



# **How to apply for PSG on “Improving Cybersecurity Capabilities”?**

**Presented by**

**April Danos**

**Director of IT**

**Greater Lafourche Port Commission  
AAPA IT Cybersecurity Subcommittee**



# Common Cyber Language



- **AAPA Security/IT Seminar identified the need**
  - **Partly from Transportation Systems Cybersecurity Working Group (TSSWG) (which is already an approved list)**
  - **Parts are from IT/Security Committees**
  
- **Goals:**
  - **Have a common cyber language between the two departments**
  - **Push the additional language back out to TSSWG so that we have one Common Cyber Language**
  
- **Why?**
  - **Port Security Grants**
  - **Cybersecurity**



# Port Security Grants



- Physical Security Projects**
  - Boats, Fences, Cameras, Radar,**
  
- Cybersecurity:**
  - Enhancing Cybersecurity Capabilities**



# How to apply for a PSG on “Enhancing Cybersecurity Capabilities”?



- 1. Manage the grant application process for a Cybersecurity Project the same way you would a Physical Security Project.**
- 2. Get Started NOW**
- 3. NOFO – Notice of Funding Opportunity**
- 4. Develop a planning team which consist of**
  - 1. Internal :**
    - a. Grant Administrator (If you have one)**
    - b. Security Personnel**
    - c. IT Personnel and/or person Responsible for Cybersecurity at your Port**
  - 2. External:**
    - a. U. S. Coast Guard AMSC/Port Security Specialist**



## 1. Objective

- a. Maritime security risk mitigation projects that support port-resilience and recovery capabilities, as identified in an Area Maritime Security Plan or Facility Security Plan

## 2. Priorities

- a. Must address the USCG and AMSC identified vulnerabilities in port security and support the prevention, protection, response, and recovery from attacks

## 3. Projects (Cybersecurity)

- a. Propose projects that would aid in the implementation of all or part of the NIST Framework
- b. Ensure that your projects are in regards to your security network or systems that would cause a Maritime Transportation Incident and impact the safety and security of your Port.

### c. Resources :

1. DHS Critical Infrastructure Cyber Community C<sup>3</sup> Voluntary Program

[www.dhs.gov/ccubedvp](http://www.dhs.gov/ccubedvp)

2. DHS Enhanced Cybersecurity Services (ECS) program

<http://www.dhs.gov/enhanced-cybersecurity-services>





# Lessons Learned



- 1. Check with your U. S. Coast Guard Port Security Specialist to ensure that they will accept an application for items that are already being provided free by DHS.**
- 2. Ensure that your projects are in regards to your security network or systems that would cause a Maritime Transportation Incident and impact the safety and security of your Port.**
- 3. Ensure your projects are clear and to the point and can easily show the impact**
- 4. Approved but not funded**
- 5. User Roles**

# Questions?

April Danos

Director of Information Technology  
Greater Lafourche Port Commission  
Port Fourchon, LA and  
South Lafourche Leonard Miller, Jr. Airport, LA  
AAPA IT Cybersecurity Subcommittee Chair

[aprild@portfourchon.com](mailto:aprild@portfourchon.com)

[www.portfourchon.com](http://www.portfourchon.com)