TRAINING AND EMPLOYMENT NOTICE	NO. 21-23
	DATE February 28, 2024

TO: AMERICAN JOB CENTERS
STATE WORKFORCE AGENCIES
STATE WORKFORCE ADMINISTRATORS
STATE WORKFORCE LIAISONS
STATE AND LOCAL WORKFORCE BOARD CHAIRS AND DIRECTORS
STATE LABOR COMMISSIONERS
WORKFORCE INNOVATION AND OPPORTUNITY ACT SECTION 166
INDIAN AND NATIVE AMERICAN GRANT RECIPIENTS
WORKFORCE INNOVATION AND OPPORTUNITY ACT SECTION 167
MIGRANT AND SEASONAL FARMWORKER JOBS PROGRAM GRANT RECIPIENTS
SENIOR COMMUNITY SERVICE EMPLOYMENT PROGRAM GRANT RECIPIENTS
JOB CORPS GRANT RECIPIENTS
RECIPIENTS OF DEPARTMENT OF LABOR FINANCIAL ASSISTANCE
SUB-RECIPIENTS OF DEPARTMENT OF LABOR FINANCIAL ASSISTANCE

FROM: BRENT PARTON /s/
Principal Deputy Assistant Secretary

SUBJECT: Protecting Identifying Information on Grant Notices of Award

1. **Purpose.** To inform grant recipients of the need to protect and prevent important identifying information in the Grant Notice of Award (NOA) from unauthorized use, including, but not limited to, use of this information to gain unauthorized access to federal systems to conduct fraudulent activities.

2. **Action Requested.** Please disseminate this information to all staff directly or indirectly responsible for grants management, including those performing financial management and financial reporting for grants and cooperative agreements of the U.S. Department of Labor (Department).

3. **Summary and Background.**

   a. Summary – This Training and Employment Notice (TEN) informs grant recipients that they should protect important information included in their grant NOA, such as the Payment System Identifier (ID), to prevent its unauthorized use, as it can be used to access federal systems to conduct fraudulent activities.

b. Background – In the past few years, cyberattacks have increased rapidly, targeting computer information systems, networks, infrastructure, personal computers, tablets, and even smartphones. The primary purpose of these attacks is to attempt to access data, functions, or other restricted areas of the system without authorization, potentially with malicious intent.

All grant-making agencies within the Department, including the Employment and Training Administration, send a NOA to entities selected to receive federal financial assistance. The NOA is the official, legally binding issuance of the federal assistance award.

The intent of this TEN is to inform grant recipients of the need to protect and safeguard important information included in the NOA that may be used to gain unauthorized access to federal information systems, networks, and infrastructure.

4. **Protecting Identifying Information on the NOA.** An award's NOA is automatically generated by the Department's grant processing system, GrantSolutions, and serves as the official document to inform grant recipients that their application for federal assistance has been approved. Upon award issuance, the GrantSolutions system transmits an email notification to the applicable Authorized Representative and Program/Project Director listed on a recipient's *Application for Federal Assistance* (also known as the Standard Form [SF]-424), informing them that the NOA and associated award documents are available for their review. The NOA provides award information to the grant recipient and indicates that funds may be requested for drawdown from the U.S. Health and Human Services (HHS) Payment Management System (PMS). NOAs are issued for the initial grant award and for each subsequent grant amendment during the project's approved period of performance. The Grants Management Officer (GMO), who is authorized to obligate funds on behalf of the Department, signs the NOA.

The NOA contains much of the information about the award that is required by 2 CFR Part 200.211. It also contains the **Payment System ID that uniquely identifies the grant recipient in PMS**. The Department's NOA includes the following information:

- **Award Identifiers:** Award Number, Federal Award Identification Number (FAIN), and Federal Award Date
- **Recipient Information:** Recipient Name, Congressional District of Recipient, contact information for the Projector Director or Principal Investigator and Authorized Official for the grant recipient organization and other important recipient identifying information, such as Payment System ID, Employer Identification Number (EIN), Data Universal Numbering System (DUNS) number, and Unique Entity Identifier (UEI)
- **Federal Agency Information:** Awarding Agency Contact Information and Program Official Contact Information
- **Federal Award Information:** Total approved amount of the federal award, period of performance start and end date, funding approved under each budget category, and accounting classification codes (account number, document number, administrative codes, etc.)

The Payment System ID, which is included in the Recipient Information section of the NOA, is **a critical data item**. This is a string of digits and letters that uniquely identifies the payment account number and type that a grant recipient uses to receive funding from their federal assistance award. It is also one of the data items used by HHS-PMS to validate grant recipient login account request access to PMS.

If it is the practice of your organization to publish NOAs[1] on a website accessible to the public, the Department recommends that you **redact or mask the Payment System ID** to prevent unauthorized use of your accounts by fraudsters. Additionally, if your organization has already published an NOA(s), consider redacting this information and reposting the NOA(s) to your website. A sample NOA, showing the redacted Payment System ID information on pages 1 and 2, is included as an attachment for illustrative purposes.

Additional Safeguards. To further protect and secure information and unauthorized access to systems, please exercise due diligence when reviewing requests received for information, access, or action on your part, particularly when the request is regarding a financial matter. The Department is offering the following tips to further bolster the security of your payment account within PMS:

- Carefully review emails received from PMS and avoid clicking on links unless the source of the email is authenticated.
- Access to systems can be gained through social engineering. Please do not provide payment account user IDs or passwords via email or phone call, as fraudsters often use social engineering to tap the credentials of others to gain unauthorized access to payment accounts.
- Do not share your user ID and password with any other individual, regardless of whether the individual is internal or external to your organization.
- Implement the following best practices if your organization has a PMS payment account set up to receive a grant award:
    - Routinely check your PMS payment account to ensure account information (list of staff who has access is current) and that account balances are accurate.
    - Immediately submit requests to deactivate user accounts if individuals leave your organization and had access to your PMS payment account.
        - Instructions on how to deactivate user accounts can be found on the PMS website (https://pmsapp.psc.gov/pms/app/userrequest/request/deactivate?), or you can contact the PMS Helpdesk to ensure prompt deactivation.
    - Immediately report suspicious account or drawdown activities not authorized by your organization via email to:
        - Your Department contact (e.g., Federal Project Officer);
        - The Department's PMS Liaison Accountants - Linda Porter (Linda.Porter@psc.hhs.gov) and Mary Lanham (Mary.Lanham@psc.hhs.gov); and
        - The PMS Helpdesk (PMSSupport@psc.hhs.gov).

[1] It is recommended that documents published on websites be 508-compliant for maximum accessibility.

Please ensure your communication provides the impacted award number and other relevant award information.

5. **Inquiries.** Please direct any inquiries regarding this topic to your contact at the Department, such as your assigned Federal Project Officer, or the appropriate regional office.

6. **References.**

- The Computer Fraud and Abuse Act (18 U.S.C. 1030);
- Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794d); and
- 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.

7. **Attachment.**

- Attachment I: Sample NOA with Redacted Payment System ID Information