November 2022

Transaction Supervisors' Forum Notes

Table of Contents

SURVEY QUESTIONS:

The following questions are submitted prior to the forum via Survey Monkey.

- **Question**: Is there a notification Human Resource (HR) offices or personnel specialist receive from CalPERS when an employee submits a retirement application? If so, where can I find it? And if not, why and can CalPERS create one?

  Answer: HR offices can check their employee's retirement status by logging into MyCalPERS and inputting the employee's information. The State Controller's Office recommends that the HR specialist review the Separation Checklist for Personnel Specialists which shows examples of how to locate this information in MyCalPERS.

- **Question**: In the last Transaction Supervisors' Forum, it was mentioned that SCO and maybe CalHR might bring back in-person training after the Covid-19 State of Emergency is lifted. As of October 2022, Governor Gavin Newsom announced that the COVID-19 State of Emergency will end on February 28, 2023. Are any preparations being done to get a jump start on in-person trainings starting March 2023, and can Personnel Specialist hired during this Covid-19 State of Emergency get first priority in registering?

  Answer: We are in the early stages of planning before any return to in-class training. Meanwhile, we will continue to provide virtual instructor-led training along with self-paced eLearning modules. While many of you would prefer that we return to training the old way, we hope you have noticed that "distance learning" gets more training to more people sooner than we were able to offer before, and less wasted time. The future of training will be primarily virtual training and eLearning, supplemented by in-class training when needed to solve learning issues.

- **Question**: Why does it take months for an Accounts Receivable (AR) to be established but only one day for us to respond to a Ding (PR 250) notice? Sometimes additional information is requested, and research needs to be done. Can the one day be changed to three business days or more?

  Answer: Since 11/1/2022-11/14/2022 the SCO Personnel and Payroll Operations Bureau has received over 3,900 AR requests. On a monthly basis, the SCO averages over 6,000 AR requests. We are doing our best to get through the documents but there are more HR offices submitting

documentation then we have staff. The Ding notices (PR 250) have a two day response time. We appreciate your understanding.

- **Question**: How can I request a duplicate Personnel Action Request (PAR) for an employee if I did not receive the original SCO 680 PAR after keying in a transaction?

  Answer: Follow the steps below to request a duplicate Turnaround PAR.

  1. On SCO Main Screen, key in the PPSD Reference number for the current day.
  2. Next to the RQST line key the employee's social security number (SSN) and press ENTER; you do not need a transaction code or a document processing number.
  3. Put an X next to the PAR Line and press Enter. A Turnaround PAR will be sent to the agency.

  If you want the PAR to be routed to another agency tab down to Route To field and enter the agency # you want the PAR to go to and the Department Code (Please note that this is NOT the unit #; it is the three-digit code located right after the position # on the PAR.

- **Question**: Why are there duplicate STD 672s that the Personnel Specialists download in Mobius? Is there a reason for the duplicates? It seems to create more work for the Personnel Specialists to have to extract the duplicates in the PDF files.

  Answer: During the modification of the 672 report from paper to electronic there was no change to the original report. The original report contained two copies. SCO has limited resources to work on conversion of its paper reports to electronic versions and will not be altering the original paper version of any of the reports.

- **Question**: Are there any updates on the progress of SCO transitioning PAR's/NOPA's to electronic versions?

  Answer: The SCO is currently working on transitioning these reports to electronic versions. Both are both in the "test" phase and we hope to have these completed soon.

- **Question**: Are there any written policies regarding non testing Temporarily Authorization (TAU) hourly employees? Does salary rule 599.677 apply to these classes when determining salary upon reappointment? Is there a policy that allows these employees to keep their earned Merit Salary Adjustment (MSA) increases when moving to a different class without a break in service?

  Answer: Salary rule 599.677 applies if the employee was permanent when they left state service and returned as a TAU. If the employee was temporary when they separated this rule does not apply and they retain no rights to their previous salary. Non-status employees do not retain any salary rights, this includes limited term, temporary, Career Executive Assignment (CEA), and Exempt appointments. There are salary exceptions that Personnel Services Branch (PSB) may approve depending on the circumstances.

