# PERFORMANCE WORK STATEMENT

**Department of War Education Activity**
**4800 Mark Center Drive**
**Alexandria, VA 22350**

# DEPARTMENT OF WAR EDUCATION ACTIVITY (DoWEA)
# PERFORMANCE WORK STATEMENT (PWS)
# FOR
# SOCIAL MEDIA MANAGEMENT

## 1.0 Introduction

The Department of Defense Education Activity (also known as DoDEA, also known as the Department of War Education Activity, also known as DoWEA) is one of only two federally operated school systems, and is operated by the Department of Defense (also known as the Department of War, also known as DOW).

DoWEA plans, directs, coordinates, and manages prekindergarten through 12th grade educational programs in 161 fully accredited schools that serve over 66,000 children of active-duty military and DOW civilian families. Our curriculum, resources and student achievement scores on standardized assessments compare favorably to those of high-performing US public school systems.

Operating as a field activity of the Office of the Secretary of War (Personnel and Readiness), DoWEA is overseen by a director located at our headquarters in Alexandria, VA. DoWEA's schools are organized into three geographic areas: Americas, Europe, and Pacific. In the Americas, DoWEA operates 50 schools located in seven states, Puerto Rico, and Cuba. In Europe and the Middle East, DoWEA operates 64 schools located in Germany, England, Netherlands, Belgium, Spain, Turkey, Bahrain, and Italy. In the Pacific, DoWEA operates 46 schools located in Korea, Japan (mainland and Okinawa), and Guam. Finally, DoWEA also operates a fully accredited virtual high school with teaching hubs in the Americas, Europe, and Pacific

### 1.1 Background

The Department of War Education Activity (DoWEA) requires a secure, web-based public affairs solution to support enterprise-wide social media management, monitoring, archiving, analytics, and compliance activities. The solution must enable centralized oversight and administration of official DoWEA social media accounts while supporting day-to-day management of individual organizational pages and profiles.

DoWEA maintains an official headquarters presence on Facebook, Instagram, and LinkedIn, as well as up to 200 individual school Facebook pages and 200 individual school Instagram accounts. All social media accounts and pages must be subject to consistent management, monitoring, archiving, security, records retention, and compliance requirements.

The solution shall provide the capability to manage, monitor, archive, analyze, and secure all authorized social media accounts from a centralized platform. All data entered into, generated by, or provided to the solution on behalf of DoWEA shall remain the sole property of DoWEA and must be returned to the Government upon contract expiration, termination, or non-renewal.

### 1.2 Scope

The Contractor shall provide a secure, web-based social media management solution to support the Department of War Education Activity (DoWEA) Public Affairs mission. The solution shall provide enterprise capabilities for social media management, monitoring, archiving, analytics, reporting, and compliance across DoWEA's authorized social media platforms.

The scope includes the provision of software, licensing, system access, maintenance, updates, technical support, and user training necessary to operate and sustain the solution. The solution shall support the management and monitoring of DoWEA's official headquarters social media presence on Facebook, Instagram, and LinkedIn, as well as up to 200 individual school Facebook pages and 200 individual school Instagram accounts. All accounts and pages shall be subject to consistent management, monitoring, archiving, security, records retention, and compliance requirements.

The solution shall enable centralized oversight and administration of authorized social media accounts while supporting the operational needs of headquarters and school-level users. All data entered into, generated by, collected through, or maintained within the solution on behalf of DoWEA shall remain the sole property of the Government and shall be returned to DoWEA upon contract expiration, termination, or non-renewal.

## 2.0 Requirement Objectives

### 2.1 (Objective #1) Social Media Management Platform (SMS)/Additional Pages

The objective of this requirement is to provide a secure, enterprise-level social media management platform with an integrated archival and records management component for systemwide use. The platform shall enable centralized management, publishing, monitoring, analytics, and long-term archiving of official organizational social media accounts while ensuring compliance with federal records management, legal discovery, and information governance requirements.

**The following listed tasks help the contractor understand the requirements to meet the objective but are not exhaustive. The contractor must develop a complete solution using a performance-based approach:**

*Supporting Tasks for Requirement (Objective #1):*

2.1.1 **Task 1, Social Media Monitoring Features**—The Contractor's SMS solution shall include the following features:

2.1.1.1 Platform/Channel Management—The Contractor's solution shall be:

- Single platform with centrally governing accounts and publishing autonomy.

