Downloaded from http://www.everyspec.com

DATA ITEM DESCRIPTION
Title: NAVAIR Cybersecurity Implementation Plan

Number: DI-MGMT-82002
AMSC Number: 9596
DTIC Applicable: No
Preparing Activity: AS
Applicable Forms: CSIP Template

Approval Date: 20151027
Limitation:
GIDEP Applicable: No
Project Number: MGMT-2015-022

Use/relationship: The Cybersecurity Implementation Plan (CSIP) will be used to ensure that industry partners are protecting government data set forth by the Cybersecurity Plan (CSP).

This Data Item Description (DID) contains the format, content, and intended use information for the data product resulting from the work task described by the contract.

Requirements:

1. Format. Contractor's format acceptable.

2. Content. The content of the CSP contains the necessary artifacts required by the DID Approval Authority (DAA), Authorizing Official (AO), or Information Systems Security Manager (ISSM) to successfully assess that industry partners are protecting Government data at the required level set forth by the CSP. The Cybersecurity Implementation Plan shall include an introduction and the following sections, and document how the contractor proposes to implement the requirements set forth in the CSP.

3. Introduction. This section shall contain a narrative of the CSIP package content.

3.1 INFORMATION ASSURANCE (Section A)

This section shall contain a description addressing how Information Assurance is related to Section A of the CSP?

Describe how your company plans on addressing Information Assurance (CS) based on Section "A" of the CSP. Address all statements in this section. The goal of this section is for the contractor to demonstrate understanding of Cyber Security/Information Assurance. Included any examples of how your company keeps up with the cyber security changing threats, industry trends, etc. Cover any general approaches to the protection of electronic information and overall awareness of threats and mitigations. This paragraph is meant to summarize the companies posture of cyber security within the business model.

3.2 ARCHITECTURE

Describe how your company plans on addressing Information Assurance based on Section "B" of the CSP. Address all statements in this section. The goal of this section is for the contractor to ensure that the contractor IT infrastructure and the Government IT infrastructure are compatible and interoperable.

Downloaded from http://www.everyspec.com

3.3 INFORMATION ASSURANCE PRACTICES

Describe how your company plans on adhering to Information Assurance practices based on Section "C" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will comply with defined IA methodologies for the continual protection of DoN information.

3.4 PUBLIC KEY INFRASTRUCTURE (PKI):

Describe how your company plans on adhering to Information Assurance practices based on Section "D" of the CSP. Address all statements in this section. The goal of this section is to articulate how PKI certificates will be acquired and utilized to meet the CSP requirements.

3.5 ELECTRONIC MAIL (E-MAIL):

Describe how your company plans on adhering to Information Assurance practices based on Section "E" of the CSP. Address all statements in this section. The goal of this section is to articulate how PKI certificates will be utilized with email programs for digital signature and encryption.

3.6 DATA AT REST

Describe how your company plans on adhering to Information Assurance practices based on Section "F" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will fulfil the CSP requirements for securing data at rest.

3.7 CERTIFICATION AND ACCREDITATION

Describe how your company plans on adhering to Information Assurance practices based on Section "G" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will appropriately support various aspects of the C&A effort. If an IT system is NOT being delivered to the Government; state that fact and mark the section "not applicable".

3.8 IA POC/IA Workforce

Describe how your company plans on adhering to Information Assurance practices based on Section "H" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will fulfill IA WorkForce requirements. If an IT system is NOT being delivered to the Government; state that fact and mark the section "not applicable".

3.9 WEB SITES, ELECTRONIC ROOMS (E-ROOMS), & COLLOBORATION TOOLS

Describe how your company plans on adhering to Information Assurance practices based on Section "I" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will appropriately fulfill CSP requirements to secure the online collaboration and management of government data.

3.10 COMMON ACCESS CARDS (CAC) & SAAR-N FORMS

Describe how your company plans on adhering to Information Assurance practices based on Section "J" of the CSP. Address all statements in this section. The goal of this section is to articulate an understanding of the process and requirements associated with obtaining a CAC and access to government systems.

3.11 CONTRACTOR OWNED UNCLASSIFIED NETWORK SECURITY

Downloaded from http://www.everyspec.com

Describe how your company plans on adhering to Information Assurance practices based on Section "K" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will protect government-controlled unclassified information while in the contractor's environment.

3.12 INFORMATION SECURITY REQUIREMENTS FOR PROTECTION OF UNCLASSIFIED DOD INFORMATION ON NON-DOD SYSTEMS

Describe how your company plans on adhering to Information Assurance practices based on Section "L" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will safeguard unclassified DoD information while stored on non-DoD information systems. Include any company specific policies and SOP's currently in place for achieving this goal.

3.13 CLASSIFIED SYSTEMS

Describe how your company plans on adhering to Information Assurance practices based on Section "M" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will meet CSP requirements when electronically transmitting classified information. If access to classified information is not a requirement in this contract state that fact and make the section "not applicable".

3.14 CLASSIFIED SPILLAGES

Describe how your company plans on adhering to Information Assurance practices based on Section "N" of the CSP. Address all statements in this section. The goal of this section is for the contractor to acknowledge the CSP requirement to appropriately report all classified spillages within the designated timeframe.

3.15 CLASSIFIED RADIOS & TEMPEST CONTROLS

Describe how your company plans on adhering to Information Assurance practices based on Section "O" of the CSP. Address all statements in this section. The goal of this section is to articulate how the contractor will comply with TEMPEST requirements. If classified radios with TEMPEST controls are NOT being delivered to the Government; state that fact and mark the section "not applicable".

3.16 PROCUREMENT OF CELLULAR TELEPHONES, PDA'S, AIR CARDS AND CALLING CARDS

Describe how your company plans on adhering to Information Assurance practices based on Section "P" of the CSP. Address all statements in this section. The goal of this section is for the contractor to acknowledge an understanding of relevant procurement instructions and restrictions for use.

3.17 MISC

Describe how your company plans on adhering to Information Assurance practices based on Section "P" of the CSP. Address all statements in this section. The goal of this section is for the contractor to acknowledge an understanding of relevant procurement instructions and restrictions for use.

End of DI-MGMT-82002