICIPATE IN THIS MEETING, PLEASE CALL THE CITY CLERK'S OFFICE AT (909) 864-8732, EXT. 226 AT LEAST 48 HOURS PRIOR TO THE MEETING.

Any disclosable public records related to an open session item on a regular meeting agenda and distributed by the City of Highland to all or a majority of the Subcommittee less than 72 hours prior to that meeting are available for public inspection at Highland City Hall, 27215 Base Line, Highland, during normal business hours.

****

Larry McCallon, Member

John Timmer, Member

FINANCE/PERSONNEL SUBCOMMITTEE
October 26, 2021 – 5:45 p.m.

CALL TO ORDER

PUBLIC COMMENT

ITEMS

1. Review Minutes of October 12, 2021 Meeting
   RECOMMENDATION: Approve the Minutes as submitted.

2. Gap Analysis Quote – City of Highland Network
   RECOMMENDATION: That the Finance/Personnel Subcommittee review and consider the Gap Analysis Quote prepared by eSecurity Solutions for City of Highland's IT Network infrastructure to aid in developing a Risk Management Plan.

ADJOURN

I, Elena Rodrigues, Administrative Assistant III, of the City of Highland, California, certify that I caused to be posted this Agenda on the 21st day of October 2021, by 5:30 p.m. on our website at www.cityofhighland.org and in the following designated areas:

City Hall	Highland Branch Library	Highland Fire Station No. 1
27215 Base Line	7863 Central Avenue	26974 Base Line

Elena Rodrigues

Elena Rodrigues, Administrative Assistant III

Agenda Item #1

MINUTES
FINANCE/PERSONNEL SUBCOMMITTEE
October 12, 2021

CALL TO ORDER

The regular meeting of the Finance/Personnel Subcommittee of the City of Highland was called to order at 5:15 p.m. in the Donahue Council Chambers, 27215 Base Line, Highland, California.

ROLL CALL

Present: Timmer
Absent: McCallon

PUBLIC COMMENT

Received no public comment.

ITEMS

1. Review Minutes of September 14, 2021 Meeting
   Approved the Minutes as submitted.

2. 2020-2022 Community Development Block Grant (CDBG) – Corona Virus (CV) Highland Grocery Delivery Program
   The Finance/Personnel Subcommittee reviewed and approved the Highland Grocery Delivery Program to all income qualifying individuals.

ADJOURN

There being no further business the meeting was adjourned at 5:25 p.m.

Submitted by:

Elena Rodrigues

Elena Rodrigues, Administrative Assistant III

Approved by:

Subcommittee Member

Agenda Item #2

Solutions
eSecurity
Expert Security•Trusted Advice

We have prepared a quote for you

Gap Analysis Quote

Quote # 013409 | Version 1

Prepared for:

City of Highland

ProServices

Qty	Description	Price	Ext. Price
Payment Due is 100% Upfront.			
1	**Gap Analysis based on NIST CFS for Staff with 40 Users**	$15,000.00	$15,000.00
		Subtotal:	**$15,000.00**

Prepared For	Prepared By	Details
City of Highland 27215 Base Line Highland, CA 92346 Shawn Kasner skasner@cityofhighland.org (909) 864-6861	**eSecurity Solutions** Alex Mansour 866-661-6685 Ext 124 Fax 949-261-5556 amansour@esecuritysolutions.com	**Gap Analysis Quote** Quote #: 013409 Version: 1 Delivery Date: 10/14/2021 Expiration Date: 10/31/2021

One-Time Summary

Description	Amount
ProServices	$15,000.00
Total:	**$15,000.00**

Shipping, Handling and other fees may apply. We reserve the right to cancel orders arising out of pricing or other errors.

By signing this Sales/Services Order, customer is agreeing to the terms of Sales/Service Order and related applicable Agreements. If not covered by a Customer specific Agreement, Standard Agreements will apply. Copies of Standard Agreements can be found on www.eSecuritySolutions.com/Agreements	**Applicable Additional Services Agrements** **1) Master Services Agreement (MSA) and/or** **2) Professional Services Agreement**

Signature _____ Date _____

eSecurity Solutions
2280 University Dr., Ste 104
Newport Beach, CA 92660

STATEMENT OF WORK

CREATED BY: Michael Ruffolo
CUSTOMER: City of Highland

DATE CREATED: 08/11/2021
EXPIRES: 09/30/2021

eSecurity Solutions has a policy of advising our clients in writing of our understanding as to the scope of our services and then asking to confirm that your understanding is the same as ours.

eSecurity Solutions agrees to assist City of Highland to any extent requested for consulting on this security risk assessment project. City of Highland, at their sole discretion, determines the level of our involvement on this project.