- Customizable interface to all ease of use and rapid learning.
- Crisis management that enables DoWEA to stop social media publishing.
- Digital Asset Management (DAM) with an asset library and content re-use.

2.1.1.2 Granular Access—The Contractor's solution shall allow access for administrators to access social sites based on DoWEA's regional infrastructure:

- Social Media Manager (and designated admins) shall have access to post to one, a subset, or all social media channels on the platform
- Americas Administrator shall have access to post to one, to a subset, or to all social media channels in the "Americas Group."
- Europe Administrator shall have access to post to one, to a subset or to all social media channels in the "Europe Group".
- Pacific Administrators shall have access to post to one, to a subset or to all social media channels in the "Pacific Group."
- Individual channel managers shall be able to post to their designated channels only; for example, the Dexter Elementary School social media administrator shall only be able to post to Dexter's Facebook and /or Instagram channels
- All media administrators shall be able to preview upcoming social media calendars (what has been scheduled for the next month) and an archive of what has been posted.
- Provide DoWEA with 360 individual accounts, with varying levels of administrator access as directed by DoWEA

2.1.1.3 Comprehensive User/Group Management—The Social Media Manager or designee shall:

- Manage access to all media sites to mitigate "native" platform posting.
- Manage permissions, adding or removing them as needed.
- Limit users on managed accounts from being able to access the native platform directly.

2.1.1.4 Post Scheduling—The Contractor's solution shall:

- Allow all administrators to schedule posts in advance. *Note*: Depending on access level and permissions post will be held in moderation/review status until someone has reviewed and approved them. Once approved, posts will go into the posting calendar.
- Allow all administrators to see upcoming posts in a calendar view (daily, weekly, monthly), including the post's current status, such as (draft, approval, etc.), target platform, and author.

2.1.1.5 Post Archival—The Contractor's solution shall:

- Have the capability of archiving content from designated social media channels/brands for FOIA compliance.
- Ensure that all archived records are searchable.

- Provide the ability to export content in csv or other industry standard format.

2.1.1.6 Workflows—The Contractor's solution shall:

- Ensure all posts go through a designated workflow for review and approval.
- Ensure only designated users are allowed to post directly without a review process.
- Include statuses similar to the following: draft, pending, approved, published, archived.

2.1.1.7 Social Media Listening—The Contractor's solution shall:

- Monitor and analyze conversations, sentiment, and emerging trends across major social media platforms
- Provide real-time alerts for negative or crisis-related content within two hours of detection.

2.1.1.8 Content Contribution and Appeal— The Contractor's solution shall:

- Ensure content is optimized for platform-specific engagement (e.g., hashtags, visuals, captions)
- Provide monthly performance reports on content reach, engagement, and audience growth. The Contractor's solution shall provide functionality to monitor conversations, sentiment, and trends across major social media platforms to include the ability to track keywords related to vendors, education technology, and procurement risks relevant to DoWEA

2.1.2 **Task 2, Product Training**: The Contractor shall provide asynchronous webinars and/or SCORM®-compliant modules that provide at a minimum an overview of the materials, explanation of the website(s), and directions for navigation. The Contractor shall provide access to a live (non-AI) customer support representative to address any questions related to the use of the services throughout the life of the contract at no additional cost. The Department of Defense Instruction (DoDI) 1322.26 mandates that modules comply with the latest possible version of SCORM®, per https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132226_dodi_2017.pdf?ver=2017-10-05-073235-400. The Contractor shall post each webinar on our learning management system (LMS, Schoology).

2.1.3 **Task 3, Transition Plan**—The Contractor shall:

2.1.3.1 Provide a time- and cost-effective draft transition plan detailing the steps the Contractor makes when assisting another contractor taking over the requirement (Exit). The draft plan shall include a timeline and estimated costs for the exit scenario. The Contractor shall finalize the transition plan based on written feedback from DoWEA.

2.1.3.2 Provide the data migration plan no later than 180 calendar days prior to the end of the period of performance. The purpose of this plan is to ensure a

seamless and orderly transition of all DoWEA data and assets to a successor vendor, should one be awarded the contract for the fiscal year 2031 competition.

