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**

<u>Notice of Intent to Award a Sole Source Procurement</u>

DATE: September 30, 2019

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**

This is <u>not</u> a Request for Proposals and there is no solicitation available. Pursuant to section 287.057(3)(c), Florida Statutes, the proposed contract action is for product or services for which the Florida Seaport Transportation and Economic Development (FSTED) Council intends to negotiate and award with only one source. Any responses received as result of this Notice of Intent shall be considered solely for the purpose of determining whether to conduct a competitive procurement. Responses will <u>not</u> be considered as proposals, bids, or quotes.

Interested firms or individuals may identify their interest and capability to respond to the requirement by submitting in writing their name, address, point of contact, telephone number, email, and a statement regarding capability to provide the specified procurement. Interested firms will be considered only if they respond with clear and convincing documentation that they are capable of meeting or exceeding the requirements stated on the attached procurement requirement. All responses received within seven (7) business days after the date of publication of this memorandum synopsis will be reviewed by the FSTED Council. A determination by FSTED Council staff not to compete this proposed action based on the responses to this notice is solely within the authority of the FSTED Council staff. All responses must be in writing and returned to ATTN: Michael Rubin, FSTED Council Assistant Secretary, 502 East Jefferson Street, Tallahassee, FL 32301, by e-mail mike.rubin@flaports.org Note the subject line of this memorandum synopsis on any documentation.

FSTED Council Sole Source Purchase Requirements

The FSTED Council purchased a common operating picture (COP) enterprise level software solution for enhanced maritime and cyber security domain awareness throughout the State of Florida in March 2018. As approved by the FSTED Council in their meeting on August 28th, the Council will be replacing and upgrading the existing ARES Command Bridge Common Operating Picture (COP) platform with a new Command and Control platform.

This new platform must use the existing Command Bridge platform, and provide enhanced features, capabilities and ease of use. The platform must be built on HTML 5 (no reliance on plug-ins or Internet Explorer) and utilizes a clustered server environment for a more reliable system. This new platform must use an upgraded server to allow for the additional state-wide enhanced features and any port-specific integrations at Florida's fourteen seaports. This will enable each port to integrate the systems/sensors of their choice over time and automate workflows and procedures throughout the port. The upgraded system must also allow each port to share information with state and local government and response agencies.

The platform must utilize an ecosystem approach so numerous organizations can be added within the same system yet maintain autonomy of data and sharing permissions. The CARRT (Critical Asset Resource Reporting Tool) application that was developed for the original purchase must remain available, and be reformatted for use within the new system.

This new platform must also focus on enhancing each port and their unique operations and provide a truly scalable system for state-wide collaboration.
The upgraded system must provide additional value to Florida's seaports and other federal and state users through the following enhancements:
- All functionality from the Phase 1 Command Bridge deployment
  - Including option to add/integrate existing GIS information at no charge
- A year of MPS-ISAO cyber security services
- Upgraded server and capacity to allow for port-specific integrations
- Continuous option to integrate systems/sensors.
- Unlimited positions for port personnel
- Ability to share with outside agencies per port using custom sharing policies, as approved by the FSTED Council
- Advanced Reporting Application
- Event Planning Application for planned and emergency event management Application
- Custom List Builder Application (SOPs, checklists, contact lists, equipment lists, etc.)

The new software platform architecture must allow Florida ports to ingest and display virtually any sensor feed or system (whether internal to FSTED or with external partners) —such as AIS, cameras, LPR, radar, CAD, weather, and alarm systems—while its web-based apps allow users, security operations command center personnel, operations personnel, analysts, and others to quickly interpret information, collaborate, and make actionable recommendations, rather than merely collecting and presenting data.

This new system must be designed to drive savings for the state and its individual ports as compared to each port acquiring and maintaining their own system and integrations. The state-wide system will also provide savings for the ports that currently have existing Command Bridge implementations in terms of the cost of upgrading to a new system and their reoccurring annual maintenance. Additionally, the ports with existing

CommandBridge implementations must have the ability to reduce operation and maintenance of their own internal servers.

Finally, the new design must ensure high reliability by using a clustered server implementation as well as automatic system health monitoring with reports to provide early detection of potential problems, critical component redundancy where needed, and system wide automatic failover.