OMB Control Number 1652-0065
Exp. 2/29/2020

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

COMPUTER ACCESS AGREEMENT (CAA)
External Personnel Only

INSTRUCTIONS: All Non-TSA personnel who will be using TSA-authorized Information Technology (IT) systems are required to complete and annually sign a TSA Form 1430 *Computer Access Agreement (CAA)*. This form is for non-TSA personnel only, including, but not limited to, airline staff, airport staff, LEOs, government staff (e.g., treaty negotiations), DHS staff who are not TSA employees or contractors and all non-TSA staff who receive access to alerts and Watchlists through TSA Form 1427. If you are a TSA employee or contractor, please use TSA Form 1403, Computer and Personal Electronic Device Access Agreement. Signature certifies understanding and acceptance of applicable policy and legal requirements concerning access to network resources within DHS/TSA. This agreement is based in part on policy delineated in TSA MD 1400.3, *Information Technology Security* and the TSA Information Assurance Handbook. Department of Homeland Security (DHS) Office of the Inspector General (OIG), TSA Office of Information Technology (OIT), and/or the Information Assurance and Cybersecurity Division (IAD) shall conduct periodic audits to determine organization compliance.

SECTION I. User Information

Full Name (Last, First, MI):	Employer
Routing Symbol/Airport Code	Email Address

SECTION II. Terms of Agreement

Credential Protection - I will protect my password, passphrase, or personal identification number (PIN) from disclosure and any authentication credentials such as the Personal Identity Verification (PIV) smart card from loss at all times. Where available, PIV smart card credentials shall be used as the primary means of logical authentication for sensitive systems and network PINS for PIV card-enabled users shall not expire. I will change my default passwords immediately when assigned. I will never reveal my password/passphrase/PINs to other individuals and I will not construct my password from obvious personal data (e.g., social security number, telephone numbers, relative's names, pet's name, etc.).
User Accounts - I will not allow others to use my account and I will not access other users' accounts. I will not attempt to access accounts or data stores that are not expressly authorized to me without authorization from my supervisor. I understand that I am accountable for all actions taken under my username.
Data/Information Protection - I will protect all data storage devices (e.g., CDs, DVDs, flash, thumb or jump drives, hard drives, etc.) in accordance with the highest level of data sensitivity requirements for the data contained on those storage devices.
Consent to Monitor/Privacy - I understand that I have no expectation of privacy when using or storing data on government systems.
Protection of Displayed Data - I will lock or log off from my computer when leaving my work area unattended for extended periods. I will use a screen saver that requires the reentry of my password, passphrase or PIV credential and PIN when my system is idle for short periods of time.
Copyright Protection - I understand I may be personally liable for any personal or other use, copying, reverse engineering, or other software copyright violations not authorized by the government and committed by me or as a result of my failure to adequately protect my password, passphrase, PIN or any authentication means, on government systems under my control.
Rules of Behavior - I will use government networks and assets in a manner consistent with the general guidelines for acceptable use and the specific requirements as outlined in this Terms of Agreement and approved TSA policy. IT assets include, but are not limited to: access to government networks, and cautiously using government networks to access public networks, such as the Internet.
Data/Information Protection - I will not attempt to create unauthorized links to other systems, bypass authentication mechanisms, circumvent data/information access control and authentication procedures, or otherwise jeopardize the security of government IT systems.
Sensitive Security Information (SSI) - SSI and Personally Identifiable Information (PII) are permitted to be entered, processed, stored and transmitted only in accordance with approved privacy guidelines.
Social Media - I shall observe proper operational security (OPSEC) and information security (INFOSEC) practices when using social media. I shall not use any sensitive government information during any engagement within social media.

Previous editions of this form are obsolete.

Responsibilities and Conduct - I understand that as a user of TSA IT systems, I must abide by approved TSA policy, and all other relevant policies, laws, and regulations. **Patching -** All software installed on end user assets shall have the latest approved security patches.
Section III: Acknowledgement
I have read and agreed to comply with the Terms of Agreement listed in Sections I and II as applicable. Signature: Date:

PRIVACY ACT STATEMENT: AUTHORITY: 5 U.S.C. § 301 Departmental Regulations. **PRINCIPAL PURPOSE(S):** All external personnel who will be using TSA information technology systems are to complete this agreement signifying understanding and acceptance of applicable policy and legal requirements concerning the operation of computer equipment and access to network resources within the TSA. **ROUTINE USE(S):** This information may be shared in connection with establishing an access account for an individual or for routine uses identified in DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records (GITAARS) System of Records. **DISCLOSURE:** Voluntary; failure to furnish the requested information may result in a loss of computer access privileges.

PAPERWORK REDUCTION ACT: This is a mandatory collection of information if you wish access to a TSA Information Board. The total average burden per response associated with this collection is estimated to be approximately 1 hour. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-0065 which will expire on 02/29/2020. Send comments regarding this burden estimate or any other aspect of this collection of information including suggestions for reducing this burden to TSA PRA Officer, 601 S. 12th Street, Arlington, VA 20598-6011. ATTN: PRA 1652-0065.

Previous editions of this form are obsolete.