Financial Statement Findings and State Responses
(Reformatted from the FY 2020 Report on Internal Control and Compliance)

2020-01

Department of Economic Security did not put all critical identity verification or other anti-fraud measures in place before paying federal CARES Act unemployment insurance benefits and reported it paid over $1.6 billion in fraudulent identity theft claims, as of June 30, 2020, and other states nation-wide also paid fraudulent identity-theft claims

Condition—The Department of Economic Security (DES) has identity verification and anti-fraud measures in place for its regular unemployment insurance (UI) benefits program, and the U.S. Department of Labor (DOL) issued guidance to states regarding 3 mandatory and 8 strongly recommended anti-theft and fraud measures for the federal CARES Act unemployment insurance (UI) benefits programs.[1] However, DES did not put in place all critical identity verification and other anti-fraud measures before paying CARES Act UI benefits starting in May 2020.

In response to the COVID-19 pandemic, on March 27, 2020, the President of the United States signed into law the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which expanded UI through new federally funded programs to provide economic relief to individuals who were unable to work because of the COVID-19 pandemic, including individuals who historically were not eligible for regular UI benefits such as self-employed and gig workers.[2] In April 2020, DES contracted to use a new UI benefits system because its more than 30-year old-system was unable to handle the computer programming needed to quickly implement the new federal CARES Act UI benefits programs. As it was implementing the new benefits
system, DES did not initially include any identity verification or other anti-fraud measures in the system or as part of its UI benefits process for the new federal CARES Act UI benefits programs like it has in place for its regular UI benefits program and despite warnings from the DOL that it had not relaxed its expectations related to fraud prevention in light of the pandemic. Specifically, in its April 5, 2020, instructions for implementing and operating the new federal CARES Act Pandemic Unemployment Assistance (PUA) program, the DOL reminded states that they were required to take reasonable and customary precautions to deter and detect fraud.[3] Then, on May 11, 2020, the DOL issued guidance specifying 3 mandated and 8 strongly recommended identity theft and anti-fraud measures for CARES Act UI benefits programs. The 3 mandated measures are consistent with those required for the regular UI benefits program.[1] However, DES did not implement the 3 mandated and 4 of the 8 strongly recommended identity theft and anti-fraud measures before paying federal CARES Act UI benefits on May 18, 2020, through its new UI benefits system (see Finding 2020-03 for additional information on this system for which it contracted in April 2020). Specifically:

- DES did not implement the mandatory requirement to cross-match claimants' immigration documents with Systematic Alien Verification for Entitlement data to verify immigration status until June 12, 2020. As of August 2021, DES still did not implement the other 2 mandated requirements to cross-match claimants with (1) quarterly wage records and (2) the National Directory of New Hires.
- Although DES implemented 4 of the 8 strongly recommended measures in May 2020, it did not implement another 2 of the strongly recommended measures until late June 2020 after it began paying CARES Act UI benefits claims from its new UI benefits system. Further, it did not implement a key strongly recommended measure that reduced a substantial amount of identity theft fraudulent claims until September 2020. As of August 2021, DES had still not implemented 1 strongly recommended measure to cross-match with the State Directory of New Hires. Specifically:
  - o On May 12, 2020, DES implemented the 4 strongly recommended measures to help identify if claimants have unemployment wages in another state, unidentified wages in another state, prevent concurrent claim filing in multiple states, and cross-matches related to individuals incarcerated in Arizona prisons and Maricopa County jails.
  - o Between June 20, 2020 and June 26, 2020, DES implemented 6 fraud alerts on its new UI system similar to the strongly recommended measure to use the DOL UI Integrity Center's Integrity Data Hub, such as restricting invalid email addresses and duplicate bank account numbers.
  - o On June 24, 2020, DES implemented the strongly recommended measure to verify claimants' identity with the Social Security Administration.
  - o Finally, on September 2, 2020, DES implemented the strongly recommended measure to use identity verification by implementing ID.me.

Effect—DES reported to us that it paid over $1.6 billion of federal CARES Act UI benefits in fiscal year 2020 to alleged fraudsters who had stolen identities. The $1.6 billion comprised nearly 3.5 million claims totaling over $379 million of PUA and over $1.2 billion of Federal Pandemic Unemployment Compensation (FPUC) CARES Act UI benefits. DES disbursed these monies during the period of May

18, 2020 through June 30, 2020, which included retroactive benefits for as far back as the week beginning January 27, 2020. An undeterminable portion of these fraudulent payments may have been prevented if DES had implemented all the critical identity-verification and other anti-fraud measures before making any CARES Act UI benefits payments. As of this report's issuance, DES estimated it paid $2.8 billion in fraudulent claims after June 30, 2020, through the end of the CARES Act UI benefits programs on September 4, 2021. Other states have also paid federal CARES Act UI benefits to alleged fraudsters who had stolen identities. For example, in May and July 2020, the U.S. Secret Service and the Federal Bureau of Investigation, respectively, reported increased fraudulent claims due to identity theft across various states.[4] Further, several other states' auditors, such as California, Kansas, Michigan, Mississippi, and Washington, reported significant dollar amounts of fraudulent UI benefits claims paid by their states.[5] For example, in a report dated February 2021, according to the Kansas Legislative Division of Post Audit, the Kansas Department of Labor could have paid $600 million in fraudulent UI benefits claims of roughly $2.6 billion in total UI benefits paid during the fiscal year ended June 30, 2020. In the same fiscal year, according to the Washington State Auditor, as of November 19, 2020, the Washington Employment Security Department estimated it paid known or probable fraudulent UI benefits claims totaling over $600 million of $7.5 billion in total UI benefits paid. Additionally, in its May 28, 2021, report, the DOL—Office of the Inspector General (DOL-OIG) reported, "Across the country, news and law enforcement agencies have reported unprecedented levels of UI fraud. In our CARES Act Alert Memorandum of February 22, 2021, we estimated potential fraud could range into the tens of billions of dollars."[6] As of this report's issuance, DES was continuing to evaluate claims paid to identify improper payments and expecting to recover some of the total improper payments it made through the help of law enforcement agencies. However, it reported that it did not expect to be required to return any unrecovered monies to the federal government. These fraudulent payments had no effect on the State's regular UI program that the State has jointly administered with the federal government for over 30 years because these same issues were not identified in that program.

