November 6, 2018

GUIDANCE FOR ASSESSING COMPLIANCE OF AND ENHANCING PROTECTIONS FOR A CONTRACTOR'S INTERNAL UNCLASSIFIED INFORMATION SYSYEM

(REQUIRES NEGOTIATION OF TERMS/COSTS ON A CONTRACT-BY-CONTRACT BASIS)

	OBJECTIVE	SOLICITATION	SOURCE SELECTION	CONTRACT
Pre-Award (Solicitation and Source Selection)				
1	Contractor 'self-attests' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171 (Status Quo with DFARS 252.204-7008)	Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012		Section I: • DFARS Clause 252.204-7012
2	Require enhanced cybersecurity measures in addition to the security requirements in NIST SP 800-171 to safeguard information stored on the contractor's internal unclassified information system	Section C: • Include Statement of Work referencing DoD approved list of enhanced security requirements Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012 Section L: • Describe contractor implementation of additional requirements Section M: • Detail specifics of how additional requirements will be evaluated	Evaluate offeror's proposed implementation of protections required in addition to NIST SP 800-171 in accordance with the specifics of how additional requirements will be evaluated as documented in Section M	Section C: • Include Statement of Work referencing a DoD approved list of enhanced security requirements Section I: • DFARS Clause 252.204-7012

	OBJECTIVE	SOLICITATION	SOURCE SELECTION	CONTRACT
Pre-Award (Solicitation and Source Selection)				
3	Establish measures (as identified below) to assess/affirm contractor compliance with cybersecurity requirements	Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012		Section I: • DFARS Clause 252.204-7012
3a	Establish 'Go/No Go' evaluation criteria/ threshold based on implementation status of NIST SP 800-171 at time of award	Section L: • Require delivery of the contractor's system security plan (or extracts thereof) (NIST SP 800-171 Security Requirement 3.12.4), and any associated plans of action (NIST SP 800-171 Security Requirement 3.12.2)* with the contractor's technical proposal Section M: • Identify requirements for an "Acceptable" (Go/No Go threshold) rating	Evaluate contractor's system security plan (NIST SP 800-171 Security Requirement 3.12.4) (or specified elements of) and any associated plans of action (NIST SP 800-171 Security Requirement 3.12.2)* in accordance with requirements for an "Acceptable" (Go/No Go threshold) rating identified in Section M	
3b	Establish compliance with NIST SP 800-171 implementation as a separate technical evaluation factor	Section L: • Require delivery of the contractor's system security plan (or extracts thereof) (NIST SP 800-171 Security Requirement 3.12.4), and any associated plans of action (NIST SP 800-171 Security Requirement 3.12.2)* with the contractor's technical proposal Section M: • Detail how evaluation of compliance of NIST SP 800-171 will be conducted	Evaluate compliance with NIST SP 800-171 in accordance with Section M	

	OBJECTIVE	SOLICITATION	SOURCE SELECTION	CONTRACT
Pre-Award (Solicitation and Source Selection)				
3c	Conduct on-site government assessment of contractor's internal unclassified information system in accordance with NIST SP 800-171A	Section L: • Require Offerors to support/provide access for on-site government assessment Section M: • Technical evaluation criteria for on-site government assessment in accordance with NIST SP 800-171A	Conduct on-site government assessment of each Offeror's internal unclassified information system in accordance with Section M and NIST SP 800-171A	
3d	Contractor to identify known Tier 1 Level Suppliers and request contractor's plan to: i) track flow down of covered defense information, and ii) assess compliance of known Tier 1 Level Suppliers	Section L: • Require Offeror's to provide their plan to: i) track flow down of covered defense information, and ii) assess compliance of Tier 1 Level Suppliers Section M: • Identify how evaluation on contractor's plan will be conducted	Evaluate Offeror's plan to: i) track flow down of covered defense information, and ii) assess compliance of Tier 1 Level Suppliers with Section M	
Post-Award				
3e	Take delivery of the Contractor's system security plan (or extracts thereof) and associated plans of action to assess/track implementation of NIST SP 800-171 security requirements and use to assess compliance.	Section C: • Include SOW referencing delivery of system security plan(or extracts thereof)/plans of action in order to assess/track implementation of NIST SP 800-171 security requirements Section J: • Include CDRL (TAB 1), referencing DID for system security plan/plans of action (TAB 2), requiring delivery of system security plan/plans of action*		Section C: • Include SOW re: delivery/tracking of system security plan (or extracts thereof)/plans of action Section J: • Include CDRL (TAB 1), referencing DID for system security plan/plans of action (TAB 2), requiring delivery of system security plan/plans of action • Incorporate system security plan (or extracts thereof)/plans of action as part of the contract