- *Data Format*: A detailed description of the current data format, including file types, schema, and any dependencies.
- *Methodology*: A step-by-step process for extracting, transforming, and loading (ETL) data. This should include the tools and technologies to be used.
- *Timeline*: A schedule with specific milestones for all data migration activities, from initial planning to final verification.
- *Resources*: Identification of the personnel, hardware, and software resources required to complete the migration.
- *Assistance*: A commitment to provide technical assistance to the successor vendor during the data migration process to ensure a successful transfer to include a clear definition of what constitutes "assistance", for example, providing documentation, responding to queries, participating in meetings.

2.1.3.3 Implement the exit plans if requested in writing by DoWEA. The Contractor shall actively assist in the migration of the data to the designated successor vendor during the transition period to include collaborating with the new vendor to execute the approved plan and resolve any issues that may arise.

**2.2 (Objective #2) Technical Requirements**

The contractor shall provide a browser-based software-as-a-service (SaaS) which is fully compliant with all DoWEA standards and requirements. This includes supplying industry-standard technical assistance; and meeting all technical requirements for digital content and interoperability. There must be no requirement that any apps or non-standard Windows software be installed on any DoWEA computer

**The tasks listed below are provided to assist the Contractor in understanding the requirements necessary to achieve the stated objective; however, they are not all-inclusive. The Contractor is responsible for developing a complete solution using a performance-based approach.**

*Supporting Tasks for Requirement (Objective #2):*

2.2.1 **Task 1, Technical Support**: The Contractor shall provide industry-standard technical support for its digital resources for the life of the contract and respond to requests via telephone, video chat (Teams), or email within one business day from the initial contact. Support shall include but not limited to assisting with service problems, product setup, upgrades, and troubleshooting.

2.2.2 **Task 2, Third-Party Programs, Software, and Applications**: The Contractor shall ensure its own and its subcontractors' (third-party) programs, software, and applications meet—at a minimum—the same technical requirements as the Contractor must meet, such as single sign on (SSO) and Federal Risk and Authorization Management Program (FedRAMP) Level 2, etc. **On a case-by-case basis, DoWEA may honor requests to waive the FedRAMP Level 2 requirement.** For more information, see URL: www.fedramp.gov. Participate if required, in interviews, and deep system architecture inspections. Per DoD / DOW policy for cloud-based services, DoWEA conducts a supplemental series of validations, which closely mirror the FedRAMP Internet Cloud vetting processes. Contractor participation is normally required to complete this process. On a case-by-case basis, DoWEA may honor requests to waive the FedRAMP Level 2 requirement.

2.2.3 **Meetings**: Attend virtual meetings at no additional cost to the Government and provide the medium through which each meeting occurs, record each meeting's minutes. Submit the draft minutes to the COR within two business days of the event and finalize the minutes two business days after receipt of written feedback from the COR. *Note*: Costs associated with attending any face-to-face meetings shall be handled/ paid for as stated in the contract.

2.2.3.1 *Post-Award Conference*: Participate in a video- or teleconference with the COR five business days after award IAW FAR Subpart 42.5.

2.2.3.2 *Communications Meeting*: Convene a video- or teleconference with DoWEA Communications Department staff ten business days after award, per Technical Exhibit #1.

2.2.3.3 *Other Post-Award Meetings*: Meet with the Contracting Officer (KO), COR, and/or other Agency personnel, as appropriate, to review Contractor performance, as required by DoWEA. The KO may discuss the Agency's view of Contractor performance, and the Contractor shall apprise the Agency of any problems being experienced. The Contractor shall take appropriate action to resolve any outstanding issues the Agency raises.

**2.3 Performance Standards and Acceptable Quality Levels (Objectives 1 and 2)**

2.3.1 *Performance Standard*: Tasks shall be completed by the required completion date.

2.3.2 *Acceptable Quality Level*: See PWS Section 7, Performance Requirement Summary.

**3.0 <u>Constraints</u>**

3.1 <u>Place of Performance</u>: Work shall be performed at the Contractor's facilities.

3.2 <u>Privacy</u>—The Contractor shall:

3.2.1 *User Accounts*: Require, wherever applicable, that individual accounts possess unique usernames and passwords that do not require personally identifiable information (PII) to access online content, i.e., first & last name and any other unique personal information.