Cause—Federal laws required states to ease claimant eligibility requirements for and access to CARES Act UI benefits.[7] DES reported that it initially interpreted the ease-of-access requirements to mean that it also needed to ease up identity verification and other anti-fraud measures for the CARES Act UI benefits programs by not putting into place measures that are required to be in place for regular UI claims payments. In addition, to receive CARES Act UI benefits, claimant eligibility self-certification was required, which was not allowed in the regular UI program.[8] This difference further contributed to DES' initial interpretation that identity verification and anti-fraud measures for the CARES Act UI benefits program were not a priority. Further, as mentioned earlier, DES was unable to use its regular UI benefits system for the new federal CARES Act UI benefits programs and therefore contracted to use a new system to quickly process claims, which took time to get online and ready to process its first CARES Act UI benefits claims. DES reported that it encountered computer programming issues interfacing with other State systems and federal databases to be able to conduct all the federally mandated and strongly recommended identity verification and other anti-fraud measures. Finally, DES also reported the speed with which it needed to process an increased volume of CARES Act UI benefits claims and confusion regarding federal laws, requirements, and guidance contributed to it not putting into place all critical identity verification and antifraud measures before it started paying benefits. Specifically:

- The number of UI benefits claims increased with the passage of the CARES Act. By way of illustration, our analysis of DES' UI systems' data found that Arizona's total unemployment compensation benefits payments increased 2,119 percent during fiscal year 2020 as compared to fiscal year 2019. For the year ended June 30, 2020, DES paid unemployment compensation to claimants totaling $5.9 billion, comprising $873 million for regular UI benefits and $5.1 billion for CARES Act UI benefits. DES disbursed the entire $5.1 billion of CARES Act UI benefits payments in less than 3 months, from April 7, 2020 through June 30, 2020.
- The DOL issued updated guidance for the CARES Act UI programs several times while states were paying UI benefits claims. For example, according to a DOL-OIG report, the DOL clarified statements on states' responsibilities for program integrity in 10 guidance documents it issued between April 2, 2020 and June 6, 2020.[9]

Criteria—Developing and implementing control activities to achieve objectives and respond to risks, including the risks of fraudulent identity theft claims for UI benefits, is an essential part of internal control standards, such as the *Standards for Internal Control in Federal Government* issued by the Comptroller General of the United States, and integral to ensuring that federal assistance monies are not improperly paid to fraudulent claimants.[10] In addition, on the noted dates, the federal government issued guidance related to anti-fraud measures applicable to the CARES Act UI benefits. Specifically:

- On April 5, 2020, the DOL's PUA implementation instructions reminded states that they were required to take reasonable and customary precautions to deter and detect fraud. [3]
- On May 11, 2020, the DOL issued guidance specifying 3 mandated and 8 strongly recommended identity theft and anti-fraud measures for CARES Act UI benefits.[1]

Recommendations—DES should:

1. Continue to evaluate the CARES Act UI benefits it has paid to identify any additional fraudulent claims payments, using all necessary critical identity verification and other anti-fraud measures.
2. Continue its efforts working with law enforcement agencies to recover improper payments for fraudulent claims it paid due to identity theft, to the extent practicable.
3. Repay any recovered improper payments to the federal government.
4. Develop and implement a plan to ensure that for any future new UI benefits programs or regular UI benefits program changes, it puts critical identity verification and other anti-fraud measures in place prior to paying any UI benefits claims.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

[1] U.S. Department of Labor, Office of the Inspector General (May 11, 2020). *Unemployment Insurance Program Letter No. 23-20. https://wdr.doleta.gov/directives/attach/UIPL/UIPL_23-20.pdf*.

[2] In response to the Novel Coronavirus Disease of 2019 (COVID-19) pandemic, on March 27, 2020, the United States Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act (Public Law 116-136), which expanded unemployment insurance through new federally funded programs to provide economic relief to individuals who were unable to work because of the COVID-19 pandemic and established the Pandemic Unemployment Assistance (PUA), Pandemic Emergency Unemployment Compensation (PEUC), and Federal Pandemic Unemployment Compensation programs (FPUC). The PUA program, which provided unemployment compensation through December 31, 2020, to individuals who were not traditionally eligible for benefits under regular UI programs, such as those who were self-employed workers, independent contractors, and gig-economy workers, those with limited work history, and certain other workers whose employment was affected by the COVID-19 pandemic. This program provided claimants with a minimum weekly benefit, pursuant to each state's unemployment compensation law, and anything above Arizona's minimum weekly benefit of $117—up to $240 total per week in Arizona—would require wage verification. In addition, the FPUC program supplemented $600 to the weekly benefits an individual may receive under regular UI or PUA through July 31, 2020, provided they were eligible to participate in the UI programs. CARES Act, Public Law 116-136, Title II, Subtitle A (2020).

[3] U.S. Department of Labor, Office of the Inspector General (April 5, 2020). *Unemployment Insurance Program Letter No. 16-20. https://wdr.doleta.gov/directives/attach/UIPL/UIPL_16-20.pdf*.

[4] Pandemic Response Accountability Committee. (2020). *Massive Fraud Against State Unemployment Insurance Programs*, May 15, 2020 (Source: Security Federal Savings Bank) and FBI Press Release: *FBI Sees Spike in Fraudulent Unemployment Insurance Claims Filed Using Stolen Identifies*, July 6, 2020 (Source: Identity Theft in Pandemic Benefits Programs | Pandemic Oversight). Retrieved 8/31/2021 from https://www.pandemicoversight.gov/our-mission/identity-theft-inpandemic-benefits-programs.

[5] Auditor reports on other states that included findings relating to CARES Act UI benefits were retrieved on 9/13/2021 at the following links: California: https://www.auditor.ca.gov/reports/2020-628.2/summary.html. Kansas: https://www.kslpa.org/audit-report-library/evaluating-the-kansas-department-of-labors-response-to-covid-19-unemployment-claims-part-1/. Michigan: https://audgen.michigan.gov/wp-content/uploads/2021/07/MIUNEM-Comp-Fund-SA-Report-Final.pdf (finding number 2020-004 on page 13). Mississippi: https://www.osa.ms.gov/documents/single-audit/20sar.pdf (finding number 2020-007 on page 69) Washington: https://sao.wa.gov/performance_audit/washingtons-unemployment-benefit-programs-in-2020/ and https://ofm.wa.gov/accounting/financial-audit-reports/single-audit-report/2020-single-audit-report (financial statement finding reported under Government Auditing Standards, number 2020-001 on page E – 19).

[6] U.S. Department of Labor, Office of the Inspector General (May 28, 2021). *COVID-19: States Struggled to Implement CARES Act Unemployment Insurance Programs*, Report Number 19-21-004-03-315. https://www.oig.dol.gov/public/reports/oa/2021/19-21-004-03-315.pdf.

[7] On March 18, 2020, the Families First Coronavirus Response Act (Public Law 116-127) authorized the Emergency Unemployment Insurance Stabilization and Access Act, which provided emergency administration and response by allowing states to ease eligibility requirements and access to unemployment compensation for claimants, including waiving the waiting week and work-search activity requirements.

[8] The CARES Act (Public Law 116-136), Section 2102(a)(3)(A) provided the criteria for which an individual self-certifies eligibility for PUA under the Presidentially declared public health emergency resulting from the COVID-19 pandemic. The self-certification required claimants to self-declare that they were eligible for the PUA program and were able to work and available for work but unable to do so because of at least 1 specific, qualifying COVID-19-related reason. In addition, the CARES Act, §2102(h), applied the Disaster Unemployment Assistance program's administrative requirements to PUA since PUA was similar to unemployment compensation provided under Presidentially declared disasters.

[9] U.S. Department of Labor, Office of the Inspector General (August 7, 2020). *COVID-19: More Can Be Done to Mitigate Risk to Unemployment Compensation Under the CARES ACT*, Report Number 19-20-008-03-315. https://www.oig.dol.gov/public/reports/oa/2020/19-20-008-03-315.pdf.

10 U. S. Government Accountability Office. (2014). *Standards for internal control in the federal government*. Washington, DC. Retrieved 8/4/2021 from https://www.gao.gov/assets/670/665712.pdf.

