CYBERSECIRITY AND INFRASTRUCTURE SECURITY AGENCY
OFFICE OF THE CHIEF HUMAN CAPITAL OFFICER
STATEMENT OF WORK (SOW)
FOR
CLOUD-BASED VIDEO INTERVIEWING SOLUTION SERVICES

1.0 GENERAL

1.1 BACKGROUND

The Cybersecurity and Infrastructure Security Agency's (CISA) mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA includes the CISA Mission Enabling Offices (MEOs) and six Divisions that include the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Integrated Operations Division (IOD), Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered with the National Capital Region (NCR).

The CISA Office of the Chief Human Capital Officer (OCHCO) mission is to serve as a strategic partner with the MEOs and Divisions by providing high-quality human resources advice, services and solutions to support leadership, employees, and the missions, reaming steadfast in a commitment to provide outstanding customer service across all human capital areas. As part of that recruitment for top talent remains a top priority for the CISA Director and Chief Human Capital Officer. In conjunction with that commitment, CISA must also innovate and modernize its approach to assess job candidates using competency-based assessments to scale back on the reliance upon educational qualifications as a substitute for competencies in the Federal hiring process, which is a requirement outlined in Executive Order (EO) 13932 published June 2020. As such, CISA seeks the continual use of the HireVue cloud video interviewing solution for hiring support services.

1.2 SCOPE

The contractor shall continue to provide access to the HireVue system with the following minimum functional capabilities:

- Shall provide cloud video interviewing solution for up to 250 hires.
- Interview Questions (video, voice, and/or type interface options)
- Game-based Skills Assessment – CodeVue Games/Challenges and Logic Games
- Training – Training classes for Hiring Manages/HR Users. Monthly, also, online training.
- Single, dedicated account manager
- Technical support team available between the hours of 8:00 am to 5:00 pm EST
- Reporting capabilities

- Privacy Act Statement to appear for all candidates in each instance of an assessment
- Reasonable Accommodations Statement to appear for all candidates in each instance of an assessment

1.3 OBJECTIVE

Obtain services that operates via cloud video interviewing solution and assessment tool.

2.0 REQUIREMENTS

2.1 Continuous Monitoring

The vendor will continue to provide all support, artifacts, documentation and technical assistance to the CISA Information System Security Officer required to maintain an ATO for the HireVue system in accordance with Federal, DHS and NIST laws, regulations and guidelines, including but not limited to, all applicable and current revisions of Homeland Security Presidential Directives, Binding Operational Directives (BODs), DHS 4300A Sensitive Systems Policy & Sensitive Systems Handbook, and the of NIST Special Publication 800-53.

Electronic Delivery

Contractor shall deliver all items to CISA OCHCO. The Policy and Accountability, Associate Chief shall identify the end users.

2.2 System Implementation

The contractor shall continue to provide access to the HireVue system with the following minimum functional capabilities:

- Shall provide cloud video interviewing solution for up to 250 hires.
- Interview Questions (video, voice, and/or type interface options)
- Game-based Skills Assessment – CodeVue Games/Challenges and Logic Games
- Training
- Single, dedicated account manager
- Technical support team available between the hours of 8:00 am to 5:00 pm EST
- Reporting capabilities
- Privacy Act Statement to appear for all candidates in each instance of an assessment
- Reasonable Accommodations Statement to appear for all candidates in each instance of an assessment

2.3 Data

CISA will leverage the vendors cloud services. Data must be fully owned and accessible by the Government. The vendor will download all data and provide CISA with the data – to include the interview responses - in an agreed upon format for reference, records management, and audit purposes after the closeout of the contract.
The data obtained specifically for CISA must only be accessed by CISA authorized

employees and is not for attribution or release without written consent by both the Program Manager and the COR.

3.0 PLACE OF PERFORMANCE

The primary place of performance will be the Department of Homeland Security at [redacted]

4.0 PERIOD OF PERFOMANCE

Base Period: 6/27/2024 – 6/26/2025
Option Period 1: 6/27/2025 – 6/26/2026
Option Period 2: 6/27/2026 – 6/26/2027

4.1 HOURS OF OPERATION

Contractor employees shall perform all work between the hours of 8:00 am to 5:00 pm EST, Monday through Friday (except Federal holidays).

4.2 TRAVEL

There will be no travel required for this Contract.

