TRAINING AND EMPLOYMENT NOTICE	NO. 26-07
	DATE January 23, 2008

TO: **ALL STATE WORKFORCE LIAISONS**
ALL ONE-STOP CENTER SYSTEMS LEADS
ALL STATE AND LOCAL WORKFORCE BOARD CHAIRS AND DIRECTORS
ALL ONE-STOP CENTER SYSTEM STAFF

FROM: **GAY M. GILBERT /s/**
Administrator
Office of Workforce Investment

SUBJECT: **Job Bank Security Fraud Awareness**

1. **Purpose.** To increase awareness of potential threats to Personally Identifiable Information (PII) and other types of data stored in state job bank data systems and inform states and local areas about resources for job bank fraud prevention and reporting.

2. **Background.** The Internet and online job banks have changed the way people look for work. A recent Internet search on the words 'job banks' returned over 1.1 million results. Many if not all state job banks are accessible over the Internet.

   While the Internet can provide a safe and easy way for job seekers to expand the scope of their job search, 'cyber scammers' are targeting unsuspecting consumers using sophisticated tools and techniques. Threats to Internet security continue to increase. Attackers are becoming more organized, and focused on financial gain. Multi-staged attacks are increasingly used to obtain confidential information that can be used in identity theft and other Internet fraud activities and schemes.

   Attackers are targeting victims by first exploiting trusted entities such as job banks. Then, using 'social engineering' techniques, they manipulate people into divulging confidential information that is then used to commit fraud. Cybercriminals are increasingly exploiting popular consumer Web sites to target trusting users. See Sharon Gaudin, Cybercriminals Lurk in Dark Corners of Trusted Web Sites, Information Week, September 18, 2007, available at (http://www.informationweek.com/story/showArticle.jhtml?articleID=201807108)

3. **Examples of Job Bank Fraud.**
According to recent media reports, major commercial job Web Sites (including a government site run by a commercial organization) have reported the theft of confidential job seeker PII in the last six months:

- A financial services company employee allegedly posed as an employer to gain access to a major commercial resume job bank in order to develop sales leads. See Ross Kerber, Online Job Hunters Grapple with Misuse of Personal Data, Boston Globe, October 1, 2007, available at (http://www.boston.com/business/globe/articles/2007/10/01/online_job_hunters_grapple_with_misuse_of_personal_data/)

- Data apparently is being stolen using fraudulent ads placed on at least two online job sites, and stockpiled by one hacker group using the latest variance of the Prg Trojan program. See Susan Gaudin, Phony Job Ad Nets More Stolen Identities, Information Week, August 21, 2007 available at http://www.informationweek.com/news/showArticle.jhtml?articleID=201801551.)

- In addition, ETA has received reports that job seekers in two states have become victims of Internet fraud after posting PII on a job bank.

4. **Online Resources.** The following government sponsored Web sites provide information about Internet fraud.
   - **Federal Bureau of Investigation (FBI)** - IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations (http://www.ic3.gov/).
   - **Common Fraud Scams and Internet Scams -** A good source of information about common fraud scams and Internet scams is the Federal Bureau of Investigation Fraud Web Site. (http://www.fbi.gov/cyberinvest/escams.htm)
   - **Federal Trade Commission** - The FTC deals with issues that touch the economic life of every American and creates practical and plain-language educational programs for consumers and businesses in a global marketplace with constantly changing technologies. (http://www.ftc.gov/)
   - **Federal Trade Commission, Fighting Back Against Identify Theft -** This Web Site is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help deter, detect, and defend against identity theft. (http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html)
   - **Internet Fraud** - This site provides a list of official government web resources to help in reporting and learning about Internet fraud.

(http://www.usa.gov/Citizen/Topics/Internet_Fraud.shtml)

- **Practical Tips from the Federal Government on How to be on Guard Against Internet Fraud** (http://onguardonline.gov/index.html). This site is maintained by the Federal Trade Commission with significant contributions from other Federal government organizations as well as the private sector.
- **Protecting Personal Information – A Guide for Business** – This site presents five key foundational principles of building a sound data security plan. (http://www.ftc.gov/infosecurity/)
- **Looks Too Good To Be True.com** - This Web Site was built to educate the consumer, and help prevent those using the Internet from becoming victims of an Internet fraud scheme. Funding for the site has been provided by the United States Postal Inspection Service and the Federal Bureau of Investigation. (www.lookstoogoodtobetrue.com)
- **U.S. Postal Inspection Service** - U.S. Postal Inspectors investigate any crime in which the U.S. Mail is used to further a scheme--whether it originated in the mail, by telephone, or on the Internet. The use of the U.S. Mail is what makes it mail fraud. (http://www.usps.com/postalinspectors/fraud/welcome.htm)

5. **Reporting Internet Fraud**. There are several sources to visit for information on how to report Internet-related fraud issues:
   - The Internet Crime Complaint Center (http://www.ic3.gov/complaint/).
   - The Department of Justice's "Reporting Computer, Internet-Related, or Intellectual Property Crime" Web page provides access to a large number of agencies where you may report your information based on the type of occurrence. (http://www.cybercrime.gov/reporting.htm)
   - The United States Computer Emergency Readiness Team (US-CERT) Web Site provides information on viruses and other issues related to cyber attacks. (http://www.uscert.gov/). In addition the US-CERT Web Site can be used to report attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII related incidents.
   - The Econsumer.gov Web Site accepts complaints about e-commerce (business or trade that takes place on the Internet) across international borders. (http://www.econsumer.gov/).

6. **Action Requested.** Addressees are requested to share this information with businesses, job seekers, and partners in their local areas as appropriate.

7. **Inquiries.** For more information about Job Bank Security Fraud Awareness, contact Anthony D. Dais, Office of Workforce Investment at dais.anthony@dol.gov (202) 693-2650.