Contents

Security Gap Analysis for Small Business 2
Objectives 2
NIST CSF Overview 2
NIST CFS Categories 3
Maturity Level 3
Scope of the Assessment 4
Security Review and Gap Analysis 4
Deliverables 5
Requirements 6
Time Frame 6
Adverse Conditions and Unaccounted Items 6
Payment Terms ..... **Error! Bookmark not defined.**

eSecurity Solutions
2280 University Dr., Ste 104
Newport Beach, CA 92660

Security Gap Analysis for Small Business

This statement of work has been prepared for City of Highland which shall be referred to as "the company" with this document.

Objectives

Provide "the company" with a remote assessment to review the foundations of information security in your organization through a Security Gap Analysis which is based on NIST CFS requirements.

The objective of the Security Gap Analysis is to gain a better understanding of your business environment and security requirements for your organizations IT/network infrastructure to aid the business in developing a Risk Management Plan with a focus on the NIST CFS Framework. eSecurity Solutions will conduct an interview with the IT/Network administrator and other knowledge staff with an understanding of your organization. The interviewees must have a thorough understanding of your network/IT infrastructure, security systems/controls, policies and procedures, and critical assets and key data/information. Based on the results of the interview, eSecurity Solutions will create a Security Report that outlines your organizations strengths and weakness regarding security for your IT/network infrastructure and recommendations to improve your security posture.

NIST CSF Overview

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was published in February 2014 as guidance for critical infrastructure organizations to better understand, manage, and reduce their cybersecurity risks. The CSF was developed in response to the Presidential Executive Order on Improving Critical Infrastructure Security, which was issued in February 2013. NIST released the CSF Version 1.1 in April 2018, incorporating feedback received since the original CSF release. An Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed in May 2017 requires US government agencies to use the NIST CSF or any successor document when conducting risk assessments for agency systems. Each agency head is required to produce a risk management report documenting cybersecurity risk mitigation and describing the agency's action plan to implement the CSF.

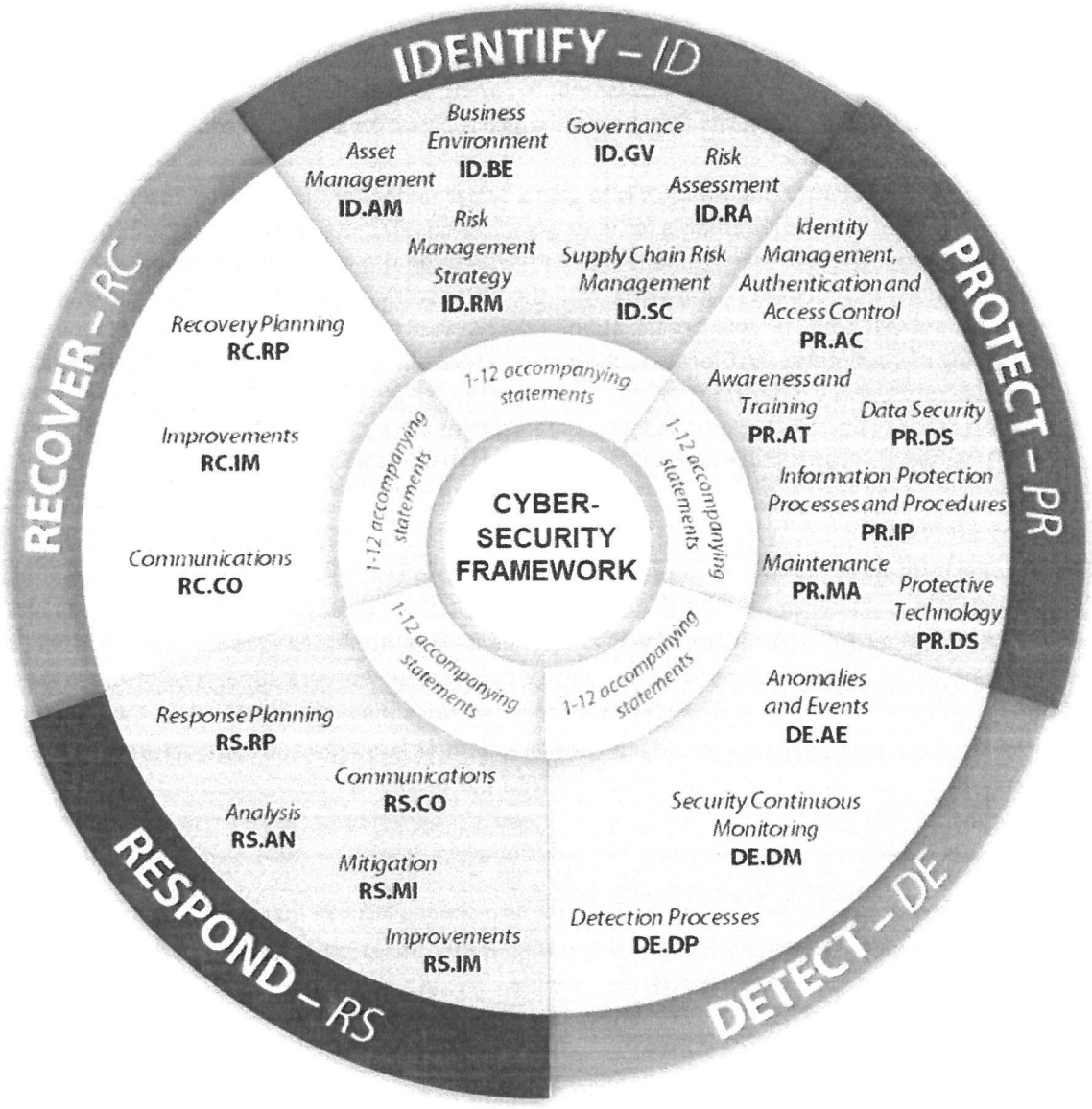
The NIST CSF references globally recognized standards including NIST SP 800-53. Each control within the CSF is mapped to corresponding NIST 800-53 controls within the US Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

