DATA ITEM DESCRIPTION
Title: CYBERSECURITY IMPLEMENTATION PLAN

Number: DI-MGMT-82002B
AMSC Number: N10222
DTIC Applicable: No
Preparing Activity: AS
Applicable Forms: CSIP Template

Approval Date: 20210218
Limitation: None
GIDEP Applicable: N/A
Project Number: MGMT-2021-004

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.

This DID supersedes DI-MGMT-82002A.

Requirements:

1. Reference Documents. None.

2. Format. Contractor's format acceptable.

3. Content. The content of the CSIP shall contain the necessary artifacts required by the Authorizing Official (AO), Functional Authorization Official (FAO), or Program Information System Security Manager (ISSM) to successfully assess that industry partners are protecting Government data at the required level set forth by the CSP.

3.1. Introduction. This section shall contain a narrative summary of the CSIP.

3.2. The content of this Cybersecurity Implementation Plan is to document how the contractor proposes to implement the requirements set forth in the Cybersecurity Plan (CSP).

3.3. Section "G" Assessment & Authorization and section "Q" Software may require additional documentation to validate the requirements set forth in the "G" and "Q" sections of the CSP per CDRL YYY, Subtitle: Cyber Security System/Software Assurance Report.

3.4. Section A.

3.4.1. CYBERSECURITY. Describe how your company plans on addressing Cyber Security (CS) based on Section "A" of the CSP. Address all statements in this section.

3.5. Section B.

3.5.1. ARCHITECTURE. Describe how your company plans on addressing Cyber Security based on Section "B" of the CSP. Address all statements in this section.

3.6. Section C.

3.6.1. CYBERSECURITY PRACTICES. Describe how your company plans on adhering to Cyber Security practices based on Section "C" of the CSP. Address all statements in this section.

3.7. Section D.

3.7.1. PUBLIC KEY INFRASTRUCTURE (PKI). Describe how your company plans on adhering to Cyber Security practices based on Section "D" of the CSP. Address all statements in this section.

3.8. Section E.

3.8.1. ELECTRONIC MAIL (E-MAIL). Describe how your company plans on adhering to Cyber Security 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.

3.9. Section F.

3.9.1. DATA AT REST. Describe how your company plans on adhering to Cyber Security practices based on Section "F" of the CSP. Address all statements in this section. List the encryption tools and the encryption methods utilized.

3.10. Section G.

3.10.1. ASSESSMENT & AUTHORIZATION (A&A). Describe how your company plans on adhering to CS practices based on Section "G" of the CSP. Address all statements in this section. If an Information Technology (IT) system that includes Platform Information Technology (PIT) systems or a system deemed as a "Control System" is NOT being delivered to the Government, state that fact and mark the section "not applicable".

3.11. Section H.

3.11.1. CYBER SECURITY (CS) POINT OF CONTACT (POC)/CYBER SECURITY WORKFORCE (CSWF). Describe how your company plans on adhering to Cyber Security

practices based on Section “H” of the CSP. Address all statements in this section. Each CSIP is required to include a CS POC.

3.12. Section I.

3.12.1. WEB SITES, ELECTRONIC ROOMS (E-ROOMS), COLLABORATION TOOLS & CLOUD SERVICES. Describe how your company plans on adhering to Cyber Security practices based on Section “I” of the CSP. Address all statements in this section. Web Sites, E-Rooms and other collaboration tools must utilize token based PKI certificates for the authentication of all users. Describe how this will be accomplished. The utilization of “Cloud Services” must contain the following information: cloud service provider, types of data being stored, sensitivity level of data being stored, off-premises connectivity, cloud service model, NIST defined cloud deployment model, security objectives level (categorization), security control baseline applied, physical location of cloud service center, personnel requirements, FEDRAMP information impact level, and any current authorizations. There should also be a network diagram and a cloud configuration diagram. Storage of CUI must utilize Impact Level (IL) 4 NSS data must utilize IL5.

3.13. Section J.

3.13.1. COMMON ACCESS CARDS (CAC) & SAAR-N FORMS. Describe how your company plans on adhering to Cyber Security practices based on Section “J” of the CSP. Address all statements in this section.

3.14. Section K.

3.14.1. CONTRACTOR OWNED UNCLASSIFIED NETWORK SECURITY. Describe how your company plans on adhering to Cyber Security practices based on Section “K” of the CSP. Address all statements in this section.

3.15. Section L.

3.15.1. INFORMATION SECURITY REQUIREMENTS FOR PROTECTION OF UNCLASSIFIED DOD INFORMATION ON NON-DOD SYSTEMS. Describe how your company plans on adhering to Cyber Security practices based on Section “L” of the CSP. Address all statements in this section. Include any company specific policies and SOP’s currently in place for achieving this goal.

3.16. Section M.

3.16.1. CLASSIFIED SYSTEMS. Describe how your company plans on adhering to Cyber Security practices based on Section “M” of the CSP. Address all statements in this section 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”.

3.17. Section N.

3.17.1. CLASSIFIED SPILLAGES & INFORMATION LEAKAGE. Describe how your company plans on adhering to Cyber Security practices based on Section “N” of the CSP. Address all statements in this section.

3.18. Section O.

3.18.1. CLASSIFIED RADIOS & TEMPEST CONTROLS. Describe how your company plans on adhering to Cyber Security practices based on Section “O” of the CSP. Address all statements in this section. If classified radios with TEMPEST controls are NOT being delivered to the Government; state that fact and mark the section “not applicable”.

3.19. Section P.

3.19.1. PROCUREMENT OF CELLULAR TELEPHONES, PDA’S, AIR CARDS AND CALLING CARDS. Describe how your company plans on adhering to Cyber Security practices based on Section “P” of the CSP. Address all statements in this section.

3.20. Section Q.

3.20.1. SOFTWARE. Describe in detail how your company plans on adhering to software deliverables based on Section “Q” of the CSP. Address all statements in this section. Ensure that each of the subsections are sufficiently explained to determine a software security posture and baseline.

3.20.1.1. Data Input Validation.

3.20.1.2. Integrity Checking.

3.20.1.3. Software Quality Assurance.

3.20.1.4. Supply Chain Management and Software Assurance.

3.21. Section R.

3.21.1. MISC. Describe how your company plans to adhere to requirements in Section “R” Misc. of the CSP.

End of DI-MGMT-82002B