5.0 OBSERVANCE OF LEGAL HOLIDAYS AND ADMINISTRATIVE LEAVE

For work to be performed at Government site(s), the Contractor must establish a standard holiday schedule that coincides exactly with the Government's schedule for employees working on a Government site. Holidays observed are listed below. For Government site work, holidays and other non-workdays are not billable unless work is specifically requested by the Government and productive hours are performed on those days. The following is a list of the official Federal Government holidays:

(1) New Year's Day	(7) Labor Day
(2) Martin Luther King's Birthday	(8) Columbus Day
(3) President's Day	(9) Veterans Day
(4) Memorial Day	(10) Thanksgiving Day
(5) Juneteenth Day	(11) Christmas Day
(6) Independence Day	

In addition to the days designated as holidays, the Government observes the following days:

- Any other day designated by Federal Statute
- Any other day designated by Executive Order
- Any other day designated by the President's Proclamation

It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. In the event

the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract. When the Federal and governmental entities grant excused absence to its employees, assigned Contractor personnel may also be dismissed. The Contractor agrees to continue to provide enough personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the CO or the COR.

Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

Contractor personnel that can continue contract performance (either on-site or at a site other than their normal workstation) shall continue to work and the contract price shall not be reduced or increased.

Contractor personnel that are not able to continue contract performance (e.g., support functions) may be asked to cease their work effort.

6.0 ACCESSIBILITY REQUIREMENTS (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of

delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

7.0 ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model

and Enterprise Architecture Information Repository.

- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

8.0 Deliverables

The contractor shall ensure the accuracy, functionality, completeness, quality, and overall compliance with Government guidelines/requirements of the deliverables – as directed by the COR. Written documents shall be concise and clearly written without grammatical or spelling errors. The vendor will provide access to the methodology data that formulates and informs the scoring, as well as details on the statistical software used. The vendor will provide a report to CISA on the adverse impact statistics in relation to the assessments.

8.1 Format

Final documentation deliverables shall be provided in hard and soft copy using MS Office products as specified below. Daily, weekly, interim, informal deliverables and working-copy products may be provided by e-mail or disk, as arranged.

8.2 Final soft copy: Developed using the current DHS version of MS Word, Power Point, and/or other standard application software and provided on a CD-ROM. If more than one deliverable is provided at the same time, deliverables may be included on the same CD.

8.3 Final hard copy: Typewritten on 8-1/2"x11" white paper. The contractor shall not use spiral binding or other binding that interferes with photocopying.

9.0 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation, including FAR 52.224-1 – Privacy Act Notification (APR 1984), FAR 52.224-2 – Privacy Act (APR 1984), and FAR 52.224-3 – Privacy Training.

10.0 CONTRACT ADMINISTRATION

10.1 Points of Contact for this contract

[redacted]

11.0 Invoice and Payment Provisions

Invoices shall be submitted via email or mail. If submitting via email, send to:

The Contractor shall submit the invoice electronically to the address below: E-mail: [redacted]

Simultaneously provide an electronic copy of the invoice to the COR, CO and CS

In accordance with FAR Clause 52.232-1 Payments, or FAR 52.232-25(a)(3), Prompt Payment, as applicable, the information required with each invoice submission is as follows:

- Name and address of the Contractor;
- Invoice date and number;
- Contract number, contract line item number, and if applicable, the order number;
- Description, quantity, unit of measure, unit price and extended price of the items delivered;
- Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
- Terms of any discount for prompt payment offered;
- Name and address of official to whom payment is to be sent;

- Name, title, and phone number of persons to notify in event of defective invoice; and

- Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in the contract.

- Electronic funds transfer (EFT) banking information.

    - The Contractor shall include EFT banking information on the invoice only if required elsewhere in the contract.
    - If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer-Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer-Other Than Central Contractor Registration), or applicable agency procedures.

    - EFT banking information is not required if the Government waived the requirement to pay by EFT.

    - For the invoicing of materials that serve as identified deliverables (not including Travel and ODCs), a fully executed DHS Form 700-21 that is completed by the Contracting Officer's Representative.

Invoices without the above information and/or not submitted by one of the approved methods (mail or email) may be returned for resubmission.

In the event that an improper invoice is submitted and rejected by the Government, the Contractor shall correct the identified deficiencies and resubmit the corrected invoice under an entirely new invoice number to the previously mentioned email address.

To constitute a proper invoice, the invoices must include those items cited in FAR 52.232-1 Payments (APR 1984) and FAR 52.232-25 Prompt Payment (OCT 2008), paragraphs (a)(3)(i) through (a)(3)(x).