Agency Response: Concur

Agency: Department of Economic Security
Name of contact person and title: Bryce A. Barraza, DERS Deputy Assistant Director

Anticipated completion date: June 2022

As of the issuance of this report, the Department of Economic Security (DES) paid an estimated total of $4.4 billion in fraudulent claims, and estimates to have ultimately prevented over $75 billion in benefit payments to perpetrators of identity theft through the development and implementation of various prevention and fraud detection measures. Throughout the pandemic, DES deployed various system fraud controls and integrity measures that were required or identified as industry best-practices to mitigate and prevent the unprecedented criminal and fraudulent activity experienced across the nation. Unemployment Insurance Program Letter (UIPL) No. 23-20 was released by the U.S. Department of Labor (DOL) on May 11, 2020. In this UIPL, states were instructed to implement three mandatory Benefit Payment Control (BPC) integrity activities for two of the CARES Act programs: the Pandemic Emergency Unemployment Compensation (PEUC) program and the Pandemic Unemployment Assistance (PUA) program. However, this UIPL did not stipulate a timeframe for the three mandatory activity implementations, only that these activities be implemented in the same manner as for the regular Unemployment Insurance (UI) program. DES took steps to implement these three mandatory integrity activities as follows:

- By June 12, 2020, one month after the release of UIPL 23-20, DES successfully implemented the mandatory activity pertaining to the Systematic Alien Verification for Entitlement (SAVE) for the three CARES Act programs--PEUC, PUA, and the Federal Pandemic Unemployment Compensation (FPUC) program.
- The two remaining mandatory activities pertaining to new hire wage crossmatching (National Directory of New Hires (NDNH) and Quarterly) were implemented within the regular unemployment insurance system for claimants at the start of the PEUC and FPUC programs.
- DES continues to work closely with its two vendors to implement the new hire and quarterly wage records crossmatch within the PUA portal system for PUA program claimants, including FPUC program payments.

It is important to note that the DOL identified only three mandatory BPC activities. The other eight integrity functions identified in UIPL 23-20, while important, are not federally mandated and therefore are strongly recommended by the DOL but not enforced. DES has been able to implement all eight of these functions for the PEUC program, and seven of these functions for the PUA program. DES will address the audit recommendations, as follows:

1. Continue to evaluate the CARES Act UI benefits it has paid to identify any additional fraudulent claim payments, using all necessary critical identity verification and other anti-fraud measures.

DES will continue efforts to identify any additional PUA fraudulent claim payments, in part by implementing the Quarterly, NDNH, and State Directory of New Hires (SDNH) wage cross-match. DES will also continue to participate in a number of integrity cross-matches, which include, but are not limited to, the Arizona Department of Corrections and Maricopa County Jail, to detect individuals filing for UI benefits while incarcerated. In addition, the DES Office of Inspector General (OIG) provides additional information regarding local, state, and federal incarceration records to the DES Division of Employment & Rehabilitation Services for processing. Continuing to conduct a Social Security Cross-match, Motor Vehicle Division (MVD) Verification, Social Security Number (SSN) check via the UI Interstate Connection Network (ICON), and a U.S. Department of Health and Human Services (DHHS) and Social Security Administration (SSA) Mortality record check. DES utilizes the Integrity Data Hub (IDH) through the OnPoint Fraud Detection Solution which consists of IDH Suspicious Actor Repository (SAR) cross-match, ID Theft, and Fictitious Employer. DES put in place a number of upfront measures that check for repetitive information, trends, and crossclaimant repetition used to identify potentially fraudulent activity. DES will continue to utilize these successful anti-fraud measures to identify any additional fraudulent claim payments.

2. Continue to work with law enforcement agencies to recover improper payments for fraudulent claims it paid due to identity theft, to the extent practicable.

DES continues to partner with federal, state, and local law enforcement agencies and financial institutions across the country to recover losses and aggressively pursue legal action against perpetrators of fraud. Throughout the pandemic, and as of September 2021, the Department has partnered with more than 200 financial institutions and over 100 law enforcement agencies that include the FBI, the DOL, the U.S. Secret Service, and the U.S. Department of Homeland Security. DES has also developed internal fraud indicators, investigated over 64,000 identity theft fraud complaints received from the DES OIG fraud hotline/website, developed a fraud scoring model in partnership with Google Analytics and Spring ML data analytics, and implemented the OPTimum Aware fraud detection software solution. As of September 2021, these efforts have recovered more than $1.4 billion in benefit payments for fraudulent claims. In addition, DES has been able to prevent more than an estimated $75 billion in benefit payments to perpetrators of identity theft through the development and implementation of various prevention and fraud detection measures. Further, over 200

cases have been submitted to the Arizona Attorney General's Office for prosecution, and more than 100 have resulted in criminal charges.

3. Repay any recovered improper payments to the federal government.

In accordance with federal and state rules and regulations, DES has a well-established business practice of performing the detection, recovery and repayment functions as required for the regular UI program. DES has performed these functions for the PEUC program since its onset, and is working toward implementing these functions for the PUA program as well.

4. Develop and implement a plan to ensure that for any future new UI benefits programs or regular UI benefits program changes it puts critical identity verification and other anti-fraud measures in place prior to paying any UI benefits claims.

In addition to other integrity measures already in use, DES will continue to utilize the third-party ID.me application and leverage the identity verification tool across any future new UI Benefit programs. In addition, any new UI benefit programs will be implemented in alignment with federal law and guidance, and where applicable, anti-fraud measures identified as successful during the CARES Act program will be adopted in our standard work and put in place prior to paying any UI benefit claims.

2020-02

Department of Economic Security paid claimants an estimated $57 million of federal Pandemic Unemployment Assistance benefits that exceeded the minimum weekly benefit but has not yet determined whether claimants qualified for them as required; therefore, it does not know how much in potential overpayments it may have paid and would need to recover Department of Economic Security paid claimants an estimated $57 million of federal Pandemic Unemployment Assistance benefits that exceeded the minimum weekly benefit but has not yet determined whether claimants qualified for them as required; therefore, it does not know how much in potential overpayments it may have paid and would need to recover

Condition—Between May 8, 2020 and June 30, 2020, as allowed by federal regulations, the Department of Economic Security (DES) reported that it paid claimants an estimated $57 million of federally funded Pandemic Unemployment Assistance (PUA) benefits above the minimum weekly unemployment insurance (UI) benefit, but DES did not determine whether claimants were qualified to receive these additional PUA benefits. Claimants were eligible to receive PUA benefits monies above the State of Arizona's minimum weekly UI benefit of $117, up to $240 weekly, if when they applied, they self-certified that their wages qualified them and, within 21 days after applying, they provided documents to support their wages, which DES was supposed to immediately review to verify the accuracy of the claimants' weekly benefit amount. However, DES did not determine whether those claimants had submitted wage documentation within 21 days of applying, as required. Further, for those claimants paid above the State's $117 weekly minimum UI benefit who did not provide wage documents within 21 days, DES did not immediately reduce the claimants' future weekly benefit payments to the $117 weekly minimum as required and determine how much it had overpaid those claimants. In addition, for those claimants who submitted wage documents, DES did not evaluate the wage documents to determine if and how much in benefits it overpaid those claimants above the weekly minimum. As of August 2021, DES reported that for those claimants who submitted wage documents, it had not yet completed evaluating the wage documents to determine if and how much in benefits it overpaid those claimants above the weekly minimum between May 8, 2020 and June 30, 2020.

