DATA ITEM DESCRIPTION
Title: Contractor's Systems Security Plan and Associated Plans of Action to Implement NIST SP 800-171 on a Contractor's Internal Unclassified Information System

Number: DI-MGMT-82247
AMSC Number: 9992
DTIC Applicable: No
Preparing Activity: OSD-SO
Applicable Forms: None

Approval Date: 20181031
Limitation:
GIDEP Applicable: No
Project Number: MGMT-2018-049

Use/relationship: This Data Item Description (DID) contains the data content, format, and intended use of the Contractor's system security plan (or extracts thereof), to include any associated plans of action, addressing the Contractor's internal unclassified information system(s). When Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 is included in a contract for which covered defense information – as defined in DFARS Clause 252.204-7012 – will be processed, stored, or transmitted on an unclassified information system that is owned, or operated by or for, the Contractor, the Contractor shall develop, document, and periodically update a system security plan(s), to include any associated plans of action, for the Contractor's internal unclassified information system in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Security Requirement 3.12.4 of the NIST SP 800-171 requires that system security plans describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. Security Requirement 3.12.2 of the NIST SP 800-171 requires that plans of action describe how the Contractor will correct deficiencies and reduce or eliminate vulnerabilities in the Contractor's unclassified information system. The system security plan (or extracts thereof) and any associated plans of action may be used by the government as input to an overall risk management decision to process, store, or transmit covered defense information on an unclassified information system that is owned, or operated by or for, the Contractor (i.e., Contractor's internal unclassified information system).

This DID contains the information that shall be conveyed within the system security plan and any associated plans of actions for the Contractor's internal unclassified information system. There is no prescribed format or specified level of detail for how that information is conveyed. There is no requirement for the government to approve the system security plan or any associated plans of action for the Contractor's internal unclassified information system, but the government may request that the Contractor submit the system security plan (or extracts thereof), and any associated plans of action, such that the government may review the Contractor's implementation of security requirements.

When requested by the government, the submitted system security plan (or extracts thereof) and any associated plans of action for the Contractor's internal unclassified internal information system may:

- Demonstrate to the government the Contractor's implementation or planned implementation of the security requirements for their internal unclassified information system, or

- Be used by the government as critical inputs to an overall risk management decision to process, store, or transmit covered defense information on an unclassified information system that is owned, or operated by or for, the Contractor (i.e., Contractor's internal unclassified information system).

Requirements:

1. Reference Documents: The applicable issue of the documents cited herein, including development dates and dates of any applicable amendments, notices and revisions, shall be specified in the contract.

2. Format: Contractor's format acceptable.

3. Content: The system security plan (or extracts thereof) shall include a description of system boundaries, system environments of operation, how security requirements are implemented or how organizations plan to meet the requirements, and the relationships with or connections to other systems. Any associated plans of action shall include a description how the Contractor will correct deficiencies and reduce or eliminate vulnerabilities in the Contractor's information system.

3.1. Cover Page: The cover page of the system security plan (or extracts thereof) and any associated plans of action shall identify the following information:

3.1.1. Title of the document (i.e., Systems Security Plan and Associated Plans of Action for [Name of Contractor's Internal Unclassified Information System])

3.1.2. Company name

3.1.3. Data Universal Numbering Systems (DUNS) Number

3.1.4. Contract number(s) or other type of agreement

3.1.5. Facility Commercial and Government Entity (CAGE) code(s)

3.1.6. System that this System Security Plan and any associated Plans of Action addresses

3.1.7. Date of latest revision

3.1.8. All appropriate distribution and classification statements/markings

3.2. System Identification: The purpose of the system security plan shall be communicated in this section, to include a description of the function/purpose of the Contractor's internal unclassified information system(s)/network(s) that is(are) addressed in the plan.

3.3. System Environment: A detailed topology narrative and graphic shall be included that clearly depicts the Contractor's internal unclassified information system boundaries, system interconnections, and key components. This does not require depicting every device, but would

include an instance of operating systems in use, virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations, firewalls, routers, switches, copiers, printers, lab equipment, etc. If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. Include or reference (e.g., to an inventory database or spreadsheet) a complete hardware and software inventory, including make/model/version and maintenance responsibility.

3.4. Security Requirements: Describe how the Contractor addresses/will address security requirements in each of the following NIST SP 800-171 security requirement families (including basic and derived requirements) for protecting covered defense information in the Contractor's systems and organizations:

3.4.1. Access Control (3.1.1 – 3.1.x)

3.4.2. Awareness and Training (3.2.1 – 3.2.x)

3.4.3. Audit and Accountability (3.3.1 – 3.3.x)

3.4.4. Configuration Management (3.4.1 – 3.4.x)

3.4.5. Identification and Authentication (3.5.1 – 3.5.x)

3.4.6. Incident Response (3.6.1 – 3.6.x)

3.4.7. Maintenance (3.7.1 – 3.7.x)

3.4.8. Media Protection (3.8.1 – 3.8.x)

3.4.9. Personnel Security (3.9.1 – 3.9.x)

3.4.10. Physical Protection (3.10.1 – 3.10.x)

3.4.11. Risk Assessment (3.11.1 – 3.11.x)

3.4.12. Security Assessment (3.12.1 – 3.12.x)

3.4.13. System and Communications Protection (3.13.1 – 3.13.x)

3.4.14. System and Information Integrity (3.14.1 – 3.14.x)

3.5. Plans of Action: In accordance with Security Requirement 3.12.2, provide any plans of action developed to address how and when the Contractor will implement any security requirements not yet implemented, identify known deficiencies and vulnerabilities in the contractor's internal unclassified information system, how and when the Contractor will correct identified deficiencies and reduce or eliminate vulnerabilities in the Contractor's system.

End of DI-MGMT-82247