3.2.2 *Contractor Personnel*

- Ensure personnel assigned to this contract take proper precautions to protect information from disclosure. Collect and/or store all agency-owned or agency-controlled PII in accordance with the relevant requirements of the Privacy Act, 5 U.S.C, which may be found at the following URL: http://www.archives.gov/about/laws/privacy-act-1974.html.
- All Contractor personnel that have access or may potentially have access to DoWEA data in any form shall be US citizens, including any third-party penetration (PEN)/security testers.

3.2.3 *Privacy Training*: Ensure Contractor staff who have access to DoWEA's student, teacher and/or staff personally identifiable information successfully complete the DoD Privacy Act/Personally Identifiable Information (PA/PII) training before gaining access to the data and yearly thereafter. Provide copies of the certificates of completion to the COR which can be audited at any time by the Chief Information Security Officer (CISO) or his/her designee.

3.2.4 *Privacy Verification*: Provide the COR written verification of compliance with the Privacy requirements (listed above) 120 calendar days prior to the expiration of each year's contract option period or annually, as required. *Note*: After reviewing the Contractor's verification, DoWEA reserves the right to ask for further verification data in order for DoWEA to comply with DoD/DOW's evolving privacy mandates.

3.3 Liaison and Alternate Liaison—The Contractor shall:

3.3.1 Provide a liaison and alternate liaison to be responsible for the performance of work. Their names shall be designated in writing to the Contracting Officer. They shall have full authority to act for the Contractor on all contract matters relating to the daily operation of this contract. Each person shall have at least one year of experience working in a similar role.

3.3.2 Notify the COR in writing regarding any change in either liaison's role ten business days in advance of the change. If the liaison or liaison alternate is changed post-award, the replacement shall meet or exceed the qualifications and experience of the person assigned upon contract award.

3.4 Holidays and Hours of Operation

3.4.1 The liaison or alternate liaison shall be available during the hours of 9AM to 3PM Eastern Standard Time (EST), except for Federal holidays. The following list shows

recognized Federal holidays: New Year's Day, Martin Luther King Jr.'s Birthday, Presidents Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

3.4.2 Although there are different time zones within Europe and the Pacific, and specific schools across DoWEA may operate on varying schedules, the normal business hours for each region generally align with the following times in Eastern Standard Time (EST):

- **Americas Region**: 0700-1500 EST
- **Europe Region**: 0200-1000 EST
- **Pacific Region**: 2000-0400 EST

These timeframes are intended to reflect typical local working hours across the respective regions and support coordination across DoWEA offices and schools.

3.5 Availability: The Contractor shall make all resources available for the life of the contract.

3.6 Section 508 Compliance—The Contractor shall:

3.6.1 *Background*: Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires Federal agencies that develop, procure, maintain, or use information and communication technology (ICT) to ensure they are accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and data that is comparable to people without disabilities.

3.6.2 *Requirement*: Ensure that products, platforms, and services delivered as part of this work statement that are ICT or contain ICT conform to the Revised 508 Standards, 36 C.F.R. § 1194.1 & Apps. A, C & D which are located at the following URL: https://www.access-board.gov/ict/

3.6.3 *ARS*: See the website link for ICT Accessibility Requirements Statement (ARS). All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards or when Chapters 4-6 do not address one or more functions of ICT. *Note the guidance in the table below*:

| Applicable Requirements | Directions |
|---|---|
| Software Features and Components | Applies to all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, and 503 Applications. |
| Hardware Features and Components | All requirements apply. |
| Support Services and Documentation | All requirements apply. |

| | |
|---|---|
| Outputs/Deliverables | Ensures that outputs/deliverables do not adversely affect accessibility features of the existing EIT technologies. |

3.7 Organizational Conflict of Interest (OCI): The Contractor (including any subcontractor) personnel performing work under this contract may receive, have access to, or participate in the development of, proprietary or Privacy Act information (e.g., personal information, education, etc.) may create a current or subsequent OCI as defined in FAR Subpart 9.5. Whenever the Contractor becomes aware that such access or participation may result in actual or potential OCI, the Contractor shall (1) immediately notify the Contracting Officer (KO) in writing and (2) promptly submit a plan to the KO to avoid or mitigate any such OCI. *Note*: The KO will unilaterally determine if the Contractor's plan is acceptable. If the KO determines the plan cannot satisfactorily avoid or mitigate an OCI, s/he may implement other remedies to include prohibiting the Contractor's further participation in contracted requirements.