Effect—DES was unable to determine how much of the estimated $57 million of PUA benefits it paid above the $117 weekly minimum UI benefit may have been overpayments to claimants, which it would then need to recover from them. Since DES had not determined the overpayments, it did not make any adjustments to the State's Unemployment Compensation Fund's applicable financial statement amounts as required by U.S. generally accepted accounting principles. Therefore, we qualified our fiscal year 2020 financial statement opinion over the Unemployment Compensation Fund's other receivables and amounts due to the U.S. government financial statement line items reported in the State's *Comprehensive Annual Financial Report,*[1] as described in financial statement finding 2020-03. Further, DES' required return of these overpaid monies to the federal government is delayed until DES determines the amount of overpayments and collects them from the overpaid claimants. Because this issue applies only to the PUA program, this finding has no effect on the State's regular UI program that the State has jointly administered with the federal government for over 30 years. reported that the system did not have an alert to notify it of claimants who were receiving more than the minimum weekly UI benefit amount but had not submitted wage documentation within 21 days of applying. In addition, DES also reported it did not initially have the staff needed to process the volume of CARES Act UI benefits claims. The number of UI benefits claims increased with the passage of the CARES Act. By way of illustration, our analysis of DES' UI systems' data found that Arizona's total unemployment compensation benefits payments increased 2,119 percent during fiscal year 2020 as compared to fiscal year 2019. For the year ended June 30, 2020, DES paid

unemployment compensation to claimants totaling $5.9 billion, comprising $873 million for regular UI benefits and $5.1 billion for CARES Act UI benefits. DES disbursed the entire $5.1 billion of CARES Act UI benefits payments in less than 3 months, from April 7, 2020 through June 30, 2020.

Criteria—Federal regulations prescribe the PUA program requirements that apply to claimants and that DES must follow.[2] Specifically, federal regulation states that claimants who are eligible to participate in the PUA program are entitled to receive the State's minimum weekly UI benefit—$117 in Arizona—and claimants may receive an increased PUA weekly benefit amount up to a maximum—$240 in Arizona—if the claimant submits wage documentation within 21 days of applying.[3,4] Federal regulations require states to determine and immediately pay a weekly benefit amount based on the claimants' self-certification of eligibility and wages contained in the claimants' application. Claimants who self-certify for more than the minimum weekly benefit amount are required to submit wage documentation within 21 days of applying for the additional weekly PUA benefit, and states are then required to immediately determine the accuracy of each claimant's weekly benefit amount based on the claimant's submitted wage documentation.[3,4] For claimants who did not submit the required wage documentation within 21 days of applying, federal regulation requires states to immediately reduce the claimants' future benefit payments to the minimum weekly benefit amount and consider PUA payments exceeding the minimum weekly benefit as overpayments.[4] In addition, federal regulation requires states to take all reasonable measures under state and federal laws to recover overpayments to claimants, regardless of whether the overpayment resulted from error or fraud on the claimant's part.[5] Finally, designing control activities, including those for its information system, to achieve program objectives and respond to risks is an essential part of internal control standards, such as the *Standards for Internal Control in Federal Government* issued by the Comptroller General of the United States, and integral to ensuring benefit payments are provided to only those who are eligible to receive them.[6]

Recommendations—DES should:

1. Perform wage verifications for all claimants who received an increased PUA weekly benefit payment to determine the weekly benefit amount they qualified for and identify and recover any overpayments.
2. Repay any PUA program overpayments received from claimants to the federal government.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

[1] Arizona Department of Administration. (2020). *Comprehensive Annual Financial Report, June 30, 2020*. Phoenix, AZ. This report includes our financial statement opinion in which we reported DES estimated its overpayments above the minimum weekly benefit were $116 million, but DES later revised its estimate to be $57 million.

[2] On March 27, 2020, the CARES Act, Section 2102(a)(3)(A), provided the criteria for which an individual self-certifies eligibility for PUA under the Presidentially declared public health emergency resulting from the COVID-19 pandemic. The self-certification required claimants to self-declare that they were eligible for the PUA program and were able to work and available for work but unable to do so because of at least 1 specific, qualifying COVID-19-related reason. In addition, the CARES Act, §2102(h), applied the Disaster Unemployment Assistance program's administrative requirements to PUA, since PUA was similar to unemployment compensation provided under Presidentially declared disasters.

[3] 20 Code of Federal Regulations §625.6(e).

[4] U.S. Department of Labor, Office of the Inspector General (April 27, 2020). *Unemployment Insurance Program Letter No. 16-20, Change 1, Attachment I, Question 20. https://wdr.doleta.gov/directives/attach/UIPL/UIPL_16-20_Change_1.pdf.*

[5] 20 Code of Federal Regulations §625.14[a].

[6] U.S. Government Accountability Office. (2014).

Agency Response: Concur

Agency: Department of Economic Security
Name of contact persons and titles: Sandra Canez, Unemployment Insurance Program Administrator
Jacqueline Butera, Quality Assurance and Integrity Administrator
Anticipated completion date: October 2021

The Department of Economic Security (DES) will continue efforts to address the audit recommendations, as follows:

1. Perform wage verifications for all claimants who received an increased Pandemic Unemployment Assistance (PUA) weekly benefit payment to determine the weekly benefit amount they qualified for and identify and recover any overpayments.

DES issued initial eligibility and Weekly Benefit Amount (WBA) determinations in accordance with 20 CFR 625.6(e), using claimants' self-reported base period income provided at the time of initial application, in addition to the record of wages that DES had on file. Throughout fiscal year 2020, the U.S. Department of Labor's (DOL) interpretation of the CARES Act was that self-certification was sufficient in and of itself to calculate the WBA. Unemployment Insurance Program Letter (UIPL) No. 16-20, Change 1 (issued April 7, 2020), states that PUA is not like DUA, in that it does not require proof of employment, but if an individual fails to provide wage documentation within 21 days, the individual's WBA must be reduced. DES began in-depth business requirement discussions with its vendor to address the system functionality requirements in August 2020. In December 2020 through February 2021, DES also developed standard work and training material regarding monetary eligibility for PUA. Team members were trained, and claim processing specific to claims with a WBA higher than $117 was initiated in March 2021. DES will continue to follow the standard quality review process for the claims being processed. Due to lack of system functionality within the PUA portal, DES has been unable to process the WBA decrease(s). System functionality is anticipated to be available in October 2021 which will support the recalculation and decrease in benefit amount.

2. Repay any PUA program overpayments received from claimants to the federal government.

In accordance with federal and state rules and regulations, DES has a well-established business practice of performing the detection, recovery, and repayment functions as required for the regular UI program. DES is working toward implementing these functions for the PUA program as well.

