THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY
INFORMATION SECURITY REQUIREMENTS

I. INTRODUCTION

This document presents the Information Security Requirements that must be met when the Port Authority of New York and New Jersey (the Authority) determines that only entities that meet the information security requirements will be eligible to receive certain documents for Contracts because bidders, and ultimately, the successful bidder require access to Port Authority Protected Information. If the Advertisement for a solicitation indicates that only entities that can satisfactorily demonstrate that they meet information security requirements can view and/or obtain the certain documents, or the entity has been notified by the Port Authority Procurement department that they must satisfactorily demonstrate that they meet information security requirements then the entity must submit documentation in accordance with this document.

II. ACCESS TO PROTECTED INFORMATION

Protected Information is information belonging to the Authority that, if it were subject to unauthorized access, modification, loss or misuse could seriously damage the Authority, public safety, or homeland security. Protecting this sensitive information requires the application of uniform safeguarding measures to prevent unauthorized disclosure and to control any authorized disclosure of this information within the Authority or when released by the Authority to outside entities. These procedures are identified in the Port Authority's "Information Security Handbook". Entities may obtain a copy of the Information Security Handbook from the Port Authority's website:

http://www.panynj.gov/business-opportunities/pdf/Corporate-Information-Security-Handbook.pdf

The Information Security Handbook requires that certain criteria be met prior to being granted access to Protected Information. Generally, an individual must be a U.S. Citizen, or be an alien who has been lawfully admitted for permanent residency or employment (indicated by immigration status), as evidenced by Immigration and Naturalization Service documentation, or be a national of the United States as defined by the Immigration and Nationality Act. This requirement may be waived in exceptional circumstances and firms seeking to be considered should refer to § 3.2 of the Information Security Handbook for details on this policy and the process for waiver. An individual may also be required to undergo background screening prior to being approved for receipt of certain information. As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Authority approved provider to be used to conduct background screening and personal identity verification, except as otherwise required by federal law and/or regulation. Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at:

http://www.secureworker.com

S.W.A.C. may be contacted directly at (877) 522-7922 for more information.

Individuals are also required to attend an Information Security Awareness and Education training session unless, within the last three (3) years, they have attended an Information Security Awareness and Education training session and have proof of same.

Meeting the information security requirements is to ensure bid documents categorized as "Protected Information," as defined in the Port Authority Information Security Handbook dated October 15, 2008, corrected as of November 14, 2013 ("Handbook"), are distributed/made available to firms that have met the applicable security requirements for access to Protected Information in accordance with the Handbook. Granting access of bid documents to a firm does not represent a determination by the Port Authority that the firm is qualified to perform the work, only that the firm has met the screening requirements for review of Protected Information.

III. SUBMITTAL INSTRUCTIONS AND CONTENT

A. Requirements

The entity shall submit required documents and present evidence that the firm has established the required information security controls, as more fully set forth in Section B below. In order to be granted access to Port Authority Protected Information. This documentation should be emailed to the Port Authority's Procurement Specialist listed in the bid/Contract documents and/or Advertisement.

B. Submission Requirements

The following items must be submitted in order to establish eligibility to receive bid documents for projects where it has been determined that certain of the bid documents contain Protected Information:

a. Name, phone number and email address of a designated representative for the entity.

b. <u>Non-Disclosure and Confidentiality Agreement</u>

Your submissions must contain the following:

(1) The Non-Disclosure and Confidentiality Agreement executed by a principal or officer of the firm on behalf of the entity;

(2) An Exhibit A- (*Acknowledgment by a Related Party Individual*) executed by the same principal who executed the entity's Non-Disclosure and Confidentiality Agreement.

(3) An Exhibit A- (*Acknowledgment by a Related Party Individual*) executed by the Security Information Manager named in paragraph (4), below.

(4) An Exhibit A- (*Acknowledgment by a Related Individual*) executed by any other member of your team, who may require access to Protected Information to assist in the preparation of your bid.