Privacy and Security Best Practices – Ronna Vandertorren (ISD)

– Privacy and Security are Important: The three primary goals of information security are protecting *availability*, *integrity*, and *confidentiality*.
  - Real Harm to Organizations and Individuals.
    - Legal, Regulatory Sanctions, Financial, Operational, Reputational…
  - Organizational and Personal Liability.
  - Ever Changing Threat Landscape.
  - Cyber War – Nation Against Nation.
  - Increasing Criminal Cyber Security Activity.
  - Increasing Financial Gain.
  - No Organization Goes Unscathed

– The Ever Changing Threat Landscape
  - Threats Include:
    - Insider Threats (can be Accidental, Negligence or Deliberate)
    - External Threats
  - Phishing Attacks:
    - #1 way cyber criminals find a way into organizations. (Email, Texting, Phone & using voice impersonation software)

  "These scams are becoming more effective, which is concerning, as you might expect growing awareness to make them less so." ~ *Principal Architect at Thomson Reuters*

  Gartner predicts a threefold increase in the number of organizations worldwide that will experience attacks on their software supply chains by 2025, compared to 2021

  - Attacks are Stealthier/More Frequent:
    - Social Engineering
    - Ransomware
    - Mobile Security Attacks
    - Remote Working Risk
    - Cloud Security Risks
    - Malware (viruses, worms, trojans, spyware, adware, key loggers, root kits, bots, fileless malware, etc.)
    - Uptick in Violence *(watch your physical security)*
  - Examples**:**
    - Infrastructure, Pipelines, Supply Chains, Military, Government, Large Corporations, Technology Theft, etc.

– The Current Threat Landscape Is More Dangerous!
  - The Scale, Sophistication and Impact of Cyber Threats is Increasing Significantly.
    - Direct Targeting of Internal Networks. Advanced Social Engineering and Malware Capability.
    - Global Attacks Increased by 28% in Q3, compared to the same period in 2021.
      ~ *Check Point Research (CPR)*

- 1,130 average # of attacks per org / per week (globally).
  ~ *Check Point Research (CPR)*
- 90% of Breaches Start with Phishing *(up 65% over last year…$12 billion in business losses).*
- It now takes 191 Days on average To Discover a Breach ~ Deloitte.

– Common Mistakes Managers Make

- Not Partnering With The Information Security and Privacy Offices.
  - Not Engaging early when new projects or products are developed or deployed.
  - Not role modeling or championing good Security and Privacy practices.
  - Not making Security and Privacy a standing agenda item for staff meetings.
- Assuming Established Vendors Have Strong Security and Not Measuring Vendor Performance.
  - Example, using key performance indicators (Adherence to contract terms, quality, delivery, risk, cost, customer service, etc.)
  - Not auditing the security level of 3rd Party Apps. (At least annually)

– Ways To Champion Security and Privacy

- Read the security policy, demonstrate compliance.
- Partner with your information security office:
  - Require employees become familiar with security and privacy policies relevant to their roles.
  - Help employees understand how to recognize something suspicious.
  - Ensure employees know how to report suspicious emails and suspicious behavior.
  - Reward good security and privacy practices.
- Do not assume all people, internal or external, have the best intentions.
- Be aware of third party risk.
- Keep track of security news, alerts, and incidents (internal and outside your organization).
- Learn from the mistakes or oversights of others.

– Opportunities To Help Others

- In Your Organization
  - Role Modeling and Championing Privacy and Security.
  - Providing information resources to educate employees on personal security (translates to better awareness at work).
- In The World
  - Practice your leadership skills outside of work while making an important difference in someone's life.
  - Educate others in your community on Security and Privacy. The Elderly, Children, Neighbors, Clubs and Chapters.

Valuable Resource Links

- Identity Theft
- Protect Children From Identity Theft
- What To Do If You Were Scammed – FTC
- Setting Up Fraud Alerts and Credit Freezes
- PDF – Protecting Personal Information - FTC