2020-03
Department of Economic Security excluded and initially reported inaccurate financial information, which could have misinformed financial statement users

Condition—Contrary to U.S. generally accepted accounting principles (GAAP), the Department of Economic Security (DES) excluded and initially reported inaccurate Unemployment Compensation Fund financial statement amounts to the Arizona Department of Administration (ADOA) to include in the State's fiscal year 2020 financial statements, which are included in the State's *Comprehensive Annual Financial Report*.[1] DES' exclusion and initial inaccuracies, as described below, were related to 2 new federal CARES Act unemployment insurance (UI) benefits programs developed in response to the COVID-19 pandemic's unemployment increase—the Pandemic Unemployment Assistance (PUA) and Federal Pandemic Unemployment Compensation (FPUC) programs. First, related to the federally funded PUA program, DES did not report to ADOA for inclusion in the State's fiscal year 2020 financial statements the receivables and amounts due to the U.S. government for possible overpayments to claimants who were eligible for the State's $117 minimum weekly UI benefit but were paid more than that minimum—up to $240 a week. As discussed in Finding 2020-02, DES paid these claimants an estimated $57 million of PUA monies in fiscal year 2020 but did not determine how much of these monies may have been overpayments to claimants who were not qualified to receive them. Further, DES did not make any financial statement adjustments for these potential overpayments. Second, DES made 3 errors totaling $579 million that, based on our discovery and subsequent recommendations, it corrected for the State's final financial statements. Specifically, DES:

- Excluded $534 million of expenditures and payables for PUA and FPUC benefit claims due to eligible individuals before June 30, 2020, but that it had not paid as of June 30, 2020.
- Misreported $22.1 million of grant revenues and benefit expenses for PUA claims that were canceled before being paid and should have been reported as cash and unearned revenue.
- Excluded $22.9 million in receivables from PUA claimants who DES paid benefits to but later determined to be ineligible, which is then owed to the U.S. government when collected.

Effect—DES not reporting to ADOA how much of the estimated $57 million in its Unemployment Compensation Fund was overpayments and should be included in the State's financial statements for fiscal year 2020 resulted in our reporting a qualified opinion on the State's Unemployment Compensation Fund's other receivables and amounts due to the U.S. government financial statement line items because those line items may have been materially misstated and could misinform someone relying on the financial information. In addition, the State's initial fiscal year 2020 Unemployment Compensation Fund's financial statement amounts related to the PUA and FPUC programs including errors totaling approximately $579 million could have misinformed financial statement users about the actual benefit amounts paid and owed to claimants and the U.S. government when collected by DES if we had not discovered and DES had not corrected those errors.

Cause—DES did not report to ADOA how much of the estimated $57 million of PUA payments was overpayments because DES did not determine the amount of overpayments and, therefore, the amount it would need to collect from overpaid claimants and remit to the

U.S. government. Further, during the audit, we determined that the new UI benefits system DES contracted to process the FPUC and PUA benefits claims had a programming error that contributed to DES initially reporting the errors totaling $579 million. Specifically, DES relied on the contractor's system-generated reports without verifying those reports included accurate summarized system data and amounts that reconciled to external sources, such as canceled and returned claimant payments reported by DES' servicing bank. During the audit, we discovered the programming error.

Criteria—U.S. GAAP requires that amounts be reported within the financial statement in the year the underlying transactions occurred that resulted in revenues, expenditures, monies being receivable to the State, such as monies owed by overpaid claimants, and monies payable to outside entities, such as the federal government. Therefore, DES must correctly report these amounts to ADOA. To do so, DES has a responsibility to implement internal controls to provide reasonable assurance over the reliability of the State's reported financial information. Accurate financial statements provide valuable information to those charged with the State's governance, management, and others who are relying on the reported financial information to make important decisions about the State's financial operations. Complete and accurate information is an essential part of internal control standards, such as the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States, and integral to ensuring financial information is accurately reported.[2]

Recommendation—DES should:

1. Implement the recommendations reported in financial statement finding 2020-02.
2. Implement a process to ensure its Unemployment Compensation Fund financial information over the PUA and FPUC federal unemployment insurance programs is reported to ADOA for inclusion in the State financial statements in accordance with U.S. GAAP.
3. Establish policies and procedures to ensure its contractor's system used to process PUA and FPUC claims produces reports that are complete and accurate and include procedures that detail how to utilize system report information to determine amounts needed for the State's financial statements. Procedures over the system reports should include ensuring daily the accuracy of system data and generated reports, verifying the system reports against detailed system data, and determining the accuracy of detailed system data by reconciling it to external sources when possible.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

[1] Arizona Department of Administration. (2020). *Comprehensive Annual Financial Report, June 30, 2020*. Phoenix, AZ.
[2] U.S. Government Accountability Office (GAO). (2014). *Standards for internal control in the federal government*. Washington, DC. Retrieved 8/4/21 from https://www.gao.gov/assets/670/665712.pdf.

Agency Response: Concur

Agency: Department of Economic Security
Name of contact person and title: Kristopher Goins, Senior IT Project Manager
Anticipated completion date: March 2022

The Department of Economic Security (DES) will continue efforts to address the audit recommendations, as follows:

1. Implement the recommendations reported in financial statement finding 2020-02.

DES will implement the necessary changes as outlined in the response to financial statement finding 2020-02 as it relates to this finding.

2. Implement a process to ensure its Unemployment Compensation Fund financial information over the PUA and FPUC federal unemployment insurance programs is reported to ADOA for inclusion in the State financial statements in accordance with U.S. GAAP.

DES has enhanced existing standard work to include procedures incorporating Unemployment Compensation Fund financial information from the new federal Unemployment Insurance PUA and FPUC programs to ensure that DES submits the related applicable financial information to ADOA for inclusion in the State financial statements in accordance with U.S. GAAP. Internal Provided By Client

(PBC) Memos have been updated to include requests for applicable PUA and FPUC financial activity. Procedures for developing internal UI financial statements have been updated to ensure applicable PUA and FPUC financial activity is accounted for. Procedures for internal review of final financial statements have been updated to ensure review of applicable PUA and FPUC financial activity.

3. Establish policies and procedures to ensure its contractor's system used to process PUA and FPUC claims produces reports that are complete and accurate and include procedures that detail how to utilize system report information to determine amounts needed for the State's financial statements. Procedures over the system reports should include ensuring daily the accuracy of system data and generated reports, verifying the system reports against detailed system data, and determining the accuracy of detailed system data by reconciling it to external sources when possible.

DES will establish policies and procedures to ensure its contractor's system produces complete and accurate reports as recommended. DES has already worked with its contractor to make several enhancements to ensure all transactions associated with a payment are recorded in a manner that allows for reconciliation and that there are no payments or cancels that remain unaccounted for. Additionally, DES is creating a request to enhance the financial reporting process to perform regular reconciliations to ensure that the system and the PUA accounts are balanced. This will allow DES the ability to perform regular validations on the system accounting process.

2020-04
The Department of Revenue did not ensure it collected all income taxes that are due to the State, increasing the risk that the State may not receive all of its income tax revenues

Condition—Contrary to State law, the Department of Revenue (DOR) failed to perform necessary reconciliations to ensure it collected all income taxes due to the State. This finding has been reported since fiscal year 2006.

Effect—DOR may not collect all income taxes that are due, increasing the risk that the State may not receive all its income tax revenues. Also, the State risks reporting inaccurate income tax revenue in its financial statements.

Cause—DOR's tax administration system lacked the functionality to perform certain automatic reconciliations, and DOR did not implement an alternative process.

Criteria—State law requires that DOR administer and enforce Arizona income tax laws, which includes collecting income tax. The *State of Arizona Accounting Manual* requires that State agencies reconcile relevant activity.

Recommendations—DOR should perform necessary reconciliations to ensure it collects all income tax due from taxpayers by addressing its system's limitations or implementing an alternative process.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

This finding is similar to prior-year finding 2019-04.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Mike Devine, ADOR Chief Internal Auditor
Anticipated completion date: December 2020

In December 2020, the Department completed a pilot project aimed at collecting and capturing W-2 and Form 1099 data and developing a tool to perform a reconciliation process for withholding and individual income taxes and will use this tool beginning with the 2021 tax year.