3.8 Security Clearance Requirements: Contractor personnel performing work under this contract shall have the necessary security clearances required to access Department of Defense / Department of War (DoD / DOW) networks and systems. The Contractor is responsible for verifying that each staff member has the appropriate clearance level prior to beginning work. This includes, but is not limited to, background checks and any other requirements set forth by DoD / DOW regulations available at https://www.esd.whs.mil/DD/DoD-Issuances/. Personnel without the requisite security clearance will not be permitted to access any DoWEA facilities or systems, thereby ensuring compliance with federal security mandates.

## 4.0 Government-Furnished Resources

None

## 5.0 Contract Data Deliverables

| Milestone/Deliverable | Format | PWS | Planned Frequency | Submit To |
|---|---|---|---|---|
| **Objective 1, Social Media Management** | | | | |
| Task 1, Features | Digital | 2.1.1 | Ongoing three business days after receipt of the initial delivery order. | COR |
| Task 2, Product Training | Digital | 2.1.2 | Ongoing three business days after receipt of the initial delivery order. | COR |
| Task 3, Transition Plan | Digital | 2.1.3.1<br>2.1.3.2 | *Draft*: 180 days prior to the end of the first contract year.<br>*Final:* Five business days after receipt of written feedback. | COR |

| Milestone/Deliverable | Format | PWS | Planned Frequency | Submit To |
|---|---|---|---|---|
| Task 3, Transition Implementation | Digital | 2.1.3.3 | In the final year of the contract, if required. | COR |
| **Objective 2, General Requirements** | | | | |
| Task 1, Technical Support | Digital | 2.2.1 | Ongoing after receipt of initial delivery order | COR or Requestor |
| Task 2, Third-Party Programs, Software, and Applications | Digital | 2.2.2 | Ongoing | COR/IT |
| **Constraints** | | | | |
| User Accounts | Digital | 3.2.1 | Ongoing after receipt of initial delivery order | COR |
| Privacy Training | Digital | 3.2.3 | Three days after receipt of a written request | COR |
| Privacy Verification | Digital | 3.2.4 | 120 calendar days prior to end of contract year | COR |

## 6.0 Definitions

**PA/PII** Privacy Act/Personally Identifiable Information
**SCORM®** Shareable Content Object Reference Model®

**Contracting Officer (KO)**: Only individuals with the expressed authority to obligate (bind) the Government by means of entering, administering, and terminating contracts within the limits of the authority delegated via the KO's warrant.

**Contracting Officer's Representative (COR)**: Qualified and trained Government employee, nominated by the requiring activity (RA) and appointed in writing by a KO primarily to perform specific technical or administrative functions on a specific contract(s); serves as the *'eyes and ears'* of a KO to assure the Government's best interests are protected via the terms and conditions of the contract(s). Appointed CORs do not have the authority to obligate (bind) the Government.

**Contractor**: Supplier or vendor contracted to provide specific supplies or services to the Government—may also be referred to as "the prime."

**Deliverable**: Usually physically delivered items but may include such items as digital documents/reports.

**Performance Requirements Summary (PRS)**: Tabular listing of performance objectives and standards.

**Performance Work Statement (PWS)**: Statement of work for performance-based acquisitions describing the required results in clear, specific, and objective terms with measurable outcomes.

## 7.0 Performance Requirement Summary (PRS)

| Performance Objective | Performance Standard | Acceptable Quality Level | Method of Surveillance | Inspector |
|---|---|---|---|---|
| **Objective 1, Social Media Management** | | | | |
| Task 1, Features PWS 2.1.1 | Completed in required timeline | All required features are fully operational and available. | System tracking and ongoing feedback from stakeholders on usage | COR & customers |
| Task 2, Product Training, PWS 2.1.2 | Completed in required timeline | Access 24/7/365 except for scheduled downtimes and one unscheduled downtime per year | Feedback on product training and from stakeholders | COR & customers |
| Task 3, Transition Plan, PWS 2.1.3.1 & 2.1.3.2 | Completed in required timeline | *Draft*: 80% complete. *Final:* 100% complete except for possible errors in grammar and formatting. | Review of the documents | COR & customers |
| Task 3, Transition Implementation, PWS 2.1.3.3 | Completed in required timeline | Seamless transition of all data | System checks to ensure seamless transition | COR & customers |
| **Objective 2, General Requirements** | | | | |
| Task 1, Technical Support, PWS 2.2.1 | Completed in required timeline | Acknowledge receipt of request within two hours. Resolve 90% of requests in one business day. Resolve the remaining 10% in five business days. | Normal usage of digital resources and customer complaints | COR & customers |
| Task 2, Third-Party Programs, Software, and Applications, PWS 2.2. | Completed in required timeline | 100% PWS-compliant | Initial and random inspections | IT |
| **Constraints** | | | | |