	OBJECTIVE	SOLICITATION	SOURCE SELECTION	CONTRACT
Post-Award				
3f	Conduct on-site government assessment of the contractor's internal unclassified information system in accordance with NIST SP 800-171A to assess/ monitor compliance of NIST SP 800-171	Section C: • Include Statement of Work requiring the contractor to support independent government assessment of compliance of NIST SP 800-171 in accordance with NIST SP 800-171A		Section C: • Include Statement of Work requiring the contractor to support independent on-site government assessment of compliance of NIST SP 800-171 in accordance with NIST SP 800-171A
4	Identify DoD controlled unclassified information requiring protection in accordance with DFARS Clause 252.204-7012 and NIST SP 800-171	Section C: • Include Statement of Work referencing information requiring protection Section I: • DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012 Section J: • Include CDRL (TAB 3), referencing DID (TAB 4), addressing requirement to identify information requiring protection		Section C: • Statement of Work referencing information requiring protection Section I: • DFARS Clause 252.204-7012 Section J: • Include CDRL (TAB 3), referencing DID (TAB 4), addressing requirement to identify information requiring protection
***** System security plans and plans of action should be handled in a manner that affords a level of security commensurate with content that describes contractor system vulnerabilities, including pending actions to implement NIST 800-171 security controls.				

REFERENCES/RESOURCES/TABs
DFARS Provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls — Requires that the Offeror represent that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting — Requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. To provide adequate security, the contractor must, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" — Provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.
Documenting Implementation of NIST SP 800-171 — Companies should have a **system security plan** in place, in addition to any associated **plans of action** to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate system vulnerabilities • **NIST SP 800-171 Security Requirement 3.12.4 (System Security Plan)** — Requires contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems • **NIST SP 800-171 Security Requirement 3.12.2 (Plans of Action)** — Requires contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems Note: When 'adequate security' requires security measures in addition to the NIST SP 800-171 security requirements (determined as necessary by the contractor), these additional measures will be evaluated and monitored in a manner similar to the NIST SP 800-171 requirements. Plans of action, continuous monitoring and the system security plan (NIST SP 800-171 Security Requirements 312.2-3.12.4) must address all security requirements.

REFERENCES/RESOURCES (continued)
NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information – • Provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171 • Intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in NIST SP 800-171
TAB 1 – CDRL – Request Contractor's System Security Plan and Any Associated Plans of Action for Contractor's Internal Information System
TAB 2 – DID – Contractor's System Security Plan and Any Associated Plans of Action for Contractor's Internal Information System
TAB 3 – CDRL – Request Contractor's Record of Tier 1 Level Suppliers who Receive or Develop Covered Defense Information
TAB 4 – DID - Contractor's Record of Tier 1 Level Suppliers who Receive or Develop Covered Defense Information (Draft)

TAB 1

CONTRACT DATA REQUIREMENTS LIST (CDRL)

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed form to the government Issuing Contracting Officer for the Contract/PR No. in Block E.

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
TBD	TBD	TDP ____ TM _____ OTHER_X_

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
xyz	xyz	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
TBD	System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System	N/A

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-MGMT-XXXXX	SOW/PWS PARA x.y.z	PMS xyz Critical Program

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	E	See Block 16	See Block 16

8. APP CODE	11. AS OF DATE	13. DATE IF SUBSEQUENT SUBM.
NA	N/A	See Block 16

14. DISTRIBUTION	b. COPIES		
a. ADDRESSEE	draft	final reg	final repr
COR	0	1	
15. TOTAL - - - - - - - - ->	1	1	0

16. REMARKS

Block 4: Hardcopy or Electronic submission is permissible if sent with encryption.

Block 7: Letter of Transmittal only

Block 9: Distribution Statement E: Distribution authorized to the Department of Defense only; Proprietary Information; dd mm yyyy. Other requests for this document shall be referred to PMS xyz.

Blocks 10, 11, 12, 13: Initial, and all subsequent annual submissions, of SSP and Plans of Action (or appropriate extracts thereof) are submitted **upon request**.

Block 12: SSP and Plans of Action (or appropriate extracts thereof) submissions, initial and subsequent, are submitted upon request. Requests will indicate what specific information is required (e.g., list of requirements not yet met and associated plans of action; description of how all requirements are met and associated plans of action)

Block 14: Notification of delivery shall be made to John Doe, COR. Further distribution will be authorized by the Program Manager.

