CLASSIFICATION *(When filled in)*: Unclassified

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires: October 31, 2020

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*: Top Secret

b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY: Top Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable.)*

- ☐ **a. PRIME CONTRACT NUMBER** *(See instructions.)*
- ☐ **b. SUBCONTRACT NUMBER**
- ☒ **c. SOLICITATION OR OTHER NUMBER** TBD — **DUE DATE** *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable.)*

- ☒ **a. ORIGINAL** *(Complete date in all cases.)* — **DATE** *(YYYYMMDD)*
- ☐ **b. REVISED** *(Supersedes all previous specifications.)* — **REVISION NO.** — **DATE** *(YYYYMMDD)*
- ☐ **c. FINAL** *(Complete Item 5 in all cases.)* — **DATE** *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☒ No ☐ Yes *If yes, complete the following:*

Classified material received or generated under _____ *(Preceding Contract Number)* **is transferred to this follow-on contract.**

5. IS THIS A FINAL DD FORM 254? ☒ No ☐ Yes *If yes, complete the following:*

In response to the contractor's request dated _____ **, retention of the classified material is authorized for the period of:** _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
TBD	TBD	TBD

7. SUBCONTRACTOR(S) *(Click button if you choose to add or list the subcontractors -- but will still require a separate DD Form 254 issued by a prime contractor to each subcontractor)*

Add Row | Remove last Row | Delete All Rows

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
The Prime Contractor will follow NISPOM requirements for issuance of a DD 254 to their sub-contractor. All subcontracting is only done with the express approval of the Government Contracting Activity (GCA) in coordination with the Government Program Manager.	TBD	N/A

8. ACTUAL PERFORMANCE *(Click button to add more locations.)*

Add Row | Remove last Row | Delete All Rows

a. LOCATION(S) *(For actual performance, see instructions.)*	b. CAGE CODE *(If applicable, see Instructions.)*	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
See Item 6a. Additional locations may include other cleared contractor facilities; and government facilities; CONUS/OCONUS as identified by the Government Contracting Activity (GCA) in coordination with the Government Program Manager.	TBD	TBD

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

The JEDI Cloud program will provide enterprise-level, commercial cloud services as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) to the U.S. Department of Defense and related mission partners.

(Note: For this effort the Contracting Officer (CO) or the term Government Contracting Activity (GCA) is Washington Headquarters Services (WHS) Acquisition Directorate (AD). The term Government Program Manager for this effort is The Defense Digital Service (DDS) and DoD Chief Information Officer (CIO) program office. The Contracting Officer Representative or Contracting Officer Technical Representative (COTR) as it applies to this effort is the component leveraging the cloud service or who purchase classified cloud services.)

10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- [X] a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION
- [X] b. RESTRICTED DATA
- [X] c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) *(If CNWDI applies, RESTRICTED DATA must also be marked.)*
- [X] d. FORMERLY RESTRICTED DATA
- e. NATIONAL INTELLIGENCE INFORMATION:
  - [X] (1) Sensitive Compartmented Information (SCI)
  - [X] (2) Non-SCI
- [X] f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION
- [X] g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION
- [X] h. FOREIGN GOVERMENT INFORMATION
- [X] i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION
- [X] j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) *(See instructions.)*
- [X] k. OTHER (Specify) *(See instructions.)*

See item 13 Continuation Pages

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: *(X all that apply. See instructions. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- [ ] a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY *(Applicable only if there is no access or storage required at contractor facility. See instructions.)*
- [ ] b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY
- [X] c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL
- [X] d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE
- [ ] e. PERFORM SERVICES ONLY
- [ ] f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S.,PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES
- [X] g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER
- [X] h. REQUIRE A COMSEC ACCOUNT
- [X] i. HAVE A TEMPEST REQUIREMENT
- [X] j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
- [X] k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE
- [X] l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI). *(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)*
- [X] m. OTHER (Specify) *(See instructions.)*

See Item 13 Continuation Pages

12. PUBLIC RELEASE

Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified here with at least office and phone contact information and if available, an e-mail address. *(See instructions)*

- [ ] DIRECT
- [X] THROUGH *(Specify below)*

Defense Office of Prepublication and Security Review (DOPSR)
1155 Defense Pentagon Washington, DC 20301

Public Release Authority:

See Item 13 Continuation Pages

13. SECURITY GUIDANCE

Add Signature | Remove last Signature | Delete All Signatures

The security classification guidance for classified information needed for this effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended.
(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. The field will expand as text is added. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. Also allows for up to 6 internal reviewers to digitally sign. See instructions for additional guidance or use of the fillable PDF.)