| Performance Objective | Performance Standard | Acceptable Quality Level | Method of Surveillance | Inspector |
|---|---|---|---|---|
| User Accounts, PWS 3.2.1 | Completed in required timeline | 100% PWS-compliant | Normal usage and customer complaints | COR & customers |
| Privacy Training, PWS 3.2.3 | Completed in required timeline | No more than one certificate per year sent to the COR for more than three business days from the date of the COR's request for it. | Receipt of a copy of the certificate | COR & PII Specialist |
| Privacy Verification PWS 3.2.4 | Completed in required timeline | Submitted 120 calendar days prior to the end of each contract year. | Written verification of compliance | COR & PII Specialist |

**7.1 Quality Assurance Surveillance Plan (QASP)**

The Government will utilize a QASP to monitor contractor performance. The QASP may be updated unilaterally by the Government throughout the contract period.

**Technical Exhibit #1 - TECHNICAL REQUIREMENTS**

*The Contractor shall comply with the applicable technical requirements detailed below.*
1.1 Software and Cloud Security Requirements—The Contractor shall:

1.1.1 Ensure all online resources, cloud-based services and instructional software meet the Department of Defense / Department of War (DoD / DOW) and DoWEA cybersecurity requirements as defined below. *Note*: Software, cloud services, and associated websites are rigorously tested to ensure no security risks are posed to DoWEA infrastructure and its users.

1.1.2 Complete the Cloud Services questionnaire that was submitted as part of the quote submission and provide copies of and/or access to any software listed in the proposed solution.

1.1.3 Ensure its content accessible from the web is compatible with the following browser platforms: Google Chrome, and Edge. Ensure that any applicable STIGs are implemented.

1.1.4 Provide a plan of actions and milestones (POA&M) to mitigate any cybersecurity findings resulting from non-compliant and/or vulnerable components in 30 calendar days of written notification from DoWEA.

1.2 System Requirements—The Contractor shall:

1.2.1 Provide, per Section 1.1 (above), any software installed and/or accessed in or by a DoWEA system, network whether stand-alone or web-based, is compatible with the standards cited herein.

1.2.2 Provide minimum desktop/server system technical specifications, reference architectures, networking specifications and diagrams, and applicable systems configuration documentation for the proposed solution.

1.2.3 Provide software that is compatible with the following minimum baseline:

| Specifications | Minimum |
|---|---|
| Memory | 4 GB |
| Hard Drive | 100 GB |
| Processor | Intel® Core™ i5-8365U Processor 8th Generation (up to 4.1GHz, 6MB cache) equivalent or better (Must show benchmark/pass mark scores) |
| Video Graphics | Integrated Intel HD Graphics 620 (1920x1080) equivalent or better |
| Operating System | Windows 11 |
| Browser Environment | Chrome, Edge, Edge Chromium |

1.2.4 Provide software that is completely functional on a standard DoWEA desktop without the need or requirement for administrative-level user rights and/or permissions or the requirement to use or insert external media to execute the software.

1.2.5 Provide software that does not require modifications to folder permissions while executing.

1.2.6 Provide, if applicable, software packages that support unattended installation methods used by enterprise software packaging and deployment systems.

- DoWEA currently distributes software packages via Microsoft's System Center Configuration Manager (SCCM) and Microsoft Intune.
- All older 16-bit software is automatically denied.

1.3 Data Management Requirements—The Contractor shall:

1.3.1 Provide a mechanism for batch administration and automation of routine data management tasks via flat file import, or representational state transfer (REST) based web service application programming interfaces (APIs). The mechanism shall provision and manage data objects within the Contractor's system, including but not limited to organizational structures, student accounts, staff accounts, courses, and class rosters.