2020-05
The Department of Revenue did not publish $18.5 million of unclaimed individual income tax overpayments dating back as far as 2007, and they were not readily available for taxpayers to search and claim

Condition—Contrary to State law, the Department of Revenue (DOR) did not include $18.5 million of individual income tax overpayments in its unclaimed property system that is used to publish abandoned property on its website for taxpayers to search and claim. These overpayments from 46,163 taxpayer accounts ranged from $50 to $269,953 and dated back as far as fiscal year 2007. Taxpayers have approximately 35 years to file a claim for abandoned property. Arizona Revised Statutes (A.R.S.) §44-317[E])

Effect—Abandoned individual income tax overpayments totaling $18.5 million were not published on DOR's website and therefore were not readily available for individual taxpayers to search and claim.

Cause—DOR's tax administration system lacked the functionality to automatically transfer individual income tax overpayments from that system to its unclaimed property system, and DOR did not implement an alternative process to publish abandoned individual income tax overpayments.

Criteria—State laws require DOR to publish information about all abandoned property of at least $50 on its website, including information about unclaimed individual income tax overpayments. (A.R.S. §§44-309 and 44-317[E])

Recommendations—DOR should:
1. Publish all individual income tax overpayments of at least $50 on its website for taxpayers to search and claim.
2. Address its system's limitations or develop an alternative process to ensure overpayments of income tax are transferred to its unclaimed property system.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

This finding is similar to prior-year finding 2019-05.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Mike Devine, ADOR Chief Internal Auditor
Anticipated completion date: Unknown

As noted in the finding, issues with ADOR's tax administration system currently prevent the Department from transferring overpayments to the unclaimed property system. However, information regarding these overpayments is still accessible by taxpayers that call in to the Department. In February 2020 the Department contracted for a feasibility study for replacing the tax administration system, which assessed the Department's current tax system, developed the scope of work necessary for procuring a new tax system, and identified funding options for the new tax system. The Department will use the feasibility study to develop a budget request for a new tax system in the 2023 legislative session. Additionally, as a part of the initiative to replace the existing system, the Department is currently engaged in a data cleanup project that includes addressing abandoned overpayments.

2020-06
The Department of Revenue did not initially report $788 million of income tax revenue, which could have misinformed financial statement users

Condition—The Department of Revenue's (DOR) Financial Services Section did not report $788 million of $5.77 billion of fiscal year 2020 income tax revenue to the Arizona Department of Administration (ADOA) to include in the State's fiscal year 2020 financial statements. If uncorrected, ADOA would have incorrectly reported these revenues in the State's fiscal year 2021 financial statements instead of in fiscal year 2020. However, DOR corrected the error after we discovered it.

Effect—The State's fiscal year 2020 income tax revenue in its draft financial statements was initially understated by $788 million, which would have caused the financial statements to indicate revenues were less than actual and could have misinformed financial statement users. This error would have also caused the State's fiscal year 2021 income tax revenue to be overstated.

Cause—DOR did not have a process in place to ensure fiscal year 2020 income tax revenues it received after fiscal year-end—primarily because the State extended the income tax filing deadline due to the COVID-19 pandemic—were correctly reported to ADOA.

Criteria—U.S. generally accepted accounting principles require that revenues reported in governmental financial statements be reported in the correct fiscal year. Therefore, DOR's Financial Services Section must correctly report revenues to ADOA.

Recommendations—DOR should implement a process to ensure income tax revenues it receives after fiscal year-end are reported to ADOA for inclusion in the correct fiscal year's State financial statements.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency's response: Concur

Agency: Department of Revenue
Name of contact person and title: Mike Devine, ADOR Chief Internal Auditor
Anticipated completion date: October 1, 2021

To address this issue, the Department of Revenue's Financial Services section has made a change to its year-end reporting process. Specifically, the Department has added a step to identify the amount of revenue collected in the first two months of each new fiscal year that is generated due to revenue accruals of the tax year prior to the current calendar year. This amount will be reported to ADOA on or around October 1 of each fiscal year.

2020-07
Four State agencies had deficiencies in their processes for managing and documenting IT risks, which may put operations and IT systems and data at unintended and unnecessary risk of potential harm

Condition—We reviewed the risk-assessment process at 4 State agencies including the Departments of Administration (ADOA), Economic Security (DES), Child Safety (DCS), and Revenue (DOR) and found that DES' and DOR's processes for managing and documenting their risks did not include an overall risk assessment process that included identifying, analyzing, and responding to the agency-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Additionally, we found that DCS used a DES program management system for which DES had not performed a risk assessment, and DCS did not coordinate with DES to ensure its program management system was properly evaluated for risks. Further, ADOA's, DES', and DCS' processes did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.

Effect—The State agencies' administration and IT management may put the agencies' operations and IT systems and data at unintended and unnecessary risk.

Cause—Because the State's risk-assessment process is decentralized and managed at each agency, the agencies are in various stages of developing or implementing policies and procedures for assessing and managing risk and have not fully implemented agency-wide risk-assessment processes that address IT security.

Criteria—The State agencies should follow the State-wide IT policies established by the ADOA Arizona Strategic Enterprise Technology Office (ADOA-ASET), which is based on the IT security framework of the National Institute of Standards and Technology, to help effectively manage risk at State agencies. Effectively managing risk includes an entity-wide risk assessment process that involves members of the agencies' administration and IT management. The risk assessment should determine the risks the agencies face as it

seeks to achieve their objectives to not only report accurate financial information and protect their IT systems and data but to also carry out their overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the agencies might be subjected. To help ensure the agencies' objectives can be met, an annual risk assessment should consider IT risks. For each identified risk, the agencies should analyze the identified risk and develop a plan to respond within the context of the agencies' defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information.

Recommendations—The State agencies should:

1. Identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. (DES)
2. Plan for where to allocate resources and where to implement critical controls. (DES)
3. Ask responsible administrative officials and management over finance, IT, and other entity functions for input in the agencies' processes for managing risk. (DCS, DES, DOR)
4. Perform an annual entity-wide IT risk assessment that includes evaluating and documenting risks and safeguards. Such risks may include inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security. Work with ADOA-ASET, as needed, to perform and document an annual entity-wide IT risk assessment. (DCS, DES, DOR)
5. Evaluate and manage the risks of holding sensitive information by identifying, classifying, and inventorying the information the agencies hold to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations. (ADOA, DCS, DES)

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

This finding is similar to prior-year finding 2019-01.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Ashley Ruiz, Assistant Director
Anticipated completion date: Unknown

The State is actively working to correct all issues related to the managing and documenting of IT risks and identification, classification, and inventorying of sensitive information on the State's IT systems. Policy and procedures have been implemented or are being developed to address any gaps. Each agency has developed a detailed corrective action plan to address this finding and will work with Department of Administration-Arizona Strategic Enterprise Technology Office as needed to implement recommendations in accordance with State-wide prescribed policies and procedures.