Program Management Office, xyz Critical
Program Directorate
Attn: John Doe, PMS xyz Contract
COR/Deliverables
1234 Dissemination Road
Bldg 567 3rd Floor
Marking, ST 54321-5000

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
John Doe	07 DEC 19	Hilda Fawn	07 DEC 19

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 **Approval Date: 20181031**
AMSC Number: 9992 **Limitation:**
DTIC Applicable: No **GIDEP Applicable: No**
Preparing Activity: OSD-SO **Project Number: MGMT-2018-049**
Applicable Forms: None

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

TAB 3

CONTRACT DATA REQUIREMENTS LIST (CDRL)

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed form to the government Issuing Contracting Officer for the Contract/PR No. in Block E.

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
TBD	TBD	TDP ____ TM _____ OTHER_X_

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
xyz	xyz	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
TBD	Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information	N/A

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-MGMT-XXXXX	SOW/PWS PARA x.y.z	PMS xyz Critical Program

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	E	See Block 16	See Block 16

8. APP CODE	11. AS OF DATE	13. DATE IF SUBSEQUENT SUBM.
NA	N/A	See Block 16

16. REMARKS

Block 4: Hardcopy or Electronic submission is permissible if sent with encryption.

Block 7: Letter of Transmittal only

Block 9: Distribution Statement E: Distribution authorized to the Department of Defense only; Proprietary Information; dd mm yyyy. Other requests for this document shall be referred to PMS xyz.

Blocks 10, 12, 13: Initial shall be delivered 30 days after Post Award Conference, all subsequent submissions, shall be submitted **in accordance with IMS.**

Block 14: Notification of delivery shall be made to John Doe, COR. Further distribution will be authorized by the Program Manager. IF deliverable contains classified data, contract COR for direction on delivery

Program Management Office, xyz Critical
Program Directorate
Attn: John Doe, PMS xyz Contract
COR/Deliverables
1234 Dissemination Road
Bldg 567 3rd Floor
Marking, ST 54321-5000

14. DISTRIBUTION	b. COPIES		
a. ADDRESSEE	draft	reg	final repr
COR	0	1	
DCMA	0	1	
DSS	0	1	
15. TOTAL - - - - - - - - ->	1	1	0

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
John Doe	07 DEC 19	Jane Fawn	07 DEC 19

DATA ITEM DESCRIPTION

Title: Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information

Number: DI-MGMT-XXXXX
AMSC Number: YYYY
DTIC Applicable: No
Preparing Activity: TBD
Applicable Forms: None

Approval Date: TBD
Limitation: TBD
GIDEP Applicable: No
Project Number: MGMT-2018-XXX

Use/relationship: When 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 a tier 1 level supplier's internal unclassified information system.

This Data Item Description (DID) contains the information that is required of the Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information. This information will 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). There is no prescribed format or specified level of detail for this information which will:

- Demonstrate to the government the Contractor's ability to restrict the flow down of covered defense information specified in, or developed under, the contract on a 'need to know' basis to execute the requirements.
- Demonstrate to the government the Contractor's ability to ensure that their tier 1 level suppliers safeguard covered defense information in accordance with, at a minimum, DFARS Clause 252.204-7012.
-

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.

   2.1. Content: The Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information must include a description of how the Contractor will identify and restrict the flow down or creation of covered defense information on a 'need to know' basis and how the Contractor will ensure that their tier 1 level suppliers safeguard covered defense information with, at a minimum, the requirements of DFARS Clause 252.204-7012.

   2.2. Cover Page: The cover page of the Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information shall include:

- Title of the document (i.e., [Name of Contractor] Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information
- Contractor's Data Universal Numbering Systems (DUNS) and Commercial and Government Entity Code (CAGE) Numbers
- Contract number(s) or other type of agreement (if available)

2.3. Tier 1 Level Supplier Information (for each Tier 1 Level Supplier receiving/developing covered defense information associated with this contract)

- Supplier Name
- Supplier contract/agreement number (if available)
- Supplier Point of Contact: name, email, and phone number
- Supplier contract/agreement contains or will contain substance of DFARS Clause 252.204-7012 Clause: Y/N
- Supplier agreement/contract contains or will contain cyber security measures/requirements other than those identified in DFARS Clause 252.204-7012 and NIST SP 800-171: Y/N
- Contractor's Data Universal Numbering Systems (DUNS) and Commercial and Government Entity Code (CAGE) Numbers:
- Supplier has conducted or will conduct a self-assessment in accordance with NIST SP 800-171A:Y/N
- Supplier System Security Plan and Associated Plans of Action in accordance with NIST SP 800-171 Rev 1 Security Requirement 3.12.4 and 3.12.2.
- List of Supplier's Tier 1 Level Suppliers receiving and/or developing covered defense information

End of DI-MGMT-XXXXX