- Video - Five Ways to Help Protect Your Identity - FTC
- Sign Up For The Do Not Call Registry
- Stop Prescreened Credit Card and Insurance Offers
- Application Development Security
- Stop Think Connect - Tips and Advice in English and Spanish
- StaySafeOnline.org - Safety Privacy Basics
- StaySafeOnline.org - Manage Your Privacy Settings
- Better Business Bureau (BBB)
- Cyber Security For Your Home (BBB)
- Cyber Security and Infrastructure Security Agency (CISA)
- Report Fraud
- Report Identity Theft
- Avoiding and Reporting Scams
- How To File a Complaint Video
- **Free credit reports** from Equifax, Experian, and TransUnion.
  - Go to annualcreditreport.com
  - Or call 1-877-322-8228.
  - National Credit Bureaus Contact Info
- **Free Information Packets**, Pamphlets, book marks, FTC Business Cards, etc.
  https://www.bulkorder.ftc.gov/
- FEDERAL TRADE COMMISSION
  600 Pennsylvania Avenue, NW
  Washington, DC 20580
  1–877–FTC–HELP (1–877–382–4357)
  business.ftc.gov/privacy-and-security

– The Holidays Are Coming Ready Or Not

- Scammers will be in full force sending fake emails and texts pretending to be merchants for financial gain.
  - Fake online vendors and email advertisers will be luring people in with enticing items to convince them to click on malicious links, visit fake websites or provide passwords, credit card numbers or other personal information.
  - Don't click suspicious links or attachments in emails, text messages, websites, or social media and don't be tricked into giving out your passwords or credit card information.
- Watch out for auction fraud, where products are misrepresented on an auction site, and gift card fraud, where a seller asks you to pay with a pre-paid card. Then asks you to send a gift card number and PIN, so they can steal the funds without ever sending the items you thought you purchased.
  - Check your statement regularly. Contact your credit card company to dispute the charge if you see a suspicious transaction.
  - Always get tracking numbers for items you buy online to ensure they have been shipped and follow the delivery process.

Be on the lookout for scams of all types…charity scams, travel scams, social security and Medicare scams, etc.

Be aware of non-payment and non-delivery scams. The Internet Crime Complaint Center's (IC3) report shows they cost people more than $337 million last year.

– The Difference Between Privacy and Security
  - Data privacy refers to the protection of personally Identifiable Information (PII). For example protecting PII by not including it in public reports or documents.
  - Data privacy protections include policies and mechanisms put in place to help control how data is collected, categorized, transmitted and stored.
  - Data security refers to the technical solutions used to protect information.
  - Data protections include technology used to monitor data and systems, access management, data encryption, incident response, etc. This is to ensure data is not accessed by unauthorized systems or persons.

  The bars on a window that protect intruders from coming inside is an example of security.
  Pulling the shade, so those outside cannot see inside is an example of protecting privacy.
  We need to protect both Privacy and Security

– Sound Privacy and Security Practices
  - Know what personal information you have in your files and on your computers.
  - Only keep what you need for your business.
  - Protect the information that you keep.
  - Properly dispose of what you no longer need.
  - Work with your Information Security Office (ISO) to understand the existing plan for responding to and reporting security incidents.

Dispose What You No Longer Need
  - What looks like trash to you is a gold mine for an identity thief.
  - Papers, receipts, USB's, DVD's/CDs, hard drives, etc…tossed in a dumpster facilitates fraud.
  - Properly dispose of sensitive information to ensure it cannot be read or reconstructed.
  - Dispose of paper records by placing them in workplace confidential bins or shredding them (must be a cross-cut shredder).
    - Ask your Information Security Office (ISO) to place confidential bins and shredders throughout the workplace and next to photocopiers.

– Best Practices for Disposing of Computing Devices
  - Contact your Information Security Office (ISO) to properly dispose of old computing equipment including printers and portable storage devices such as drives, USB's and memory cards, etc.
    - Deleting files with keyboard commands is not sufficient because the files can continue to exist on the computer's hard drive where they can easily be retrieved.
    - Remove hard drives and memory cards before donating equipment. Ask your Information Security Office (ISO) to take care of it for you.
  - Make sure employees who work from home follow the same procedures.
    - Train employees to only take electronic notes (OneNote, Word…) when working from home to eliminate pieces of paper with business information that could end up in household trash.

  Cybercriminals use various devices and tools to aggregate bits of information they find. Therefore, even tiny pieces of information are valuable can be used to commit future attacks!

– What Causes a Data Breach?
  - Sharing documents and spreadsheets with unauthorized persons.
  - Sharing documents and spreadsheets without removing unnecessary personal information.
  - Sending documents to the wrong person(s)
  - Discarding paper documents in trash instead of shredding or using confidential bins.
  - Disposing devices without properly wiping the contents.
  - Extraction of information with malicious software (documents, databases, financial and medical records, etc.
  - Lost or stolen devices with personal information.