(5) An Exhibit B- (*Acknowledgment by a Related Party Entity*) executed by a principal of any subconsultant or subcontractor who may require access to Protected Information to assist in the preparation of your bid, if applicable.

(6) An Exhibit A- (*Acknowledgment by a Related Party Individual*) executed by the same principal who executed the subconsultant's/subcontractor's Exhibit B, if applicable.

(7) An Exhibit A- (*Acknowledgment by a Related Party Individual*) executed by executed by any other subconsultant/subcontractor employee, who may require access to Protected Information to assist in the preparation of your bid, if applicable.

c. Designation of Security Information Manager

Each entity seeking to be considered, who will have access to Protected Information, shall designate **at least one (1)** Security Information Manager (a "**SIM**") responsible for each firm's compliance with Information Security Requirements, identifying members of their teams who will need access to documents and for assuring that those members have passed the requisite background checks and have completed the requisite forms.

If a **joint venture** (JV) is seeking consideration, the bidding entity shall be responsible for designating **at least one (1)** SIM in order to receive the Protected Information. This SIM shall be responsible for ensuring the JVs compliance with Information Security Requirements, and ensuring that if an additional firm(s) will have access to Protected Information, such firm or firms shall designate a SIM.

The SIM will be responsible for maintaining his/her firm's access list.

With your submission, your firm (or at least one member firm of a joint venture seeking to be considered) must include the following information for your SIM(s):

(1) Full legal name
(2) Title
(3) Physical address
(4) Email address
(5) Phone number and fax number; and
(6) Proof that the SIM has been issued a SWAC Credential (see below).

Your firm's designated SIM will require a SWAC credential, proof of which must be included with your firm's submission in order to access the Protected Information. Any member of your team that requires access to Protected Information must also have a SWAC credential.

Proof of SWAC issuance shall be demonstrated by submitting a photocopy (preferably in color) of the face of the team member's SWAC card. The failure to demonstrate that, at a minimum, your firm's SIM has been issued a SWAC credential, will result in your firm not being found eligible to receive access to documents which are categorized as "Protected Information."

d. Checklist for Project Team

Your submission must include a Microsoft Excel spreadsheet providing the status of your firm's team for this project with respect to Information Security Requirements. The spreadsheet should list all persons at your firm that may require access to Port Authority Protected Information, and set forth their status as to whether they have (1) undergone Port Authority Information Security Training; (2) executed a Port Authority Non Disclosure and Confidentiality Agreement (NDA); (3) executed a Port Authority Exhibit A (4) executed an Exhibit B (if applicable); and (5) been issued a SWAC credential, if required.

Example Spreadsheet Illustration:

Name	Trained	NDA	Exhibit A (to NDA)	Exhibit B (to NDA)	SWAC
Luke Jones (Principal, C.E.O)		1/31/2013	1/31/2013		
Noah Jacobs (Estimator)	2/12/2013		1/13/2013		Yes
Melissa Manning (SIM)	1/12/2013		1/12/2013		Yes
Franklyn Benjamin, P.E. (Sub-Contractor)	2/12/2013		2/15/2013	2/15/2013	

If the entity is seeking access to information as part of a solicitation, the interested entities are encouraged to submit these items early, **at least two weeks before the Solicitation due date,** as the review process may take time, and may result in a delay to the receipt of bid documents. Information that is submitted too close to the solicitation due date (as per the solicitation documents) may not be reviewed in time for entities to respond prior to the solicitation due date.

Any questions concerning these requirements shall be directed to the Authority's Procurement Specialist listed in the applicable solicitation documents. Neither the Procurement Specialist nor any employee of the Port Authority is authorized to give additional information as to its requirements. Such interpretation or additional information will be given only by written addendum.

IV. NOTIFICATION

Notification as to whether a firm meets the Information Security Requirements will be made via email to the email address provided by the firm.