NIST CFS focuses on 5 high-level functions:

- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Each of the 5 high-level functions are broken down into 23 categories.

NIST CFS Categories



Maturity Level

Each category is evaluated by maturity. The more mature, the better.

Maturity Level 1: Initial

- At this level, there are no organized processes in place. Processes are ad hoc and informal. Security processes are reactive and not repeatable, measurable, or scalable.

Maturity Level 2: Repeatable

- At this stage of maturity, some processes become repeatable. A formal program has been initiated to some degree, although discipline is lacking. Some processes have been established, defined, and documented.

Maturity Level 3: Defined

- Here, processes have become formal, standardized, and defined. This helps create consistency across the organization.

Maturity Level 4: Managed

- At this stage, the organization begins to measure, refine, and adapt their security processes to make them more effective and efficient based on the information they receive from their program.

Maturity Level 5: Optimizing

- An organization operating at Level 5 has processes that are automated, documented, and constantly analyzed for optimization. At this stage, cybersecurity is part of the overall culture.

Scope of the Assessment

Security Review and Gap Analysis

eSecurity Solutions will conduct a review of IT architecture and security strategy for "the company". Leveraging the extensive experience of eSecurity Solutions security team to understand "the company" profile, key assets, how and who access your data, and controls you have or should have in place to protect your assets and assist you in achieving your Compliance and Security Objectives.

Project Initiation

- Tasks
  - Hold kickoff meeting with internal stakeholders
  - Determine which systems and processes are in scope
  - Confirm project plan (timeline / milestones)
  - Ensure adequate resources are available to support the assessment
  - Submit discovery request to client for the required documentation
- Estimated Time Frame: Weeks 1
- Deliverable: Kick off meeting, Key Stakeholders and resources defined, Project plan

Data Gathering & Discovery

- Tasks
  - Receive discovery documentation from client
  - Review all discovery documentation and conduct required follow ups
- Estimated Time Frame: Week 2
- Deliverable: Receive discovery documentation

Execute Security Assessment

- Tasks
  - Interview key stakeholders and personnel

    - Compile working papers and assessment data
- Estimated Time Frame: Week 3
- Deliverable: Assessment. Working Papers

Analyze Assessment Data, Gap Analysis & Final Deliverables

- Task
    - Analyze assessment data
    - Document implementation gaps against framework requirements
    - Draft gap analysis and security assessment report
    - Submit initial deliverable(s) to client
    - Client review and feedback
    - Finalize client deliverables
- Estimated Time Frame: Week 4
- Deliverable: Gap analysis and Security Assessment Report

*** Exclusions:** Personal equipment / laptops, vulnerability scans, data privacy assessment, custom reports.

Deliverables

eSecurity Solutions will provide verbal results on all findings on a daily, weekly, or as needed basis. At the conclusion of the assessment, we will provide an Executive Summary report and a Detailed Technical report.