  Prevent Data Breaches
  - Don't share passwords (individual logins, for example).
  - Don't trust any email, phone call or text message you haven't expected or that seems suspicious.
  - Don't email spreadsheets with personal information.
  - Don't store personal information on unauthorized cloud apps.

  Consequences of a Data Breach:
  - Compromised companies or agencies suffer Implications, Financial loss, Reputation loss, etc.
  - Individuals whose personal information was compromised face financial loss, reputation harm and physical or psychological harm.

  Examples of harm:
  - Financial fraud including unauthorized credit card transactions or credit fraud.
  - Identity theft causing financial or emotional and psychological harm.
  - Violence or intimidation.

SCO KEY INITIATIVES:

SCOConnect: Cal Employee Connect (CEC) Project/ConnectHR – Liz James (ConnectHRhelp@sco.ca.gov)

Cal Employee Connect (CEC)

- CEC Phase II – Employee Service features:
  - Wave I departments (110 civil service and 8 CSU campuses), and Wave II departments (47 civil service and 4 CSU campuses) have been deployed with Multifactor Authentication (MFA) and Direct Deposit features.
  - As of 11/15/22: 1448 employees have enabled MFA
  - As of 11/15/22: CEC has received 563 direct deposit transactions.
  - Electronic W-2 Survey sent on 11/14/22 and is due by the end of the month.

ConnectHR

- New Help and Feedback Web Form!
- Telework Stipend Update - October:
  - 120,896 payments were issued to 97,954 employees
  - More than 85% were the result of data submitted via ConnectHR rather than the Payroll Input Process (PIP)

SCO – California State Payroll System (CSPS) Project – Paula Giannini (CSPSHelp@sco.ca.gov)

– Project Information:

- **Objective:** To modernize and integrate the State's Human Resource and Payroll systems
- **Goals:** Manager and Employee Self-service, Reduction in manual/paper submissions, Improved reporting capabilities, Efficiencies in processes/workflow
- **Scope:** Personnel, Benefits, Position Control, Time & Attendance, Travel & Business Expense and Payroll
- **Why CSPS:** Current system is 50 years old and not integrated; current system does not reflect or incorporate IT, HR, PR innovations over past 50 years.
- **Who will this impact:** State HR and Payroll staff and all state employees

– Status Updates / Progress:

- **Recent Progress:**
  - Delivered "Improving Employee Pay" presentations to the Labor Relations Forum
  - Data team has finalized the new Single Source Employee Data table
  - DART Sponsor and Liaison October kickoff completed
- **Upcoming Activities:**
  - Continued meetings with Fi$CAL to mitigate risk
  - DART Sponsor and Liaison November kickoff
  - Completion of the Proof of Concept phase
- **Schedule:**

Activities	Start	End	Status
Conduct Solicitation Phase 2 - Proof of Concept and Evaluate Proposals	August 2022	November 2022	In progress
DART Sponsor and Liaison Kickoff Meetings	October 19, 2022	November 14, 2022	In progress
Conduct Solicitation Phase 3 – Negotiate and Select Vendor	November 2022	June 2023	

BENEFITS ADMINISTRATION:

SCO – Statewide Benefits Program - Ryan Baughman (ppsdcsbenefits@sco.ca.gov)

– Open Enrollment Form Counts – 11/15/2022

Dental STD. 692	FlexElect Cash Option STD. 701C	Consolidated Benefits Cash Option STD. 702	FlexElect Reimbursement STD. 701R
Received ~ 15,250	Received ~ 3,446	Received ~ 910	Received ~ 11,990
Completed ~ 8,885	Completed ~ 2,319	Completed ~ 324	Completed ~ 8,302
Remaining ~ 6,365	Remaining ~ 1,127	Remaining ~ 586	Remaining ~ 3,688