ITEM 10. CONTRACTOR WILL REQUIRE ACCESS TO:
With approval of the GCA, in coordination with the GPM, the contractor will require access to multiple types of information/equipment specified below (Items 10a through 10k) and Statement of Work. The contractor will comply with laws, rules, regulations designed to protect the information, and report known or suspected failures to safeguard information to the GPM and appropriate security office. The contractor will ensure all training requirements and access approvals are completed, prior to actual access. All information, classified materials and government furnished equipment will be returned to the Government upon conclusion of the contract or when no longer needed for performance, whichever occurs first.

ITEM 10a. COMSEC INFORMATION
COMSEC information includes accountable or non-accountable COMSEC information; controlled cryptographic items (CCI); COMSEC Material Control System (CMCS). The GPM will determine if the contractor requires a COMSEC account or if COMSEC materials will be provided on loan from a Government COMSEC account holder. (See comments for item 11.h)

Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the GCA. Non-accountable COMSEC information may still require a level of control within a document control system. Refer to NSA/CSS Manual 3-16, "Control of Communications Security Material," and the Committee on National Security Systems Instruction (CNSSI) 4001, "Controlled Cryptographic Items," for guidance.

ITEM 10b. RESTRICTED DATA
Access to Restricted data requires a final U.S. Government clearance at the appropriate level. Once a final clearance is in place, the contractor will coordinate with the Defense Security Service's Personnel Security Management Office for Industry to facilitate any reciprocity requirements for individual "Q" or "L" clearances, if required, with the Department of Energy for any of the contractor personnel.

ITEM 10c. CNWDI
GCA approval is required prior to granting CNWDI access to a subcontractor. Special briefings and procedures are required. Access to CNWDI requires a final U.S. Government clearance at the appropriate level. Briefing certificates for access must be given to the appropriate Government Security Office.

ITEM 10d FORMERLY RESTRICTED DATA
Access to Formerly Restricted Data requires adjudication by the appropriate Government Security Office.

ITEM 10e(1) SCI
The Director of National Intelligence (DNI) has jurisdiction and control over National Intelligence Information. The need for access to specific categories of SCI will be determined by the GPM and WHS Security Office. The GPM will provide additional security requirements outlined in applicable DNI and DCI Directives.

An accredited Sensitive Compartmented Information Facility (SCIF) is required to store and/or process SCI. The contractor will comply with DNI and DCI Directives for construction, accreditation, and operation of a SCIF.

ITEM 10e(2) NON-SCI
The GCA and appropriate GPM will determine if the contractor requires access to non-SCI information. The contractor will comply with laws, rules, and regulations to safeguard the information.

ITEM 10f. SAP INFORMATION
SAPs impose requirements that exceed the NISPOM. The applicable Government SAP office will provide the contractor with the additional security requirements needed to supplement the NISPOM (DoD 5220.22-M) requirements and ensure adequate protection of the SAP information involved. Approval from the GCA and SAP office is required prior to subcontracting.

ITEM 10g. NATO INFORMATION
The GCA and appropriate GPM will identify the specific levels of NATO, required for access. Access to NATO information requires a final U.S. Government clearance at the appropriate level and a NATO access briefing/debriefing. Special briefings are required for access to NATO. Briefing certificates must be provided to the appropriate Government Security Office. GCA approval is required prior to subcontracting.

If the GCA and appropriate GPM determine the contractor does not require access to or knowledge of NATO information, but does require access to SIPRNET, the contractor must complete the required NATO awareness briefing.

ITEM 10h. FOREIGN GOVERNMENT INFORMATION (FGI)
Prior approval of the GCA and GPM is required prior to subcontracting. FGI is information provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information or both, are to be held in confidence, or produced by the U.S. pursuant to, or as a results of, a joint arrangement with a foreign entity government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence. Access to classified FGI requires a final U.S. Government clearance at the appropriate level.

Item 10i. ACCM INFORMATION
The GCA and appropriate GPM will provide appropriate classification guidance. See DoDM 5200.2, Volume 3, "DoD Information Security Program: Protection of Classified Information," available at: http://www.esd.whs.mil/DD/

ITEM 10j CUI
The contractor will have access to CUI which is not classified information, but does require protection from unauthorized disclosure. The

contractor must comply with all requirements to safeguard CUI. Refer to DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI), available at: http://www.esd.whs.mil/DD/

The contractor will likely have access to or knowledge of Personally Identifiable Information (PII) and/or Protected Health Information (PHI), both a type of CUI. The contractor must ensure PII and PHI are protected as required by the Privacy Act and associated laws, rules, and regulations. The contractor must complete Privacy Act training before access.

