EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OUI/DPM
	DATE November 2, 2020

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 4-21

TO: STATE WORKFORCE AGENCIES

FROM: JOHN PALLASCH /s/
Assistant Secretary

SUBJECT: Unemployment Insurance (UI) Information Technology (IT) Security – Additional Information

1. **Purpose.** To provide State Workforce Agencies (SWAs) with information on the National Institute of Standards and Technology (NIST) IT security guidelines for use by SWAs to ensure the security of their UI IT systems.

2. **Action Requested.** The Employment and Training Administration (ETA) requests that state administrators provide this information, including the attached UI IT Security Guide, to the appropriate staff, including UI Directors and Chief Information Officers.

3. **Summary and Background.**

   a. Summary - In an ongoing effort to provide updates to the UI IT security information to the SWAs, this advisory transmits and provides the link to the UI IT Security Guide (https://ui.workforcegps.org/resources/2019/08/19/16/47/UI_IT_Security_Guide) on the UI Community of Practice (UI CoP) website.

   b. Background – It is critical to the integrity of the UI program that SWAs continuously improve the security of their UI IT systems. Since 2004, ETA has periodically provided security guidance to the SWAs. Unemployment Insurance Program Letter (UIPL) No. 24-04, and its Changes 1, 2, 3, 4, and 5 provided the SWAs with IT security guidance via a Compact Disk (CD), titled *IT Security Information.* With this UIPL, ETA has collaborated with the Department of Labor's Office of Chief Information Officer to provide an updated version of the UI IT Security Guide as an attachment to this UIPL.

4. **IT Security Guidance.** Conducting periodic IT security assessments and audits offer an opportunity for SWAs to ensure compliance with Federal requirements, to help receive the authority to operate from state authorities, connect to Federal systems to meet program requirements, and to identify and respond to areas where system security can be improved.

RESCISSIONS None	EXPIRATION DATE Continuing

ETA strongly encourages each SWA to conduct periodic IT security assessments and audits of its UI IT systems in accordance with the NIST IT security guidelines, specified in the NIST Special Publication (SP) 800-53A, and to take necessary steps to improve its IT security based on the results of the assessments. Additionally, ETA recommends the use of an "independent" entity to conduct state IT security assessments and audits as a best practice. The entity conducting the assessment or audit must be technically, managerially, and financially independent of the system that is under review.

The results of the security assessment can be used each year as a basis for providing an update on the assurance referenced in State Quality Service Plan Handbook 336, Chapter 1, Section VIII, J, Assurance of Automated Information System Security.

Each state is required to provide an assurance that it is maintaining adequate IT security and that such security is commensurate to the level of risk associated with the UI program and the UI IT environment. Given the massive quantities of personally identifiable information (PII) and confidential data maintained on state IT systems, it is critical that SWAs follow industry protocols for maximum IT security.

NIST IT security guidelines are based on best practices complied from several security documents, organizations, and publications, and are designed as a framework for Federal agencies and programs requiring stringent IT security measures. NIST SPs assist federal agencies to meet requirements mandated under the Federal Information Security Management Act (FISMA) and other regulations. The NIST IT security-related guidance is widely used by Federal agencies, and it offers a comprehensive security framework and guidance for SWAs to follow when implementing an information security program.

The UI IT Security Guide provides information for SWAs to conduct periodic security assessments and provides references to specific laws, regulations, and NIST SPs for IT security-related guidance. The security assessment guidelines are based on criteria and guidance established by NIST and specified in the SPs. SWAs may conduct a security assessment of their UI systems to verify that security controls conform to the laws, regulations, and the guidance established by NIST.

The following NIST publications are important for conducting security assessments of UI IT systems. The links to access these and other external publications are provided in the attached UI IT Security Guide.

- Federal Information Processing Standards (FIPS) Publication 199, which provides standards for categorizing information and information systems;
- FIPS Publication 200 and NIST SP 800-53, which provide guidelines for selecting and specifying security controls that meet minimum security requirements for information systems; and
- NIST SP 800-53A, which provides guidelines for assessing the effectiveness of security controls employed in information systems.

Protecting Personally Identifiable Information (PII)

Securing the confidentiality, integrity, and availability of information stored in SWA UI IT systems is vital to controlling fraud in the UI program. Recent Office of Inspector General investigations have identified that, in some situations, state employees abused their positions of trust by misusing confidential PII to enable UI fraud. The NIST SP 800-53, Personnel Security (PS) security control (Position Risk Designation (PS-2) and Personnel Screening (PS-3)), provides guidance on controls that should be followed prior to assigning personnel handling PII. ETA recommends that SWAs conduct pre-employment and periodic background and credit checks for employees with direct access to PII related to the UI program and take appropriate actions with employees who have negative results related to periodic suitability investigations in accordance with NIST SP 800-53. Additionally, SWAs should strengthen existing systematic audit controls to track access to PII.

ETA strongly recommends that SWAs implement the following security controls in accordance with the guidance provided in NIST SP 800-53 to protect PII:

- Access Control;
- Awareness and Training;
- Audit and Accountability;
- Identification and Authentication;
- Individual Participation;
- Physical and Environmental Protection; and
- Personnel Security.