– ConnectHR Tips & Reminders

STD. 701c/702 Cash Option & STD.692 Dental

- Employees often switch between Cash Option & Dental plan
- It is okay to upload the STD.692 Cancel/Change/New with the STD. 701c/STD. 702 form in the same PDF. (Example: pg.1 701c New, pg.2 STD.692 cancel)
- You will only upload once under the FlexElect dropdown, no need to upload another Dental Cancel/Change/New if uploaded with the FlexElect/CoBEN form
- If employee wants to cancel Cash Option and in Dental, you will upload both forms under the Dental New dropdown (Example: pg.1 STD. 692 New, pg.2 STD.701c cancel)

Duplicate Forms

- There is no need to upload "inquiry" forms anymore or submit duplicates
- If you receive the receipt from ConnectHR, that means we have the form

Open Enrollment Peak Workload

- Check the Civil Service Weekly Processing Dates prior to calling for a status on a form
- Peak Open Enrollment processing now, processing dates may stagnate temporarily
- For a status on the form, contact Statewide Customer Contact Center (916-372-7200)

PROGRAM UPDATES:

Statewide Payroll Program – Renee McClain and Christina Campbell (Contact SCCC @ (916) 372-7200)

– Payroll Reminders

- Personnel Action Requests (PAR) must be submitted via ConnectHR to SCO by the following timelines:

Separation Month	Submit 1st PAR to SCO no later than…	Submit 2nd PAR to SCO between these dates…
October	ASAP	N/A
November	12/9/22	12/12/22 to 12/23/22
December	12/9/22	12/29/22 to 1/13/23

- PAR packages received by SCO after the dates specified will be processed; however, there may be charges assessed by CalHR to the agency (as stated in Section 1802 of the CalHR Manual) and/or a corrected W-2 for the 2022 tax year.
- Please submit these forms timely and accurately.

– REMINDER – Lump Sum Separation Toolkit

- NEW: HR Separation Checklist
- Lump Sum Guide and Tools for Personnel Specialists
  - Lump Sum Separation FAQ
  - A Guide to Avoiding Common Errors: Lump Sum Documentation and Processing
  - Lump Sum Worksheet
  - Lump Sum Pre-Tax Calculator
  - 1st Tax Year PAR Package Sample
  - 2nd Tax Year PAR Package Sample
- Planning and Training for Departmental Human Resource Offices
  - Talking Points and Activities for a Lump Sum Peak Workload Kickoff Meeting
  - eLearning Series for Personnel Specialists
- Lump Sum Information for Employees
  - NEW: Civil Service State Employee Guide to Retirement

California Leave Accounting System – Megan Vinson (CLAS@sco.ca.gov)

Annual Purge

- Taking place on December 5, 2022
- Clean up any outstanding employee record issues prior to that date

New eLearnings

- Earned Benefit Transfer
- Temporary Separations – coming soon!

New Holidays

- Lunar New Year, Genocide Remembrance, Juneteenth, and Native American Day
- New Use transaction code: 03, Use – In Lieu of Holiday Credit
- Exempt employees only

Management Information Retrieval System (MIRS) Training – Angela S. Cipollone (ppsdmirs@sco.ca.gov)

Initial Training Modules

1. MIRS Master File Descriptions (MFD)
2. Navigating the MIRS System
3. MIRS Procedure Overview
4. MIRS Procedure Writing (Verbs, Formats, and By Phrases)
5. MIRS Procedure Writing (Selecting Records)
6. MIRS Procedure Writing (Customizations)

Intermediate Training Modules – Coming Soon!

1. MIRS Procedure Writing (Defines)
2. MIRS Procedure Writing (Prompts)
3. MIRS Procedure Writing (Match Procedures)

MIRS eLearning Modules

1. MIRS File Description (FD)
    - Describes the files available in MIRS
        - Each file pulls from an SCO System
        - Ex: CSEMPL pulls from Employment History
    - Lists and describes the fieldnames in each file
    - Overview of the Data Element Dictionary (DED)
2. Navigating the MIRS System
    - Demonstrates:
        - Logging in and out
        - The menu options
        - Create new procedures
        - Executing procedures
        - Copying procedures
3. MIRS Procedure Overview
    - Explains the Update Schedule
    - Describes a Procedure vs. Report
    - Overview of the Procedure Writing Summary
    - Navigating a Procedure
    - Navigating a Report
    - Executing a Procedure in FOCUS
4. MIRS Procedure Writing (Verbs, Formats, and BY Phrases)
    - How to use verbs to generate report data
    - Describes the formats affiliated with fieldnames
    - How to use BY phrases to sort report data
5. MIRS Procedure Writing (Selecting Records)
    - Defines what a WHERE phrase is
    - Describes single selection criteria
    - Describes multiple selection criteria
    - How to limit the number of records in a report
    - How to verify data by checking and validating WHERE phrases