ITEM 10k. OTHER

The contractor will comply with government security requirements specific to authorized locations of performance. Personnel security clearances along with additional accesses (e.g. NATO), must be annotated in the DoD personnel security system of record (e.g. JPAS).

DOD COMPUTER SECURITY
The contractor must meet all requirements in the GPM-approved Cyber Security Plan. The contractor will have access to government provided unclassified information systems. With the approval from the GCA, GPM and the applicable COR/COTR will assess and authorize the contractor to have access to classified information systems (e.g., SIPRNET, JWICS). The contractor must meet all requirements before accessing a particular information system. Information systems must be used only for the official government purpose specified in this contract. Government furnished equipment must be returned when no longer required for performance on this contract.

ITEM 11 IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:
With GCA and GPM approval or direction, the contractor will be required to conduct specific actions, allowed to use the services described below, or prohibited from specific actions (Items 11a through 11m). The contractor will comply with laws, rules, and regulations specific to each situation.

ITEM 11c / ITEM 11d.: Classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Classified information and materials shall be protected in accordance with established policies and procedures. Specific classification guidance will be provided on individual tasks by the GCA, GPM and CORs / COTRs as needed to support classified cloud services. In any case where classification guidance has not been provided, the contractor is to safeguard the information and seek written guidance from the GCA and GPM prior to release of the information. Upon completion /termination of this contract the U.S. Government will be contacted for the disposition of or distribution of classified materials.

- Contractors must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need-to-know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the GCA, GPM and appropriate approving official. The designated custodian shall comply with NISPOM requirements for receipt or accounting of classified material received under this contract.
- Upon completion / termination of the classified contract the contractor will return all classified information. Within 30 days after the final product is received and accepted by the procuring agency, all classified materials released to the contractor, must be returned to the originating agency. (Note: All materials belonging to the Component, who purchased the classified cloud services, will be return to them on termination of this effort.) Requests to retain materials shall be directed to the GCA and GPM in writing with a full justification for retention identified.

Contractor is authorized to process and store up to and incoming (Top Secret, Secret) information and hardware at contract facility listed in 6a. Actual knowledge and production of classified information is required for performance of this contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded. The contractor is not authorized to release classified information to any activity or person, including sub-contractors, without the government GCA's written approval. Only with the expressed permission of the GCA and GPM may the contractor reproduce any classified information / materials. All requirements for control and accounting for original documentation and copies apply.

ITEM 11g. USE OF DTIC
With GCA and appropriate GPM approval and certification of need-to-know to DTIC, the contractor may register with DTIC.

ITEM 11h. REQUIRE A COMSEC ACCOUNT
Refer to Item 10 and 10a.

ITEM 11i. TEMPEST REQUIREMENT
If the Government determines the contractor must have specific information systems, TEMPEST may be required. TEMPEST is an unclassified term referring to investigation and study of compromising emanations. If TEMPEST is required, the GCA and appropriate GPM will identify in writing any TEMPEST requirements. The contractor may not impose TEMPEST requirements on a subcontractor without GCA approval.

ITEM 11j. OPSEC REQUIREMENTS
The GCA and appropriate GPM will identify and provide additional protection or countermeasures to safeguard the operations associated with the program or function (as identified by specific program needs). If required, these OPSEC measures are outside of NISPOM requirements. The contractor will be provided with a copy of the system, command or OPSEC plan that supports the identification of critical information. The contractor may not impose OPSEC requirements on a subcontractor unless the GCA approves the OPSEC requirements.

ITEM 11k. USE OF DEFENSE COURIER SERVICE
Only certain classified materials qualify for movement by USTRANSCOM's Defense Couriers. The GCA is responsible for complying with both DoD and the USTRANSCOM's Defense Courier Division (TCJ3-C), Scott AFB, IL policy and procedures related to Defense Courier operations. TCJ3-C must provide written approval to a GCA to use Defense Courier Services. Prior GCA approval is required before a Prime Contractor can authorize a subcontractor to use the services or USTRANSCOM's Defense Couriers.

