



Office of the City Manager

CONSENT CALENDAR
July 24, 2018

To: Honorable Mayor and Members of the City Council
From: Dee Williams-Ridley, City Manager
Submitted by: Savita Chaudhary, Director, Information Technology
Subject: Contract: Presidio Networked Solutions Group, LLC for the development of a Cyber Resilience Plan (CRP)

RECOMMENDATION

Adopt a Resolution authorizing the City Manager to execute a contract with Presidio Networked Solutions Group (“Presidio”) to develop a Cyber Resilience Plan (CRP), for a total not to exceed \$100,000 from July 25, 2018 to June 30, 2019.

FISCAL IMPACTS OF RECOMMENDATION

One time funding for this project is allocated in the Department of Information Technology’s Fiscal Year (FY) 2019 General Fund budget as follows, and is subject to Council approval of the proposed City-wide budget and Annual Appropriation Ordinances:

	FY 2019 Professional Services
\$100,000	Budget Code: 891-2701-410-3038 (Information Technology Cost Allocation Plan Fund , Information Technology, Professional Services)
<hr/>	
\$100,000	Total FY 2019 Professional Services

The funding for this contract will be included in the First Amendment to the FY 2019 Annual Appropriations Ordinance.

The contract has been entered into the City’s contract management system and assigned CMS No. LJEC4.

CURRENT SITUATION AND ITS EFFECTS

The Cyber Resilience Plan (CRP) is a critical step in establishing the strategy, methodical approach, and evolving cyber-security plan for the City of Berkeley. The CRP development and planning process will be a citywide effort involving key staff representing multiple departments.

The CRP has two primary goals. The first goal is to develop a comprehensive needs assessment that discusses cyber resilience objectives and the requirements of each City

department. The second goal is to provide an implementation plan with a holistic roadmap that addresses cyber security concerns, staff training, and provides a strategy with actions and concerns. The CRP will align with the City's vision of reducing cyber-risk exposure, maturing cyber-security capabilities, technologies and systems, and effecting efficient regulatory compliance.

In developing the needs assessment, Presidio will conduct surveys, interviews, and onsite workshops with Staff to provide an assessment and analysis that considers the culture, business expectations, and business needs of the City. Workshops with the City's Department Directors and key staff members will determine cyber resilience gaps, potential milestones, as well as timing gates and dependencies. The assessment will also discuss the cyber resilience objectives and requirements of each Department as well as opportunities for incorporation of existing activities, staff, systems, resources, plans, vehicles, and of supporting emergency and disaster response capabilities into the cyber resilience strategic plan and roadmap.

The CRP will assess current gaps and evaluate the City's current cyber resilience posture, capabilities, and technology environment, including services provided, cybersecurity and application portfolio, infrastructure tools, organizational readiness, funding, product lifecycles, and service methodology.

The final task is to develop an implementation plan that addresses the most critical cyber resilience needs over the next five years, and serve as a crucial tool to not only measure our performance, but to push us to look at the possibilities of what we can and should be doing to continue innovating as we deliver projects and services to the City of Berkeley community. The CRP will be a living document which will be updated every three to five years and will help us identify the organizational priorities in line with our Department's vision, mission and values.

BACKGROUND

The City of Berkeley is one of 100 cities worldwide that has been designated by the Rockefeller Foundation as a Resilient City and as such has produced a plan to be more resilient to physical, social, and economic shocks and stresses. The City has also adopted a City-wide Strategic Plan and a five-year Digital Strategic Plan (DSP), with the latter setting priorities, identifying budget expectations, and scheduling projects and milestones that contribute to transforming technology. Finally, the City has also adopted Department of Information Technology (DoIT) GIS Master Plan and is looking into Smart city and Internet of Things (IoT) initiatives, including micro grid and a solar powered garage.

The City's Cyber Resilience Program is to be built around five (5) core focal points: (1) the unique balance of data privacy, transparency and security that defines a California municipality and Berkeley in particular; (2) a program that is designed to include, create new and/or evolve existing functions that are key across each focal area; (3) that set of policies and rationale that facilitate a thriving and resilient cyber program; (4) the foresight, monitoring, response and mitigation that are essential in cyber incidents up through events impacting technology's role in enabling continuity of government as well as the

delivery of a smart-city services; and (5) training that builds, matures and nurtures a culture of cyber reliance across all departments and levels of the municipality.

More Specifically:

- (1) **Data Transparency, Data Privacy and Data Security** – Creation of a program driven by a data classification and controls framework that enables uncontentious and judicious availability, access, management and monitoring of data relating to contractual, local, State and other relevant code/definitions of “private” (or “confidential”) data, including but not limited to criminal, EHD and HIPAA, PII, PCI, and City of Berkeley ordinances and vehicles (e.g., Memorandums, boilerplate contracts, NDAs, business license form), and align to the California Public Records Act.
 - Will drive capability, and security, and application requirements.
 - Will address the public’s right to know, data exchange (e.g., interagency) and situations where data privacy is compromised, data is stolen, held hostage, illicitly altered.
- (2) **Program Functional Design** – Creation of a foundational program that contains the leading cyber security programmatic elements to meet today’s cyber resilience needs. This focus will include strategy and objectives, the business of the cybersecurity program, its organizational structure, budgeting, process, communications plan, governance, and more. This focus area will also be designed for the evolution of the program aligned with City of Berkeley’s transformation into an increasingly Smart city.
- (3) **Policy and Rationale** – Creation of a Charter for the cyber resilience organization and the set of policies, methodologies, processes which it will provide, as well as the vehicles it will execute (e.g., contract pro forma, enterprise security architecture, test plans, etc.). Will include a cyber risk assessment function which will provide the rationale for when risk assessments need to occur and the selection of controls. This focus area will plan for the establishment of the cyber resilience policy, governance surrounding the policy, cyber resilience participation and gateways in City business work efforts and projects, and cyber resilience compliance and testing, security optimization and effectiveness metrics – e.g., Key Performance Indicators (KPI’s).
- (4) **Monitoring, Response & Mitigation** – This focus area seeks to mature and integrate the City of Berkley’s cybersecurity incident response and management capabilities (IR), and support for City and Departmental emergency management plans and organizations, including but not limited to DoIT’s Business Continuity and Disaster Recovery, DoIT’s participation in City Continuity of Government (CoG)/Continuity of Operations (COOP) and Community-centric Emergency Response (DOC / EOC / OES). It will address Business Impact Analysis (BIA), Business Recovery, Resumption and Contingency, the maintenance, execution and coordination of local and regional Plans, table top and other exercises, and communications plans.

- (5) **Training and Culture** – Creation of a security awareness program that changes the culture within and across the City of Berkeley through both basic end-user awareness training for all staff at all levels as well as IT staff. The CRP should identify the strategic benefits as well as the reasons and value factors and propositions for each department and staff member of the City of Berkeley (including “what’s-in-it-for-me”). This focus area may include computer-based training (CBT) within its mix of awareness days/open-house days, Video trainings, communications schedules and campaigns, reinforcement tools/vehicles, and topical/functional sessions and workshops. And, the efforts will be designed to reduce the risk of known attacks targeting people and processes (e.g., anti-phishing training, “CEO-fraud,” secure use of the Internet, etc.) as well as to provide individual and cultural-change effectiveness and optimization measuring and reporting.

The Cyber Resilience Plan (CRP) is an important part of establishing the strategy, methodical approach and evolving cyber-security plan for the City of Berkeley. This CRP aligns with the City’s vision of reducing cyber-risk exposure, maturing cyber-security capabilities, technologies and systems, and effecting efficient regulatory compliance. The new CRP should specify ways in which recommended solutions will improve the City of Berkeley’s operations and overall service delivery, streamline operations to achieve cost efficiencies and increased productivity, and support open and transparent governance.

ENVIRONMENTAL SUSTAINABILITY

By establishing a strategic plan that aligns the cyber-security needs of each department with a holistic implementation roadmap, the CRP provides the opportunity to advance the City’s environmental sustainability goal to maintain an environmentally-sound information technology infrastructure. Specifically, the software and hardware purchases that are made as a result of this CRP have the opportunity to be fiscally and operationally sustainable as well as driven by policy and rationale.

Additionally, Presidio will conduct some of their work remotely, and when they do come on-site for face to face meetings, they will cluster those visits over multiple days to minimize both travel costs and greenhouse gas emissions related to travel.

RATIONALE FOR RECOMMENDATION

A review committee of eight evaluated each of the fourteen (14) RFP responses and determined that Presidio’s proposal best fits the City’s business and fiscal requirements. Staff recommends the Presidio Networked Solutions Group to develop the Cyber Resilience Plan (CRP). The timeline of the project will allow for recommendations from the consultant to be considered to be incorporated into the City’s FY20/FY21 budget.

ALTERNATIVE ACTIONS CONSIDERED

Staff considered developing the Cyber Resilience Plan internally, however Staff determined it would be most beneficial to obtain an outside perspective that provides industry best practices and experience working with other local municipalities to help establish a framework that the City can use for the next three years and beyond.

CONTACT PERSON

Savita Chaudhary, Director, Information Technology, 510-981-6541

Attachments:

1: Resolution

RESOLUTION NO. ##,###-N.S.

CONTRACT: PRESIDIO NETWORKED SOLUTIONS GROUP FOR THE
DEVELOPMENT OF A CYBER RESILIENCE PLAN

WHEREAS, a Cyber Resilience Plan (CRP) is an important part of establishing the strategy, methodical approach, and evolving cyber-security for the City of Berkeley; and

WHEREAS, recommended solutions will improve the City of Berkeley's operations and overall service delivery, streamline operations to achieve cost efficiencies and increased productivity, and support open and transparent governance; and

WHEREAS, on March 02, 2018, the City issued a Request for Proposals (RFP) for a Cyber Resilience Plan (CRP) (Specification No.18-11195-C) and received 14 qualifying vendor responses; and

WHEREAS, the RFP review committee evaluated each proposal and determined that the Presidio Networked Solutions Group, LLC ("Presidio") proposal best met the City's operational, technological, and fiscal requirements; and

WHEREAS, funding for this contract has been allocated in the Department of Information Technology's FY 2019 General Fund Budget and is subject to Council approval of the proposed City-wide budget and Annual Appropriation Ordinances, and is entered into the citywide contract database as CMS No. LJEC4.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Manager is authorized to execute a contract and all amendments with the Presidio to developing a Cyber Resilience Plan (CRP) for the Department of Information Technology, for a total not to exceed \$100,000 from July 25, 2018 to June 30, 2019.