2020-08
Three State agencies' control procedures over IT systems and data were not sufficient, which increases the risk that the agencies may not adequately protect those systems and data

Condition—We reviewed the access, configuration management, information technology (IT) security, and contingency-planning controls at the Departments of Administration (ADOA), Economic Security (DES), Child Safety (DCS), and Revenue (DOR) and found that ADOA's, DES', and DOR's control procedures were not sufficiently developed, documented, and implemented to respond to risks associated with their IT systems and data. DCS uses a DES program-management system and relies wholly on DES for configuration management, security, and contingency planning. The agencies lacked sufficient procedures over the following:

- **Restricting access**—Procedures did not consistently help prevent or detect unauthorized or inappropriate access to IT systems and data. (ADOA, DES, DOR)
- **Managing system configurations and changes**—Procedures did not ensure configuration settings were securely maintained and all IT system changes were adequately managed. (DES)

- **Securing systems and data**—IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss. (ADOA, DES, DOR)
- **Ensuring operations continue**—Contingency plan should include steps necessary for restoring operations in the event of a disaster or other system interruption. (ADOA, DES, DOR)

Effect—There is an increased risk that the State agencies may not adequately protect their IT systems and data, which could result in unauthorized or inappropriate access and/or the loss of confidentiality or integrity of systems and data. It also increases the agencies' risk of not being able to effectively continue daily operations and completely and accurately recover vital IT systems and data in the event of a disaster or system interruption.

Cause—Because the State is decentralized and IT systems and data are managed at each agency, the State agencies are in various stages of developing and implementing policies and procedures for access, configuration management, security, and contingency planning and have not fully implemented them.

Criteria—The State agencies should follow State-wide IT policies established by the ADOA Arizona Strategic Enterprise Technology Office (ADOA-ASET), which is based on the IT security framework of the National Institute of Standards and Technology, to implement effective internal controls that protect their IT systems and help ensure the integrity and accuracy of the data they maintain, as follows:

- **Restricting access through logical access controls**—Help to ensure systems and data are accessed by users who have a need, systems and data access granted is appropriate, and key systems and data access is monitored and reviewed. (ADOA, DES, DOR)
- **Managing system configurations and changes through well-defined, documented configuration management process**—Ensures the agencies' IT system configurations are documented and that changes to the systems are identified, documented, evaluated for security implications, tested, and approved prior to implementation. This helps limit the possibility of an adverse impact on the systems' security or operation. (DES)
- **Securing systems and data through IT security internal control policies and procedures**—Help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to their IT systems and data. (ADOA, DES, DOR)
- **Ensuring operations continue through a comprehensive, documented, and tested contingency plan**—Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption. (ADOA, DES, DOR)

Recommendations—The State agencies should:

1. Make it a priority to develop and document comprehensive IT policies and procedures and develop a process to ensure the procedures are being consistently followed. (ADOA, DES, DOR)
2. Work with ADOA-ASET on the ways to implement the audit recommendations. (ADOA, DES, DOR)

   Restricting access—To restrict access to their IT systems and data, the agencies should develop, document, and implement processes to:

3. Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities. (ADOA, DES, DOR)
4. Remove terminated employees' access to IT systems and data. (ADOA, DES, DOR)
5. Review all other account access to ensure it remains appropriate and necessary. (ADOA, DES, DOR)
6. Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts. (DES, DOR)
7. Enhance authentication requirements for IT systems. (DES, DOR)
8. Protect IT systems and data with session time-outs after a defined period of inactivity. (DES)

   Managing system configurations and changes—To configure IT systems securely and manage system changes, the agencies should develop, document, and implement processes to:

9. Establish and follow a documented patch management process. (DES)
10. Maintain configurations for all system services, assets, and infrastructure; manage configuration changes; and monitor the system for unauthorized or unintended configuration changes. (DES)

Securing systems and data—To secure IT systems and data, the agencies should develop, document, and implement processes to:

11. Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges. (ADOA, DOR)
12. Provide all employees ongoing training on IT security risks and their responsibilities to ensure systems and data are protected. (DES)
13. Ensure awarding and subsequent monitoring of IT vendor contracts is adequately conducted to ensure vendor qualifications and adherence to the vendor contract. (ADOA)

Ensuring operations continue—To ensure operations continue, the agencies should develop, document, and implement processes to:

14. Develop and implement a contingency plan, and ensure it includes all critical elements to restore critical operations, including being prepared to move critical operations to a separate alternative site if necessary. (ADOA, DOR)
15. Test the contingency plan. (DES, DOR)
16. Train staff responsible for implementing the contingency plan. (ADOA, DOR)

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

This finding is similar to prior-year finding 2019-02.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Ashley Ruiz, Assistant Director
Anticipated completion date: Unknown

The State is actively working to correct all issues related to the access of its IT resources and security of data on those IT systems. IT systems access and security of the IT data is of the utmost importance to the State. Policy and procedures have been implemented or are being developed to address any gaps. Each agency has developed a detailed corrective action plan to address this finding and will work with Department of Administration-Arizona Strategic Enterprise Technology Office as needed to implement recommendations in accordance with State-wide prescribed policies and procedures.

2020-09
The other auditors who audited the Public Safety Personnel Retirement System (PSPRS) reported the following internal control deficiency over PSPRS' financial statement compilation process for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements. PSPRS' and the State's 2020 financial statements were adjusted for all material misstatements noted

The other auditors who audited the Public Safety Personnel Retirement System (PSPRS) reported the following internal control deficiency over PSPRS' financial statement compilation process for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements. PSPRS' and the State's 2019 financial statements were adjusted for all material misstatements noted.

Condition—During fiscal year 2020, PSPRS did not use a fully functional accounting and financial reporting system. As a result, we identified multiple audit adjustments. Specific to the financial systems limitations, we noted the following:

- PSPRS' financial reporting database does not have a consolidated general ledger module.
- PSPRS' financial reporting database does not allow for accounting periods to be closed and locked from transactions and journal entries.
- PSPRS' financial reporting database does not have adequate journal entry approval controls or segregation of duties built into the system.

- PSPRS' financial reporting database does not allow for bank reconciliations to be accurately completed and reviewed in a timely, efficient manner.

Effect—PSPRS' internal controls over financial reporting of their financial statements were not designed and operating to ensure that a misstatement would be prevented or detected and corrected in a timely manner.

Cause—PSPRS' financial reporting system was created in house and was not designed to incorporate standard GL reporting functionality and controls. Management has not implemented sufficient controls to mitigate the risks posed by the financial reporting system's deficiencies.

Criteria—Management is responsible for designing, implementing, and maintaining internal controls that include controls over the general ledger, and complete and accurate financial statements.

Recommendations—PSPRS implemented a fully functional financial accounting system, which went live as of July 1, 2020. We recommend management continue to optimize the functioning of that system and incorporate it into all current and new accounting processes.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

This finding is similar to prior-year finding 2019-09.

Agency's Response: Concur

Agency: Public Safety Personnel Retirement System
Name of contact persons and titles: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: Unknown

Management will review the current General Ledger system functionality and implement effective internal controls to allow for accounting period closing, bank reconciliation functionality, and workflow capabilities that will improve segregation of duties. Additionally, procedures are currently being implemented to ensure journal entries are reviewed with documented approval by either the Controller or CFO.

2020-10

The other auditors who audited the PSPRS reported the following internal control deficiency over unreconciled balance sheet accounts for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements. PSPRS' and the State's 2020 financial statements were adjusted for all material misstatements noted

Condition—PSPRS did not reconcile cash or contributions receivable activity since implementing the financial reporting system module in 2018. As a result, we identified multiple audit adjustments.