The Executive Summary report contains a summary of the test/assessment performed and the overall finding with non-technical descriptions of all high-risk findings along with the business risk associated with each finding, a table displaying a count of Critical, High, Medium, and Low items discovered (if applicable) and restates the project scope.

The Detailed Technical reports starts with a copy of the Executive Summary report followed by a findings section structured to facilitate remediation of deficiencies by client security or technical staff, and although we can omit and add additional areas (such as management response) by request, the listing typically includes the following information for each vulnerability found as part of our assessment efforts:

- A text description of the vulnerability
- The host(s) affected by the vulnerability
- The relative business and technical risks of the vulnerability
- The vulnerability classification (high, medium or low) that describes the risk level as a function of the role that the exploited item or technology plays in supporting the business. For example, if a commonly used delivery area of the facility is insecure and gets exploited and that entry way allows entry into largely populated or highly secured areas of the facility that entry way may pose a higher risk than the front door that provides limited access to other areas of the facility
- Technical description of how to reduce or eliminate exposures of the vulnerabilities

The Detailed Technical report also includes all the findings (if applicable) including detailed on how we tested/assessed each item and what we discovered.

Requirements

eSecurity Solutions will:

- Review this scope of work at the start of the project and verify goals and existing environment are accurate to complete the project as required.
- Execute on the steps listed in the scope of work in a timely fashion and inform "the company" of progress on a weekly basis.
- Review the project plan and the time required to complete the project and request any adjustments if necessary.

"The company" must provide:

- Dedicated time (phone call) to complete a survey with eSecurity Solutions engineer
- Network diagrams and IT infrastructure and security systems and controls documentation
- Dedicated time to speak with personnel with a thorough understanding of your network/IT infrastructure and security systems and policies (phone call)
- Dedicated time to speak with personnel with a thorough understanding of your critical assets and key data/information (phone call)

Time Frame

The project kickoff will usually start 2 to 4 weeks after project approval (allowing time to allocate appropriate resources). The project will take approximately 4 weeks to complete and deliver final report the management team after the project kickoff.

Adverse Conditions and Unaccounted Items

In order to ensure non-biased reporting, this engagement shall be conducted independently from "the company" staff and "the company" staff will have no influence on tools or processes used to conduct the assessment.

Disclosure of adverse conditions that potentially could affect this project.

- "The company" ability to response in a timely fashion to eSecurity Solutions requests via email or phone.
- "The company" ability to schedule time for conference call with eSecurity Solutions review portions of complete documentation and provide information in a timely fashion.
- Scope creep (changing of scope), this SOW specifically outlines what is included in the scope and deliverable, any changes to scope or deliverables will require quoting out additional services.
- If "the company" has a need to delay or stop this engagement after Engagement Initiation, eSecurity Solutions makes no guarantee that personnel/resources assigned to this engagement will be available following work resumption

- Infrastructure assessments may be performed against production systems; eSecurity Solutions will make reasonable efforts to minimize impact to production systems, however, eSecurity Solutions cannot guarantee/warrant zero production system impact

eSecurity Solutions is not responsible for:

- Third party software functionality within Client's existing technical environment
- Management decisions with respect to this project
- Data consistency and integrity issues
- Activities related to system programming and certification of reporting results

During the course of this Project, the need to accept Deliverables will occur. Transmittal of Deliverables shall be submitted by eSecurity Solutions using the following procedure:

- "The company" shall be informed by eSecurity Solutions when a Deliverable is completed and available for review and approval. "the company" shall have a maximum of 5 business days to review the Deliverable for conformity with this SOW
- In the event that "the company" rejects a Deliverable, "the company" must provide eSecurity Solutions with a notice of deficiencies. eSecurity Solutions will correct any identified deficiencies within 10 calendar days (the "Correction Period") and shall submit such corrected Result to "the company" for review as set forth above