Additionally, NIST SP 800-122 provides specific guidance that SWAs can use in protecting the confidentiality of PII, including how to prevent inappropriate access, use, and disclosure of this information. This SP provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The guide also suggests safeguards that may offer appropriate levels of protection for PII.

Preventing Cyber Threats and Attacks on Critical Infrastructure

Cyber-attacks on digital and physical infrastructure systems are growing areas of concern. These threats are escalating as more sophisticated, organized groups are designing targeted attacks to damage or disrupt vital services and critical physical systems. The National Infrastructure Advisory Council is tasked with assessing how existing Federal authorities and capabilities can be employed to assist and better support the cybersecurity of critical infrastructure assets that are at greatest risk of a cyber-attack, possibly resulting in catastrophic regional or national effects on public health or safety, economic security, or national security.[1]

[1] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017.

SWAs are strongly encouraged to protect their IT systems and information from cyber-attacks such as viruses, trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information), and control system attacks. The Cybersecurity Infrastructure Security Agency (CISA), a division of the Department of Homeland Security, is responsible for protecting the nation's critical infrastructure from physical and cyber threats. CISA's website provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders. SWAs should use available guidance and resources provided by CISA to implement a cybersecurity program. For example, there have been recent ransomware attacks on state and county governments, a type of virus that can compromise the computer networks across agencies. A ransomware attack typically locks an infected computer system until payment, usually in the form of cryptocurrency, is sent to the hacker. CISA provides information on how to protect IT systems from ransomware attacks, and how to respond to possible ransomware attacks. See Cybersecurity and Infrastructure Security Agency Ransomware at https://www.us-cert.gov/Ransomware.

Incident Reporting

Computer security incident response has become an important component of IT programs. Cybersecurity-related attacks have become more numerous and diverse as well as more damaging and disruptive. New types of security-related incidents emerge frequently; therefore, preventive activities based on the results of risk assessments can help to minimize these types of incidents. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

States are encouraged to implement formal procedures for Incident Reporting using NIST SP 800-61 that provides guidelines for incident handling including data breaches, particularly for analyzing incident-related data and determining the appropriate response for each incident. Additionally, while states may have their own security breach notification laws that require them to notify individuals or entities affected by a data breach and take specific steps to remedy the situation, SWAs are encouraged to periodically review and enhance their notification procedures using best practices and other guidance provided in NIST SP 800-122. This publication provides recommendations for developing incident response plans for breaches involving PII.

UI Information Technology Support Center (ITSC)

UI ITSC provides SWAs with the full scope of IT Security guidance as part of its UI IT Modernization support and delivery, as well as the application of FIPS, FISMA, NIST, and Internal Revenue Service (IRS) Publication-1075 standards. UI ITSC IT Security-related services includes collaborating with SWAs for the development of a System Security Plan, assisting in remediation of System Security Plan deficiencies and addressing SWA Security Audit findings. UI ITSC provides guidance to SWAs in NIST-driven areas such as Contingency Planning, Auditing, Continuous Monitoring, FIPS-140-2 Encryption, and Configuration Management.

With the growing emphasis of the use of the Cloud technology in the UI Domain, UI ITSC provides expert advice on Cloud preventative, detection, countermeasure, and remediation security Cloud services. UI ITSC has worked very closely with SWAs who were early Cloud technology adopters, especially emphasizing Social Security Administration (SSA) security requirements for accessing SSA data and IRS Publication-1075 standards for cloud compliance and safeguards for the Treasury Offset Program[2]implementation.

UI ITSC has IT Security-related resources on its members only website www.itsc.org. SWAs can contact UI ITSC at securitycorner@itsc.org for IT Security guidance and services.

5. **Inquiries.** Please direct inquiries to the appropriate ETA Regional Office or to Jagruti Patel, 202-693-3059, patel.jagruti@dol.gov in the National Office**.**

6. **References.**
   - Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017;
   - UIPL No. 24-04, *Unemployment Insurance Information Technology Security*, and its Changes 1, 2, 3, 4, and 5, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=1575;
   - ET Handbook No. 336, 18th Edition, *Unemployment Insurance (UI) State Quality Service Plan (SQSP) Planning and Reporting Guidelines, Chapter 1, Section VIII, J, Assurance of Automated Information Systems Security*, https://wdr.doleta.gov/directives/attach/ETAHandbook/ETHand336_18th_Ch3.pdf?DOCN=2831;
   - FIPS Publication 199, *Standards for Security Categorizations of Federal Information and Information Systems*;
   - FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
   - NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*;
   - NIST SP 800-53A, *Assessing the Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*;
   - NIST SP 800-61, *Computer Security Incident Handling Guide*; and
   - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

7. **Attachment.** UI IT Security Guide

[2] The Treasury Offset Program is a centralized offset program, administered by the Bureau of the Fiscal Service's Debt Management Services (DMS), to collect delinquent debts owed to federal agencies and states (including past-due child support), in accordance with 26 U.S.C. § 6402(d) (collection of debts owed to federal agencies), 31 U.S.C. § 3720A (reduction of tax refund by amount of the debts), and other applicable laws.