ITEM 11l. RECEIVE, STORE, GENERATE CUI
Refer to Item 10j.

ITEM 11m. OTHER

IN/OUT PROCESSING
The contractor must complete in-processing upon entry to the contract and out-processing prior to departing from this contract. All government property and information must be returned at or before out-processing.

COMMON ACCESS CARD (CAC)
If required by GPM, A CAC will be issued as required for access to facilities and/or information systems. Personnel must meet and maintain investigative and adjudicative requirements specified in DoDI 5200.46, and immediately report to the WHS Security Office any issues affecting eligibility to possess a CAC. Government issued credentials are the property of the United States Government and must be returned when no longer required for performance on this contract. Return CACs to: WHS Security Office,
4800 Mark Center Drive, Suite 03F09-02, Alexandria, VA 22350.

DESTRUCTION OF INFORMATION
Information not already formally approved for public release must be destroyed using approved methods.

PHOTOGRAPHY/RECORDING
The recording of DoD information, equipment, personnel, and facilities by any means is prohibited.

ITEM 12 PUBLIC RELEASE
Release of DoD information to the public or other unauthorized recipient is prohibited. All DoD information intended for publication or dissemination must undergo a security and policy pre-publication review. This material includes, but is not limited to: books, manuscripts and theses, biographies, articles, book reviews, audio/video materials, speeches, press releases, conference briefings, research papers, gaming materials and other media. The Government must initiate the release process and the proposed information must be reviewed by the WHS Security Office. Unauthorized releases must be reported to the WHS Security Office.

SECURITY INCIDENTS
Security incidents must reported in accordance with the NISPOM and Cyber Security Plan.

*OCMO Security Office: Please refer all related security questions or concerns to the whs.pentagon.em.mbx.security-officers@mail.mil, or 571-372-3170.

List of Attachments (All Files Must be Attached Prior to Signing, i.e., for any digital signature on the form)

Add Attachment | View Selected Attachment | Remove Selected Attachment

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE

14. ADDITIONAL SECURITY REQUIREMENTS

Requirements, in addition to NISPOM requirements for classified information, are established for this contract.

☐ No ☒ Yes *If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the CSO. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

Release of SCI / Non SCI materials is only authorized for US Contractors. Access to intelligence information requires special briefings and a US Government clearance at the appropriate TS/SCI. Prior approval from the GCA is required before the contractor can impose additional security requirements on a subcontractor. Specific categories of intelligence information will be identified if appropriate.
SAP requirements will be provided if appropriate.
OPSEC requirements beyond the NISPOM will be provided if appropriate

15. INSPECTIONS

Elements of this contract are outside the inspection responsibility of the CSO.

☐ No ☒ Yes *If Yes, explain and identify specific areas and government activity responsible for inspections. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

Defense Intelligence Agency (DIA) has security cognizance over an accredited SCIFs and systems containing intelligence information. Special Security Office (SSO) DIA has exclusive security responsibility for all SCI classified material release to or developed under this contract. DSS is relieved of security inspection responsibility for all such materials. DIA is responsible for reviewing the contractor SCIF documentation to ensure compliance with SCIF regulations DSS retains oversight responsibility for collateral information.

16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
Washington Headquarters Services (WHS)	WHS Acquisition Directorate 4800 Mark Center Drive, Suite 09F09-02 Alexandria, VA 22350	TBD
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)*
HQ0034		**f. EMAIL ADDRESS** *(See Instructions)*

17. CERTIFICATION AND SIGNATURES

Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below. Upon digitally signing Item 17h, no changes can be made as the form will be locked.

a. TYPED NAME OF CERTIFYING OFFICIAL *(Last, First, Middle Initial)* *(See Instructions)*	d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*	h. SIGNATURE
Forshey, Chris M.		
b. TITLE	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	
c. ADDRESS *(Include ZIP Code)*	**f. TELEPHONE** *(Include Area Code)*	**i. DATE SIGNED** *(See Instructions)*
WHS Security Office 4800 Mark Center Drive, Suite 03F09-02 Alexandria, VA 22350	+1 (571) 372-3170	
	g. EMAIL ADDRESS *(See Instructions)*	
	chris.m.forshey.civ@mail.mil	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

☒ a. CONTRACTOR

☐ b. SUBCONTRACTOR

☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION

☒ e. ADMINISTRATIVE CONTRACTING OFFICER

☐ f. OTHER AS NECESSARY *(If more room is needed, continue in Item 13 or on additional page if necessary.)*