1.3.2 Provide all necessary documentation and assets to facilitate batch administration and automation of routine data management tasks, including but not limited to roster template files (i.e., comma separated value templates); data element/field definitions documentation; data interchange formats and schemas (XML/ JSON); and/or data dictionaries for the purpose of mapping organizational student information system (SIS) data to the Contractor's required input formats.

1.3.3 Provide a single point of contact to support DoWEA in performing the required data integration activities within the Contractor's system.

1.3.4 Configure DoWEA enterprise within its system and/or databases as the appropriate organizational entity (i.e., region, district, school) upon a request in writing from the contracting officer's representative (COR). *Note*: DoWEA's organization hierarchy consists of the following: one system, three regions, nine districts, 62 communities, and 161 schools, including the K-12 virtual school programs.

1.3.5 Participate in a technical meeting with DoWEA within ten business days after award for the purposes of preparing for onboarding of new services and initial configuration of administrator-level accounts.

1.3.6 Ensure the transfer of any Sensitive, Confidential data including but not limited to PII data be transferred in a secure means meeting any requirements set by DoWEA's Chief Information Security Officer (CISO).

1.4 DoWEA Software License Keys: The Contractor shall provide (1) license keys and electronic downloads for software required under this Contract to the COR and (2) software directly to DoWEA schools, districts, or regions, only if explicitly required to do so in the contract or in writing by the COR.

1.5 Cybersecurity Supporting Elements/Requirements and Scalability—The Contractor shall:

1.5.1 Comply with the same Federal law and DoD / DOW policies and guidance to which DoWEA is subject that include but are not limited to the cybersecurity requirements defined in the following documents:

- DoD Directive (DoDD) 8500.01E, Information Assurance, be found at the following URL: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.
- DoD Security Technical Implementation Guidance (STIG), which may be found at the following URL: https://public.cyber.mil/stigs/downloads/.
- DoD Risk Management Framework (DODRMF) per DoD Instruction 8510.01, which may be found at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-3004.5.2.

1.5.2 Provide security patches/upgrades to include third-party applications in response to public-released security vulnerabilities associated with its software solution. Provide a POA&M for any security vulnerabilities within five business days of discovery. Software upgrades/patches shall be included in the licensing cost and be performed at the least disruptive times as determined by DoWEA in writing. *Note*: Any exception to this requirement must be approved in advance and in writing by DoWEA's Chief Information Officer (CIO) or designated official.

1.5.3 Protect DoWEA data against all cyberattacks, notifying DoWEA within 72 hours of an identified and confirmed breach/intrusion.

1.5.4 Perform security incident investigations upon identification of an event or at the request of DoWEA.

1.5.5 Address all information assurance vulnerability messages (IAVM) in the defined timelines to include IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA).

1.5.6 User passwords must not be readable by anyone having access to the system.

1.5.7 Ensure any portion of its solution that involves Internet access by DoWEA students complies with the relevant requirements of the Children's Internet Protection Act, Public Law 106-554, § 1(a)(4) [Div. B, Title XVII, § 1701], Dec. 21, 2000, 114 Stat. 2763, 2763A-335. All Contractor personnel that have access or may potentially have access to DoWEA data in any form shall be US citizens. *Note*: If its solution does <u>not</u> involve Internet access by DoWEA students, please ensure the following are included:

- Maintaining system security IAW the latest versions of the (1) DoD Cloud Computing Security Requirements Guide, (2) Family Educational Rights and Privacy Act (FERPA), and (3) Protection of Pupil Rights Amendment (PPRA).
- Providing a solution robust enough to serve the needs of a large community of learners dispersed across the world using a variety of bandwidths and scalable to meet future growth, both in terms of instruction and the number of users. In addition, provided solutions shall be applicable to the digital learning environment of the DoWEA Virtual School.
- Ensuring Contractor staff who have access to DoWEA's student, teacher and/or staff personally identifiable information take the DoD Privacy Act/Personally Identifiable Information (PA and PPI/PII) training before gaining access to the data and yearly thereafter. Provide copies of the certificates to the COR which can be audited at any time by the CISO or his/her designee.