Florida Seaport Transportation and Economic Development Council

Canaveral Port Authority · Port Citrus · Port Everglades · Port of Fernandina · Port of Fort Pierce
Jacksonville Port Authority · Port of Key West · Manatee County Port Authority · PortMiami · Port of Palm Beach
Panama City Port Authority · Port of Pensacola · Port St. Joe Port Authority · Port of St. Petersburg · Tampa Port Authority ·
Florida Department of Transportation · Florida Department of Economic Opportunity

Request for Solution Proposals: Description of Commodities or Contractual Services Sought

POSTING DATE: March 7, 2018

RESONSES DUE: March 16, 2018

FROM: Florida Seaport Transportation and Economic Development Council

SUBJECT: **COMMON OPERATING PICTURE (COP) ENTERPRISE LEVEL SOFTWARE SOLUTION FOR ENHANCED MARITIME AND CYBER SECURITY DOMAIN AWARENESS THROUGHOUT THE STATE OF FLORIDA PROCUREMENT**

I. Overview.

Pursuant to section 287.057(3)(c), Florida Statutes, the Florida Seaport Transportation and Economic Development (FSTED) Council is seeking to purchase a common operating picture (COP) enterprise level software solution for enhanced maritime and cyber security domain awareness throughout the State of Florida. Florida has sustained multiple natural disasters over the years and has identified gaps in information sharing during these events. The FSTED Council wishes to strengthen the level of maritime domain awareness and communications at Florida's seaports, during natural and manmade events, between ports and other government agencies within the State.

While no Florida port has been identified as experiencing a significant cyber-attack, a shipping line operating out of Florida ports was the target of an attack that caused a disruption to the Florida supply chain. As a part of this project, the FSTED Council wishes to identify a technology solution capable of increasing our awareness of potential cyber-attacks and strengthening our cyber security response capabilities.

The FSTED Council is seeking a COP solution to be deployed in up to 14 Florida ports and other state or regional agencies, as needed.

II. Detailed Specifications Section. The COP solution must include the following features:

A. Users.

1) The COP solution will be a web-based system, which will allow any authorized user with a workstation to access the solution.

2) Any proposal will allow for each of Florida's 14 active ports to be provided one (1) to five (5) simultaneous connections to the web-based system. The total connections per seaport will be determined by the data governance / integration team during the development process and after COP final acceptance.

3) Provisions for up to ten (10) additional non-port agencies to be provided with a simultaneous user connection to the web-based system. These additional agencies will be determined by the data governance / integration team during the development process and after COP final acceptance, as needed.

B. Hosting.

1) The web-based system will run in a hosted and managed server environment at a highly secure co-located facility, located in the continental United States. All development, testing, production and backup environments shall utilize best-in-class servers. Server data centers are required to be secure environments with access strictly controlled by a double layer (e.g., card, pin, or biometrics) access protocol system.

2) The provider of maintenance service and support must be located and operate in the continental United States, with all primary and backup servers for the development, testing and production, and backup environments of databases located in the continental United States, in physically secure and protected facilities. No outsourcing or off-shoring maintenance or development is permitted.

3) All systems and data will be available and accessible 24 hours a day, and 7 days a week. The servers should be patched, updated, and maintained on a monthly schedule (or sooner if required). Services and efforts shall be made to ensure that the server hardware is functioning, capable and efficient for the demands placed on the system. Systems shall be continuously monitored and, when necessary, repaired, updated, and enhanced for efficiency and stability.

4) Appropriate sub systems shall be incorporated to ensure that server security is maintained at a high level and suitable backups are initiated. In addition, the production environment will have a fully redundant failover to the virtual environment in a second location, located within the continental United States. The servers must meet and exceed all industry standards of best security and backup practices. Systems should utilize encryption for user access, with all access events logged and monitored.

C. Functional Specifications.

1) Marine vessel Automatic Identification System (AIS) tracking, with all associated AIS information for all vessels within 25 nautical miles of the port.

2) Integration of port video, radar and sensor systems.

3) Individual configured rules for each port including zone entry rules, line crossing rules, speed zone rules, predetermined user alerts, and others.

4) Individual configured zones for reports and creating alarm zones.

5) Integration with weather monitoring and forecasting service and National Oceanic and Atmospheric Administration (NOAA) weather buoys, where services are publicly available.

6) Nautical chart (NOAA online) integration.

7) Integration of Geographic Information System (GIS) data features (e.g., points, lines, polygons, jurisdictional boundaries, tenant information, shore based structures, fuel tanks,

buildings, critical assets, pipe lines, or electric lines), if GIS information already exists for individual ports, in a compatible format.

8) Quick access to historical data for analysis, reporting and training purposes. Including, a replay capability of vessel tracks for areas of a port's area of responsibility.

9) Reports based on data provided by U.S. Customs and Boarder Protection (CBP), when available.

10) Economic reports to support economic monitoring and development.

