DEPARTMENT OF THE ARMY
U.S. ARMY HUMAN RESOURCES COMMAND
1600 SPEARHEAD DIVISION AVENUE, DEPARTMENT 500
FORT KNOX, KENTUCKY 40122-5500

MEMORANDUM OF UNDERSTANDING
BETWEEN
UNITED STATES ARMY HUMAN RESOURCES COMMAND
AND
THE UNITED STATES ARMY ACQUISTION SUPPORT CENTER
MOU 19-02

SUBJECT: Protection of Data Provided to the United States Army Acquisition Support Center by the United States Army Human Resources Command, MOU 19-02

1. References:

a. Department of Defense Instruction (DoDI) 5400.11 (DoD Privacy and Civil Liberties Programs), 29 January 2019.

b. DoDI 4000.19 (Support Agreements), 25 April 2013, Incorporating Change 2, 31 August 2018.

c. Title 5 USC 552a, The Privacy Act of 1974 and Amendments.

d. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47 (Security Guide for Interconnecting Information Technology Systems), August 2002.

e. Federal Information Processing Standards 140-2 (Security Requirements for Cryptographic Modules), 25 May 2001, Change Notice 2, 3 December 2002.

f. DoDI 8500.01 (Cybersecurity), 14 March 2014, Incorporating Change 1, 7 October 2019.

g. NIST SP 800-53r4 (Security and Privacy Controls for Federal Information Systems and Organizations), 22 January 2015.

h. DoD 8570.01-M (Information Assurance Workforce Improvement Program), 19 December 2005, Incorporating Change 4, 10 November 2015.

i. DoDI 8510.01 (Risk Management Framework (RMF) for DoD Information Technology (IT)), 12 March 2014, Incorporating Change 2, 28 July 2017.

j. Army Regulation (AR) 25-2 (Army Cybersecurity), 4 April 2019.

k. AR 25-1 (Army Information Technology), 15 July 2019.

SUBJECT: Protection of Data Provided to the United States Army Acquisition Support Center by the United States Army Human Resources Command, MOU 19-02

2. Supersession. There is no previous Memorandum of Understanding (MOU) relevant to the Subject of this MOU between U.S. Army Human Resources Command (HRC) and the United States Army Acquisition Support Center.

3. Purpose. This MOU outlines the terms, conditions, and responsibilities between HRC and USAASC regarding the development, management, operation, data usage, security, and the security of interface connections. From this point forward, HRC and the USAASC will be referred to as the parties. This document covers the initial data discovery, through interface development, to production/persistent interface implementation.

4. Background. USAASC is a Direct Reporting Unit of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology responsible for providing oversight of the Army Acquisition Corps and the 40,000-strong Army Acquisition Workforce. In the Acquisition Corps there are mandated certification and education requirements that must be tracked and updated in the Career Acquisition Personnel Position Management Information System. USAASC requires HRC data in order to facilitate tracking of training and certifications for Army Reserve and Army National Guard to meet tracking requirements in a manner similar to what is done for the active component.

5. Scope. This document describes the overall understanding of obligations, responsibilities, deliverables, and delivery methods between the parties. Technical coordination between the two parties' representatives are authorized.

6. Security. Both parties agree that they will protect the data/information stored and/or received in accordance with (IAW) Department of Defense (DoD) and Army regulatory and statutory guidance. Furthermore, both parties will:

a. Agree that all data received from either party will be used only for the purpose(s) stated in the Data Interface Information Form (DIIF) (see paragraph 8 below) supporting each data exchange and specific personally identifiable information (PII) data will not be shared with other organizations without written specific prior approval of the data owner as specified by HRC policy and as defined by USAASC.

b. Ensure individuals accessing data have had training in the protection and proper handling of data and know how to report loss, spillage, or inappropriate release of sensitive data.

c. Ensure compliance with all data at rest, data in transit, and protection of PII IAW policies issued by the DoD or Army.

d. Ensure all applicable DoD security requirements are met specifying the classification and sensitivity of data provided, received, and/or stored.

e. Ensure data provided will be protected based on the security criteria found in references listed in paragraph 1 and any other associated DoD and Department of the Army regulations, directives, and policies.

f. Ensure proper breach reporting and notification procedures are followed IAW reference 1a if there is a loss, theft, or compromise of any sensitive data or PII.

g. Ensure the respective parties' Freedom of Information/Privacy Act Office is notified immediately upon the discovery of any loss, theft, or compromise of any sensitive or PII data.

h. Ensure that the other party is provided with a copy of the valid Authority to Operate (ATO) before any data transfer. Each party may assess risk and choose to cease data transfers if a party's ATO expires or a Denial of Authorization to Operate is rendered.

i. Destroy, erase, and/or anonymize expired or useless PII data/files that have been provided by the other party promptly while preventing loss, theft, misuse, or unauthorized access regardless of method of storage or transmission.

