



Board Report

File #: 2022-0511, File Type: Contract

Agenda Number: 40.

OPERATIONS, SAFETY, AND CUSTOMER EXPERIENCE COMMITTEE SEPTEMBER 15, 2022

SUBJECT: AGENCY ENTERPRISE SECURITY ARCHITECTURE ASSESSMENT

ACTION: APPROVE CONTRACT AWARD

RECOMMENDATION

AUTHORIZE the Chief Executive Officer to award a professional service firm-fixed price Contract No. PS77693-3000 to Regents & Park, in the amount of \$1,259,400, subject to resolution of protest(s), if any.

ISSUE

High-profile cyberattacks on public and private infrastructures such as the recent intrusion of the New York MTA, the ransomware attack on the Colonial Pipeline operation, and the breach of the JBS meat-packing plants highlight the vulnerable nature of critical infrastructure and the emerging threat profile of public and investor-owned systems. Further, the organizations' true economic and public-trust reputation suffered because of these financially motivated malicious criminal activities.

Entities or groups that attempt to breach computer security, including foreign governments that sponsor or condone activities to access data/intelligence to target governments, organizations, or individuals (aka nation-state actors), have become more sophisticated over time while private and public sector organizations struggle to keep up with new threats introduced by advancing technology and the need to support these vital systems.

BACKGROUND

Metro must continually review and improve its information security posture to manage the current and evolving risk and threat landscape. While Metro is actively implementing recommendations and remediations from other completed security reviews, it is evident Metro must concurrently engage and contract with a well-qualified information security consulting firm in assessing modern Agency IT, IoT/ Industrial Internet of Things (IIoT) systems and SCADA/ICS asset risks.

Keeping with the agency-wide goal of providing safe, secure, private, efficient, and high-quality services to its customers, Metro has identified the following non-exhaustive list of Cyber Security Domains to be included in the scope of this Security Architecture Review (SAR).

- Governance, Compliance, and Organization
- Data Protection
- Security Risk Management
- Tiered Security
- Centralized Management
- Least Privilege/Least Denial
- Role-based Access Authorization
- Separation of Duties
- Identity and Access Management
- Incident Response
- Host and Endpoint Protection
- Application, Database, and Mobile Protection
- Network Cloud and Data Center
- Security Awareness Training
- People
- Process
- Tools

DISCUSSION

Metro intends to contract with Regents & Park to conduct an in-depth evaluation of the agency's information security program and architecture.

The result of this agency-wide assessment will provide the following deliverables:

- Highlight existing and future weaknesses in the Metro Security Architecture;
- Provide recommendations for improvement in key performance areas;
- Outline and prioritize short, medium, and long-term recommendations designed to improve the organization's security posture based on its risk profile and level of security maturity at the time of review; and
- Identify and examine the holistic risk posture of the organization to provide specific findings where organizational economies-of-scale through automation could lend to a reduction in operational complexity, organizational risk, and costs.

The Security Architecture Assessment will perform a study that uncovers systemic security issues in our environment. Metro would like to maximize its return on any security technology investment by evaluating our needs and validating the security of our existing deployments. The result is an actionable roadmap to help remediate identified security deficiencies.

This review and assessment output will complement ongoing Governance, Risk Management and Compliance (GRC) initiatives and provide the foundation for Metro's Security technology roadmaps.

DETERMINATION OF SAFETY IMPACT

The contract award will directly and positively impact the agency's safety, security, service quality,

and systems reliability posture. Providing a current and refreshed agency-wide assessment of the current Metro IT security architecture and risk profile provides senior leadership with the visibility and insights to make informed technology and resource decisions to secure the Metro Enterprise and its supported systems adequately.

FINANCIAL IMPACT

Funding for this service is included in the FY23 Adopted Budget under Project Number 300119, Cyber Security Architecture Assessments, Cost Center 2613 - Physical Security.

Impact to Budget

The funding source is an FY20 Transit Security Grant Program (TSGP) Award for Facilities Hardening, Video Management System/Security Intelligence, and Cyber-Security, which is not eligible for bus and rail capital and operating expenditures. No other source of funds was considered for this project because the TSGP funding completely covers this expenditure.

EQUITY PLATFORM

Metro technology systems and services are contained within data centers, rail operations centers, subway stations, and bus garages in multiple locations throughout LA County. These on premise and web-based systems host various bus/rail, bike, rideshare, and related services serving all demographic communities. This contract will identify potential security risks so they can be addressed and remediated, thus preserving the public trust of Metro's stakeholders.

The services are not anticipated to impact the external customer community adversely (e.g., people of color, low income, disabled, marginalized communities, minorities, women, disadvantaged or disabled veterans).

This open solicitation included a Small Business Enterprise (SBE) goal of 12% and a Disabled Veteran Business Enterprise (DVBE) goal of 3% for the project management contract. The recommended firm made a 30.54% SBE commitment and a 4.17% DVBE commitment.

IMPLEMENTATION OF STRATEGIC PLAN GOALS

The Security Architecture Assessment supports **Metro Vision 2028 Strategic Goal 5**: Provide responsive, accountable, and trustworthy governance within the Metro organization.

ALTERNATIVES CONSIDERED

The Board may choose not to proceed with the contract award. This option is not recommended based on the need and desire to protect, defend, and secure real-time information and mission-critical infrastructure from cyberattacks; and the commitment to continually enhance the security and privacy of information and data for our customers.

NEXT STEPS

Upon approval by the Board, staff will execute the contract, and the contractor will provide a Project Management Plan (PMP) with a detailed review and work breakdown structure (WBS) schedule focused on the key activities to produce the contract deliverables and other warranted deliverables based on the vendor's methodology/approach for conducting information security engagements over a twelve-month (12) period following award.

ATTACHMENTS

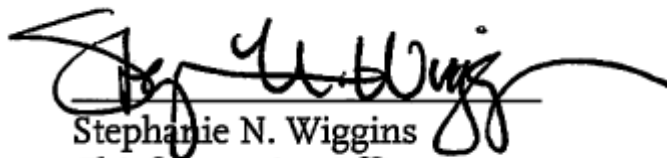
Attachment A - Procurement Summary

Attachment B - DEOD Summary

Prepared by: Janice Lim, DEO Enterprise Information Management, Information Security, (213) 922-5590
Bill Balter, DEO Enterprise Information Management, ITS Administration, (213) 922-4511
Joe Giba, EO Information Technology, Operations and Service Delivery, (213) 922-3450
Susan Walker, Director, Physical Security, (213) 922-7464

Debra Avila, Deputy Chief VCM Officer (213) 418-3051

Reviewed by: Bryan Sastokas, Chief Innovation Officer (Interim), (213) 922-5510
Robert Bonner, Chief People Officer, (213) 922-3048



Stephanie N. Wiggins
Chief Executive Officer