6. MIRS Procedure Writing (Customizations)
    - How to customize a report
        - Totals
        - Headings and Footings
        - Change Titles
        - Current Date & Time Variables
        - Reformatting Fieldnames
        - Skipping Lines

Statewide Tax Support Program – Monique Perez (PPSDW2MiscDed@sco.ca.gov)

– Document Cutoff Dates for 2022 Calendar Year-End Processing and Direct Mailing of Form W-2

Document Cut Off Dates

- Payroll Letter #22-020: Direct Mailing of 2022 Form W-2 And 2022 Form 1095-C Return Address on the Forms to Employees
- Fringe Benefits processed in December can generate a one-time payroll deduction A/R for the January master payroll. This is for accurate Form W-2 reporting purposes only.
- If the SCO does not receive the documents by the specified cutoff dates, employees may receive a Corrected Wage and Tax Statement, Form W-2C.

Direct Mailing of Form W-2's

- Payroll letter #22-020: Direct Mailing of 2022 Form W-2 And 2022 Form 1095-C Return Address on the Forms to Employees

Validate Addresses

- Agencies and or campuses must validate return addresses used last year for your Form W-2's.
- If you are unsure if the address SCO has is correct, please contact PPSD Statewide Tax Support Unit at PPSDSTSP@sco.ca.gov.
- PPSD Statewide Tax Support Program will confirm the address change
- If the address is incorrect, the employee must submit an Employee Action Request Form, STD. 686, with their new address to their Personnel Office, not SCO.

PPSD General Reminders

- December Transaction Supervisors Forum Date – December 14, 2022
- Utilize ConnectHR to submit documents or upload data – include SSN
- Include the employee's complete social security number (SSN) when sending documents through ConnectHR
- Check Weekly Processing Dates before sending inquiries
- Update California Personnel Office Directory (CPOD)
- The PPSD Register – PPSD's Monthly Newsletter
- Check out recommended Human Reources subscriptions
- Review Communication from State Policy and Instructional Departments for Business Process impacts
- It is recommended that the Human Resources (HR) staff follow Section M of the Payroll Procedures Manual (PPM) for certifying payroll, which requires HR staff to validate that both mandatory and voluntary deductions have been withheld appropriately and to certify the employee's payroll is accurate.
- Share this information with your Human Resources Team!

SCO EMAIL SUBSCRIPTION SERVICE:

- To ensure you're receiving essential PPSD notifications, please subscribe to our email subscriptions listed below. Also, we invite you to share this information with anyone who would be interested in PPSD notifications.
  - California Leave Accounting System (CLAS) Letters
  - State Controller's Office Letters (Personnel / Payroll Operations)

CUSTOMER RELATIONS SURVEY:

How would you like to receive information from us during this time? Please send suggestions to our HR Suggestions Inbox at PPSDHRSuggestions@sco.ca.gov.

SCO RESOURCES:

- Websites:
  - Human Resources (HR): https://sco.ca.gov/ppsd_state_hr.html
  - State Employees: https://sco.ca.gov/ppsd_se_payroll.html

SCO KEY INITIATIVES:

- SCOConnect
- California State Payroll System Project

CONTACTS:

- Affordable Care Act (ACA) Email acasupport@sco.ca.gov
- Cal Employee Connect Email connecthelp@sco.ca.gov
- Cal Employee Connect Feedback Email connectfeedback@sco.ca.gov
- California Leave Accounting System (CLAS) Email Clas@sco.ca.gov
- ConnectHR Email (All HR Staff) connecthrhelp@sco.ca.gov
- ConnectHR Feedback Email (All HR Staff) connecthrhelp@sco.ca.gov
- CS Escalation Email (HR Supervisors and Managers) PPSDOps@sco.ca.gov
- HR Suggestions Email (All HR Staff) PPSDHRSuggestions@sco.ca.gov
- Management Information Retrieval System (MIRS) Email ppsdmirs@sco.ca.gov
- Statewide Customer Contact Center (916) 372-7200