Payment shall be made to the contractor upon delivery to and acceptance by the Government office requesting services in the following manner.

12.0 Post Award Evaluation of Contractor Performance

12.1. Contractor Performance Evaluations

In accordance with FAR Subpart 42.1502, Policy, agencies are required to prepare an evaluation of contractor performance for each (non-construction/A&E) contract in excess of $150,000. An assessment must be prepared at least annually and at the conclusion of the contract. In addition, contracts with a period of performance exceeding one year (including option periods) require interim evaluations so as to document contractor performance and provide current information for source selection purposes.

12.2 Contractor Performance Assessment Reporting System (CPARS)

The U.S. Department of Homeland Security utilizes the Department of Defense's Contractor Performance Assessment Reporting System (CPARS), a web-enabled application that collects and manages the library of automated contractor performance assessments, to collect and maintain contractor performance assessments. An assessment evaluated evaluates a contractor's performance, both positive and negative, and provides a record on a given contractor during a specific period of time, under a specific contract. CPARS is for UNCLASSIFIED use only.

12.3 Contractor Performance Information

The DHS Office of Procurement Operations' (OPO) assessments of contractor performance shall be accessed by the contractor electronically after completion of the assessment by logging onto CPARS at https://www.cpars.csd.disa.mil. Contractors shall be given a minimum of thirty days to submit comments, rebut statements, and/or provide additional information to the Government.

The OPO Assessing Official shall review the Assessing Official Representative's assessment and consider the potential for disagreements between the Government and the contractor. If the contractor's response to the report is contentious, the Assessing Official will forward the evaluation to the Reviewing Official, who will serve as the mediator and shall resolve any dispute between the contractor and Government. If the Reviewing Official cannot resolve the dispute, the matter shall be referred to the Deputy Director, Office of Procurement Operations, for decision and resolution.

Copies of the evaluation, contractor response, and review comments, if any, shall be retained as part of the evaluation. The evaluation may be used to support future award decisions. The release of the completed contractor evaluation shall be restricted to Government personnel and the contractor whose performance is being evaluated. Once the evaluation is completed, it is copied into the Contractor Performance Assessment Reporting System (CPARS), a web-enabled, government-wide application that provides timely and pertinent contractor past performance information to the Federal acquisition community for use in making source selection decisions, where it can be viewed by authorized personnel at any agency for source selection purposes.

12.4 Interconnection Security Agreement (ISA)

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.

12.5 Encrypted Data

All encryption of data shall be FIPS 140-2 and FIPS 197 Advanced Encryption Standard (AES)

256 encryption compliant. The following methods are acceptable for encrypting sensitive information:

a. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

12.6 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personnel whose duties require them to access DHS data in the performance of this contract, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a DHS Non-Disclosure Agreement (DHS Form 11000-6) to the COR. This is required prior to the commencement of any work on any other contract, and whenever replacement personnel are proposed under this contract. Any information obtained or provided in the performance of the contract is only to be used in the performance of the contract.

12.7 Protection of Information

Contractor access to proprietary information may be required under this contract. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

12.8 Occupational Safety and Health Act Requirements

This contract requires that Occupational Safety and Health Act (OSHA) requirements be met when applicable. This contract may contain mandatory clauses relating to Environment, Safety, and Occupational Health (ESOH) considerations.

12.9 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribes policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for this contract require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in this contract.

12.10 Post-Award Instructions Regarding Security Requirements for Contracts

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is mandatory.

a. Contractor employees (to include applicants, temporaries, part-time and replacement employees) requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security Office/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security Office/PSD. The Standard Form (SF) 85P will be completed electronically through the Office of Personnel Management's e-QIP System. The below completed forms must be given to the DHS Office of Security Office/PSD no less than thirty (30) calendar days before the start date of the contract or thirty (30) calendar days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1) Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
2) FD Form 258, "Fingerprint Card" (2 copies)
3) DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
4) DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

    a. Only complete packages will be accepted by the DHS Office of Security/PSD.
    b. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information, at any time during the term of the contract. No employee of the Contractor shall begin work under the contract or be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

c. The DHS Office of Security/PSD shall be notified of all terminations/resignations within five (5) calendar days of occurrence. The Contractor shall return to the COR all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

d. Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process, which are not caused by the Government, do not relieve a contractor from performing under the terms of the contract.

e. Your POC at the Security Office is:

DHS OCSO/PSD Security Customer Service Center
Telephone: [redacted]
E-mailbox: [redacted]