Effect—Increased likelihood of unidentified errors and inaccurate investment account balances.

Cause—Turnover in key positions and lack of documented policies and procedures for month end and year-end closing. Additionally, the system's insufficient financial reporting functionality and account structure has made reconciliation of these accounts overly complex.

Criteria—Management is responsible for designing, implementing, and maintaining internal controls including controls over account reconciliations that ensure complete and accurate financial statements.

Recommendations—We recommend PSPRS review the current policies and procedures related to the reconciliation processes to ensure that all bank, investment, and receivable accounts are reconciled in a timely manner. These policies and procedures should include the establishment of deadlines, responsibility for completion, and independent supervisory review. Evidence of completion and review of the reconciliations should be documented.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency Response: Concur

Agency: Public Safety Retirement System
Name of contact persons and titles: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: Unknown

Policies and procedures are currently being implemented to ensure timely and accurate reconciliations of bank accounts and employer contribution revenues and receivables. These reconciliations will occur monthly and be reviewed by the Controller or CFO. We will also research the prior fiscal year balance to identify possible errors or needed adjustment entries.

2020-11
The other auditors who audited the PSPRS reported the following internal control deficiency over investment accounting for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements

Condition—Investment activity is only recorded to the general ledger at year-end. Additionally, it was noted that a complete monthly custodial bank reconciliation process has not been implemented. Lastly, external investment fund net asset values and related investment income and expenses are not reconciled monthly by fund between the custodial bank and external manager capital account statements.

Effect—Increased likelihood of unidentified errors and inaccurate investment account balances.

Cause—PSPRS does not have a formal investment accounting position and have not created and implemented routine investment accounting policies, procedures, and activities.

Criteria—Management is responsible for designing, implementing, and maintaining internal controls that include controls over account reconciliations, and complete and accurate financial statements.

Recommendations—We recommend PSPRS standardize and document investment-accounting procedures, including robust, timely reconciliation of investment balances, income, and expenses between the custody bank, external manager reporting, and general ledger.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency Response: Concur

Agency: Public Safety Retirement System
Name of contact persons and titles: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: Unknown

A new Investment Accountant position was filled in Investment Operations (IO) beginning in FY2021 and additional procedures were implemented with respect to both investment transaction and valuation reconciliations including monthly review of all investment transactions, LP unfunded commitment records, verification of all manager-reported account valuations to the BNY Mellon Bank (BNYM) book of record posting, and maintaining an internal log of any BNYM adjustments. The quarterly reported final valuations of all investment accounts will be provided to the Investment Team CIO and the respective Portfolio Managers for review and identification of any missing items after the cutoff date and also to review valuation data for reasonableness and completeness. Additional consideration will be given to add staff ensuring that a comprehensive and consistent investment reporting structure is established and maintained to coordinate with the Finance department for recording and reconciling investment activity in the general ledger.

2020-12

The other auditors who audited the PSPRS reported the following internal control deficiency over segregation of duties for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements

Condition—We noted that for portions of fiscal year 2020, due to turnover, the PSPRS accounting department included only two accountants, which created general segregation of duties concerns within the accounting department. We specifically identified segregation of duty concerns related to the processing of cash receipts and benefit payments.

Effect—A lack of segregation of duties results in an increased risk of fraud or error.

Cause—PSPRS experienced significant turnover throughout the fiscal year and PSPRS was not able to replace the number of positions timely. Additionally, certain processes were structured such that they did not provide for proper segregation of duties.

Criteria—Segregation of duties requires that no one employee have access to both physical assets and the related accounting records or to all phases of a transaction from initiation to recording.

Recommendations—We recommend PSPRS evaluate the most effective way to segregate various duties amongst the current staff and implement a supervisory review of the daily cash reconciliation and journal entry process as well as the payment of benefit payments. Where duties cannot be adequately segregated, mitigating controls should be designed and implemented. We also recommend PSPRS holistically evaluate all process flows in conjunction with general cash controls to develop efficient processes with appropriate segregation of duties and supervisory review.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency Response: Concur

Agency: Public Safety Retirement System
Name of contact persons and titles: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: Unknown

PSPRS Administrators understand the risk associated with unfilled positions in the accounting process. PSPRS has currently filled all Finance vacancies. Further, system capabilities are being reviewed and procedures established to properly control/segregate the functions of transaction processing and review/authorization processes.

2020-13

The other auditors who audited the Arizona Department of Transportation (ADOT) reported the following internal control deficiency over expenditure cutoff within the Other Governmental Funds, Enterprise Funds, and Internal Service Funds in the State's financial statements. ADOT's and the State's 2020 financial statements were adjusted for all material misstatements noted

Condition—During the course of our audit, we proposed and ADOT subsequently recorded adjustments to correct accounts payable/expenditures. As a result of audit procedures, we noted that 6 transactions were not recorded in the proper period totaling

$4,780,552. Additionally, ADOT had difficulties determining the accounts payable amounts for transactions processed through the Arizona Procurement Portal (APP).

Effect—The lack of controls in place over the review of subsequent disbursements increases the risk of misstatements or errors occurring and not being detected and corrected.

Cause—ADOT's internal control procedures failed to detect subsequent disbursements requiring accrual in the current audit period. In addition, the ADOT transactions processed through the APP system did not include service dates within the data, making it difficult to determine accounts payable at year-end.

Criteria—Internal controls should be in place to provide reasonable assurance that expenditures are recorded in the proper period in accordance with generally accepted accounting principles.

Recommendations—We recommend that ADOT implement policies and proper internal control procedures to ensure that expenditures are recorded in the proper period.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency Response: Concur

Agency: Department of Transportation
Name of contact person and title: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: Unknown

2020-14
The other auditors who audited ADOT reported the following internal control deficiency over accounts receivables and revenues for the State Aviation Fund that is reported within the Other Governmental Funds in the State's financial statements. ADOT's and the State's 2020 financial statements were adjusted for all material misstatements noted

Condition—ADOT did not have internal controls in place to ensure that receivables and revenues for aircraft registrations in the State Aviation Fund were properly recorded. As a result, an adjustment in the amount of $7,234,169 was necessary to reduce receivables and revenues at year end.

Effect—The lack of controls in place over the review of accounts receivable and revenues increases the risk of misstatements or errors occurring and not being detected and corrected.

Cause—ADOT was behind in recording adjustments within its accounting records to reflect the reduction of receivables for revenues that had been collected, resulting in an overstatement of revenues and receivables.

Criteria—Internal controls should be in place to provide reasonable assurance that accounts receivables and revenues are properly recorded in accordance with generally accepted accounting principles.

Recommendations—We recommend that ADOT implement policies and proper internal control procedures to ensure that receivables and revenues are properly recorded.

The State's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

Agency Response: Concur

Agency: Department of Transportation
Name of contact person and title: Tina Munoz, Financial Compliance Coordinator
Anticipated completion date: June 30, 2021

ADOT concurs with the finding and an adjustment was made to reduce receivables and revenues at year end. With new systems comes opportunity to validate our reconciliation processes and ensure we are capturing all receivables as we continue to monitor though out the year. Internally, ADOT will be performing a GEMBA with our RFTA and Aviation groups to better understand their systems.