11) Connectivity to a certified Maritime and Port Security Information Sharing & Analysis Organization (MPS-ISAO) or service for a minimum of one year. This service shall allow access to critical cyber issues that can impact port operations. This includes:

- **a.** Cybersecurity situational awareness intelligence products, including daily advisories and alerts, analytical reports, and webinars.
- **b.** Access credentials to a cyber threat intelligence information sharing platforms, including port and maritime customer sharing, security partner sharing (e.g., cyber intelligence, dark web monitoring, key logger outputs, sinkholes monitoring, etc.), multi-directional information sharing with other sector ISAOs/ISACs via the International Association of Certified ISAOs (IACI), and the U.S. Department of Homeland Security.
- **c.** Access credentials to a secure communications platform which hosts the threat intelligence repository.
- **d.** Services must be available at time of COP beta roll-out and extend at a minimum, to the end date of the contract service period with the FSTED Council.

12) Compatibility with integrated situational awareness and information sharing platforms, already adopted by four (4) Florida ports.

13) Collaboration with state and local agencies. Authorized agencies can view the data in the system, and coordinate with local resources in support of law enforcement and emergency operations. This capability includes:

- **a.** Information from the AIS system and other tracking systems.
- **b.** Information for critical structures such as owners, coordinators, contact information etc.
- **c.** Management tools for emergency situations including preplanned checklists, dynamic checklist creation and management, checklist execution tracking, integration of other assets and systems into the response, replay, and analysis tools.
- **d.** Integration of a critical asset resource reporting tool that will allow voluntary coordination between agencies. This feature will allow ports to report to their state partners' critical information during state wide emergencies, including the tracking of strategically important port or tenant resources (e.g., petroleum) or status (e.g., open or closed).
- **e.** A minimum of three (3) graphical user interfaces (GUI's) will be provided that allow ports to report information to authorized users. Based on additional discussions, GUI's will be determined after contract signing and during project kickoff meetings.

III. <u>Compatibility</u>. Four (4) of the fourteen (14) ports have already competitively procured, adopted and integrated situational awareness and information sharing platforms. The COP solution must provide both baseline and enhanced components for up to fourteen (14) ports. The service period of existing platforms, already integrated by the four (4) ports, may expire during the period of this Agreement, and at different intervals. Services covered under the COP solution contract service period must be seamless, so that there is no lapse in services during transitions between vendors or services.

The platform will be compatible with all existing COP solutions, already integrated by the four (4) ports, and provide enhanced components to supplement existing COP solutions. The other identified remaining ports will receive both baseline and enhanced COP solution components, which are compatible with existing COP solutions, already integrated by the four (4) ports. Compatibility is important, because the platforms of all ports must be able to communicate with each other, and with COP solutions provided to and accessed by state and local agencies.

IV. Contract Purchase Limit. The initial cost of the purchase of the COP solution shall not exceed $500,000. The FSTED Council may enter into a multiple year contract for the COP solution, and ongoing system operation, maintenance and support should be provided in the response by any prospective service provider. A minimum of one calendar year (365 days; commencing on the date of final system acceptance) of system operation, maintenance and support will be incorporated into the initial cost.

V. Prospective Service Provider Response Requirements. Any service provider wishing to provide the COP solution and additional services requested, shall provide the following:

- **A.** A cover letter introducing the company to FSTED and the name of the individual authorized to enter into contract negotiations and execute the contract with FSTED. The letter shall discuss the company's main service offerings, how long they have been in business, and the vertical markets served. Please include your company's legal name and 12-digit "Document Number" for verification purposes by FSTED that your company is registered to do business in the State of Florida.
- **B.** Provide a description of how you plan to approach this project. This section shall discuss all phases of anticipated project planning, deployment, and training typically utilized in large scale enterprise level deployments of your solution. The section shall not exceed ten pages.
- **C.** Provide a technical description of your proposed solution that meets the requirements of the "Detailed Specifications Section" of this Request for Proposal. The section shall not exceed 4 pages.
- **D.** Provide at least six (6) port locations where your COP solution is currently deployed. Please include the name of the seaport and the length of time the solution has been provided to that seaport.
- **E.** Provide a not to exceed guaranteed maximum price for the cost of services to deploy, train, operate, and maintain the solution for a period of one year from the date of final acceptance.
- **F.** Provide a guaranteed price for operations, maintenance and support on an annual basis, for a period of three years after the first year (year 2, year 3, and year 4).

VI. FSTED Proposal Point of Contact. Please submit proposal packages to Mr. Michael Rubin, FSTED Council Assistant Secretary, at the following address:

Michael Rubin
Assistant Secretary
FSTED Council
502 East Jefferson St.
Tallahassee, FL 32301

VII. Transmittal of Proposals. Proposals are due by 5:00 pm (EST) on March 16, 2018. Proposals shall include one (1) original hard copy and electronic copies on four (4) USB drives, with all required documents referenced in this *Request for Proposals*, organized and collated into a single portable document file (.pdf) format. The submittal package shall be transmitted in a single, sealed envelope clearly marked: "Proposal Submission for a Common Operating Picture (COP) Enterprise Level Software Solution for Enhanced Maritime Domain Awareness at Florida's Seaports."