7. Responsibilities. Both parties will:

a. Provide technical instructions/guidance as necessary to execute the data transfers.

b. Coordinate with the other party for any proposed changes affecting data exchanges and agree upon a timeline for implementation.

c. Collaborate with the other party within ten business days to resolve errors resulting from data exchange.

d. Comply with any existing supplemental guidance and direction regarding cybersecurity policies, processes, and enforcement.

e. Ensure no data is sent unless all parties have signed the appropriate DIIF (see paragraph 8) and meet RMF requirements.

f. Develop anonymized data to support testing.

8. DIIF:

a. The technical details of each interface/interconnection will be documented in an DIIF. In certain negotiated instances, an agreed upon alternate document may be drafted IAW HRC's policies and procedures. Proposed changes to either system or the interconnecting medium will be reviewed and evaluated to determine the potential impact on the interconnection and/or the organization.

b. Both parties will work together to develop required DIIF(s), which must be signed by both parties and meet RMF requirements before the interconnection is activated. Signatories for each DIIF shall be the authorizing official or the formally designated appointee.

c. The parties will provide the following to the other party's management as appropriate:

(1) Required data elements.

(2) Requested data IAW the agreed timeline and the agreed format as specified in the DIIF.

(3) Special instructions associated with the use of the provided data.

(4) Technical instructions/guidance to the other party for providing sample data, executing the data calls, interface testing, and persistent production interface implementation.

(5) Notification of technical changes that impact receiving and/or processing the requested data at least 90 days in advance. The appropriate agreement(s) will be renegotiated before changes are implemented.

(6) Memorandum for Record signed by both parties for point of contact (POC) changes.

9. Data Delivery. Data delivery methods will be specified in the appropriate DIIF and will comply with current Army and DoD standards.

10. Communication:

a. Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical

levels. All communications described herein should be conducted in writing unless otherwise noted.

b. Both parties agree to provide notice of specific events within the time frames indicated below to safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit:

(1) Security Incidents. Technical staff shall immediately notify their designated counterparts of the other party by telephone and electronic mail (e-mail) when a security incident(s) is detected, so the other party may take immediate steps to determine whether its system has been compromised and to take appropriate security precautions. The affected system management shall send formal notification via e-mail to the security POC of the affected system within one hour after detection of the incident(s). The respective party shall notify the other party immediately if an incident occurs that involves loss or breach of PII (see paragraph 6f above).

(2) Disasters and Other Contingencies. Technical staff will immediately notify their designated counterparts by telephone and e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.

(3) Personnel Changes. The parties agree to provide notification of the separation or long-term absence of their respective POC(s). Both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

11. Amendment and Modification. All parties must agree in writing to any amendments or modifications to this MOU. Upon agreement and approval of the changes by all parties, modifications will be documented, and a new MOU drafted.

12. POCs:

a. The primary POC for the USAASC is Mrs. Miesha Purcell at (703) 664-5690 or miesha.l.purcell.civ@mail.mil.

b. The primary POC for Personnel Information Systems Directorate, Governance and Plans Division, Policy, Process and Agreements (PERSINSD-PSC-G) is Mr. Robert E. Lee at (502) 613-4917 or robert.e.lee43.civ@mail.mil.

13. Personnel. Each party is responsible for all costs of its personnel, including pay and benefits, support, and travel. Each party is responsible for supervision and management of its personnel.

14. Funds and Manpower. This MOU does not document or provide for the exchange of funds or manpower between the parties nor does it make any commitment of funds or resources.

15. Disputes. Any disputes relating to this MOU will, subject to any applicable law, executive order, directive, or instruction, be resolved by consultation between the parties or IAW reference 1b.

16. Termination of Understanding. The parties may terminate this MOU at any time upon mutual written agreement. Either party may unilaterally terminate this MOU upon 30-days advance written notice or in the event of a security incident that necessitates an immediate termination. If this agreement is terminated, all associated interconnection agreements will be terminated as well.

17. Transferability. This MOU is not transferable except with the written consent of the parties.

18. Entire Understanding. It is expressly understood and agreed that this MOU and any related DIIF(s) embody the entire understanding between the parties regarding the MOU's subject matter.

19. Effective Date. This MOU is effective on the date of final signature by all parties.

20. Expiration. This MOU will remain in effect for five years from the date of the final signature. After five years, this MOU will expire without further action. If the parties wish to extend this MOU, they may do so by reviewing, updating, and reauthorizing this agreement.

CASTILLO.ROBERTO.ROEL.1131761003
Digitally signed by CASTILLO.ROBERTO.ROEL.1131761003
Date: 2020.04.22 09:44:25 -04'00'

ROBERTO R. CASTILLO
COL, EN
Director, PERSINSD

_____
(Date)

SPISAK.CRAIG.A.1038819310
Digitally signed by SPISAK.CRAIG.A.1038819310
Date: 2020.04.17 10:44:45 -04'00'

CRAIG A. SPISAK
Director,
Acquisition Career Management

_____
(Date)