MEMORANDUM OF UNDERSTANDING
BETWEEN THE FEDERAL AVIATION ADMINISTRATION
AND THE
NATIONAL AIR TRAFFIC CONTROLLERS ASSOCIATION

This Agreement is made by and between the National Air Traffic Controllers Association, ("NATCA" or the "Union") and the Federal Aviation Administration ("FAA" or the "Agency"), collectively known as the Parties. This Memorandum of Understanding (MOU) represents the complete understanding of the Parties concerning the Agency's migration from Lotus Notes/Domino Lightweight Directory Access Protocol (LDAP) to Microsoft Active Directory (AD) Authentication for systems and programs used by bargaining unit employees ("BUEs").

Section 1. The Agency has determined to migrate from LDAP to AD, which will require BUEs to use their AD passwords to sign into their accounts, for the following systems and programs:

- CDR/Player;
- TARP-A;
- NOP Client;
- CEDAR;
- FALCON; and
- Safety Suite.

The deadline for BUEs affected by the migration to establish/reset their AD passwords is Tuesday, February 27, 2018 ("password deadline").

Section 2. The Agency will provide notice to affected BUEs that they must establish/reset their AD passwords in order to continue to access the systems and programs listed in Section 1 above. The attached notices will be conveyed to the BUEs via Mandatory Briefing Item (MBI), the Daily Download, and Broadcast messaging (Attachment 1) and via banner message that will appear on system/application sign in screen (Attachment 2). Attachments 1 and 2 will be issued within two (2) business days after the Parties execute this Agreement. Additionally, the Agency will ensure that the information in Attachment 1 is included via MBI issued within ten (10) days after the Parties execute this Agreement. The Agency will collaborate with NATCA regarding the contents of this notice prior to dissemination to BUEs.

Section 3. For BUEs who do not have access to personal workstations with a computer, access to a computer with privacy and Internet access will be provided in a reasonable and accessible location at the local level for BUEs to establish/reset their AD passwords.

Section 4. BUEs shall be granted sufficient duty time, if otherwise in a duty status, to establish/reset their AD passwords.

Section 5. BUEs who are unable to establish/reset their AD passwords by the password deadline because they are in an approved leave status (e.g., excused absence, LWOP, suspension) shall be afforded sufficient duty time upon their return to establish/reset their AD passwords.

Section 6. BUEs who did not establish/reset their AD passwords by the password deadline shall not have a loss of, charge to, or reduction of leave, pay, or benefits.

Section 7. This Agreement does not constitute a waiver of any right guaranteed by law, rule, regulation, or collective bargaining agreement (CBA) on behalf of either Party.

Section 8. This MOU shall remain in full force and effect for the duration of the Parties' CBAs, unless modified by mutual agreement of the Parties.
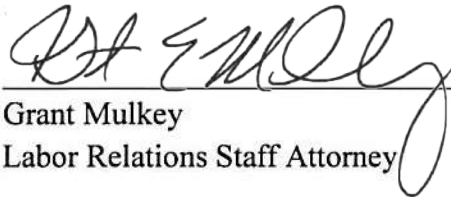
Signed this 9th day of February 2018.

For NATCA:

Dean Iacopelli
Eastern Regional Vice President

Ryan Smith
Director of Labor Relations

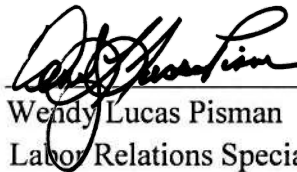Grant Mulkey
Labor Relations Staff Attorney

For the FAA:

James C Stroiney

Digitally signed by James C Stroiney
DN: c=US, o=U.S. Government, ou=FEDERAL
AVIATION ADMINISTRATION, ou=FEDERAL
AVIATION ADMINISTRATION, cn=James C
Stroiney
Date: 2018.02.09 08:01:03 -05'00'

James Stroiney, FAA Acting Deputy CIO
Office of Information & Technology (AIT-2)

Raymond C. Mittan, Group Manager,
Labor & Employee Development, AJG-L1

Wendy Lucas Pisman
Labor Relations Specialist (AHL-300)

<div align="center">

Decommissioning Lotus Notes / Domino Services and Servers

Employee Notification

</div>

February XX, 2018

After the transition to EMS365 (Microsoft Outlook, Lync) in 2013, the Office of Information & Technology (AIT) began decommissioning the Lotus Notes/Domino infrastructure, including servers and services, that were used by personnel across the FAA.

On February 27, 2018, AIT will sunset a Lotus Notes/Domino service:

• LDAP (Lightweight Directory Access Protocol) – This enabled application authentication. Several services now provide user authentication, based on the need of each impacted application.

The following applications, which currently use the above service, will be migrated to Microsoft's Active Directory (AD) Password Authentication:

> CEDAR
> FALCON
> Safety Suite
> CDR/Player
> TARP-A
> NOP Client

NATCA bargaining unit employees shall be granted sufficient duty time, if otherwise in a duty status, to establish/reset their AD passwords in order to maintain continued access to these applications.

On February 28, 2018, the above systems/programs will prompt employees to sign in using their Microsoft AD password.

After this migration, users of the above applications will use their AD username and password to obtain access. If an employee does not know their AD password, AIT cannot retrieve this—the password can only be reset. However, the individual can change their own password by using one of the job aids at the links below:

> **Change FAA Network Password:**
> https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/services/training/aids/HowToChangeFAANetworkPassword.pdf
>
> **Change Network Password in OWA from Home:**
> https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/services/training/aids/ChangeFAANetworkPasswordInWebmailfromHome.pdf
>
> **Change Network Password in OWA from the Office:**
> https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/services/training/aids/ChangeFAANetworkPasswordInWebmailfromTheOffice.pdf

These three job aids can also be found on the IT Training Services Training Aids site:
https://my.faa.gov/org/staffoffices/afn/information/services/training/aids.html

> Using one of these job aids, the employee can logon using their PIV card via PIV/MyAccess and enter a new password; it does not require that you know your current password. The change is immediate and does not require a call to or ticket placed with the HelpDesk.

> As an alternative, the employee can also contact the MyIT Service Center, which is available 365/24/7, to reset their password.

While AIT believes that all applications that utilize the Lotus Notes/Domino services or servers described above have been identified and addressed, anyone aware of an application that may have been missed should contact Steve Terres, steve.terres@faa.gov, AIT's Lotus Notes / Domino Decommissioning project manager, immediately.

LDAP ID Migration to Microsoft ID
ATTACHMENT 2
February 5, 2018

Message Banner that will appear on the sign-on screen for all systems/programs

As of February 27, 2018, LDAP ID passwords will no longer be effective for accessing this system/application. Beginning February 28, 2018, you must use your FAA Windows (Active Directory) username and password to access this system/application. If you have any issues logging in, please contact {Application Owner Email}.

For more detailed information, click here.

The "click here" would take you to the Attachment 1 message.