



Commission on Peace Officer Standards and Training

860 Stillwater Road, Suite 100
West Sacramento, CA 95605-1630
www.post.ca.gov

Date: July 27, 2022

Bulletin: No. 2022-34

Subject: **Amendments to Peace Officer Selection Standards, Commission Regulations 1953 and 1955**

At the May 26, 2022 meeting, the Commission approved changes to Regulations 1953 and 1955, adopting the use of the Bias Assessment Framework in screening peace officer candidates for bias against race or ethnicity, gender, nationality, religion, disability, or sexual orientation [Regulation 1955(a)]. These regulatory changes were made in response to mandates imposed by [Assembly Bill \(AB\) 846](#) (2020).

The Office of Administrative Law approved the regulatory changes on July 18, 2022. The [Notice of Approval](#) (pdf), which includes the approved text, may be accessed on the [POST Website](#). These regulation changes become **effective August 1, 2022**. Significant changes are addressed below.

Bias Assessment Framework

The new regulations incorporate a Bias Assessment Framework, which identifies three constructs - biased behaviors, biased attitudes, and bias-relevant traits and attributes – by which candidates will be evaluated. The evaluation will rely on data sources that include the candidate's personal/background history, written assessments (e.g., written psychological exams), and a clinical interview. The new regulations also require that background investigators and screening psychologists report bias-relevant findings to the hiring department.

Multicultural Competence

Multicultural competence is added to the current list of peace officer psychological evaluator competencies, to ensure psychologists have the ability to interact with candidates in cross-cultural situations.

Social Media Check

A social media check is being implemented as part of the background investigation as another potential source of bias-relevant information and to ensure that a thorough background investigation is conducted in compliance with Government Code section 1031(d) and Commission Regulation 1953(a). To assist departments with implementing this new requirement, attached to this bulletin is a list of Frequently Asked Questions (FAQs) and information on additional resources and considerations.

Earlier this year, Chapter 5 of the Peace Officer Psychological Screening Manual (PSM) and Chapter 2 of the Background Investigation Manual (BIM) were revised to include the Bias Assessment Framework (Framework) as a recommendation for meeting the bias screening

Amendments to Peace Officer Selection Standards, Commission Regulations 1953 and 1955

Page 2

requirement of Commission Regulation 1955(a). Both manuals are in the process of being updated to reflect the new regulations, including changing the current recommendations to requirements.

Additionally, amendments to Commission Regulations 1953 and 1959, mandating background investigator training, were recently approved (see [Bulletin 2022-27](#)). Although the regulatory action was implemented on July 1, 2022, the mandatory training requirement is not in effect until July 1, 2023. In anticipation of this requirement, POST is in the process of updating the current recommended background investigation course curriculum, identifying mandatory curriculum content, and exploring the development of additional training options. Investigators are encouraged to obtain POST-certified background investigation training prior to the effective date, to ensure they are compliant with the requirement. Available POST-certified courses can be found in the [Course Catalog](#). A list of FAQs regarding the mandated background investigation training is attached to this bulletin.

Questions regarding Commission Regulations 1953 and 1955 may be directed to [Melani Singley](#), Selection Standards Program Manager, at [\(916\) 227-4258](tel:9162274258).

MANUEL ALVAREZ, JR.
Executive Director

MA:mls

Attachment

Social Media Check FAQs

Q1: Does the social media check require that the background investigator access a candidate's private social media account(s)?

A1: The social media check requires that a search be conducted of postings made by the candidate to determine suitability for peace officer employment, regardless of where the postings are made (e.g., on social networking sites, blogs, forums). It does not, however, require nor permit infringement of a candidate's privacy rights. All searches must be conducted in accordance with state and federal laws.

Q2: Section 980 of the Labor Code prohibits employers from requiring or requesting applicants to: "(1) Disclose a username or password for the purpose of accessing personal social media. (2) Access personal social media in the presence of the employer. (3) Divulge any personal social media." What does this mean for law enforcement employers (e.g., POST-participating departments) who must conduct a social media check?

A2: Whether Labor Code section 980 applies to public sector employers is unsettled. Some cases hold that Labor Code provisions must specifically be made applicable to public employers to bind them [see e.g., [Johnson v Arvin-Edison](#) 174 Cal.App.4th 729 (2009) - unless a Labor Code provision specifically states it applies to public employers, it is presumed to apply only to private employers]. While the Legislature may have intended in enacting Labor Code section 980 that it apply to public employers (because, among other things, an example given as a justification for it was a background investigation of a Maryland correctional officer), no provision was included in the legislation specifically applying it to public agencies. While this may have been an oversight, a subsequent legislative attempt to clarify its applicability to public agencies did not survive the legislative process. Therefore, as it currently stands, the law is not clear-cut on this issue, especially when considering legislative history and intent. Thus, departments are encouraged to work with their legal counsel to develop a cyber vetting policy to address this and other relevant laws.

Q3: What information should be provided in the social media search results?

A3: Only information that is relevant to peace officer suitability should be reported and documented. This would include evidence of bias-related behaviors, traits and/or attributes, illegal and/or immoral behaviors, or other behaviors that indicate unsuitability to be a peace officer. This could also include evidence that may mitigate past behaviors, such as positive character traits and/or activities that indicate the individual has matured and/or been rehabilitated. All results should be directly related to either the background investigation dimensions or the bias assessment framework.

Q4: Is there specific information that should not be included in the social media search results?

A4: Employers should not be provided information that is protected under fair employment laws, privacy provisions, or any information that is not relevant to peace officer suitability. This

may include pregnancy status, religion, disability information, political affiliation, and sexual preference to name a few. Results should be restricted to candidate information only.

Q5: *How far back should the social media search be conducted (e.g., should only recent social media postings be reviewed)?*

A5: It depends. A younger candidate may not need as lengthy of a search as an older candidate. Evidence of unsuitable behavior may necessitate a longer history search to determine patterns of behavior. Departments should establish a cyber vetting policy to ensure that all candidates are being treated in a fair and consistent manner.

Q6: *Where in the background file should the social media findings be placed?*

A6: Documentation (e.g., printouts, screenshots) should be included under Tab L – Relatives/Personal References. The tabs are in the process of being updated with the new regulations. In general, the location of current tab information will not change. Social media findings, including bias-relevant information, must be included in the narrative report.

Additional Resources and Considerations

The information below is intended as guidance for investigators in conducting social media searches and for departments in establishing cyber vetting policies for screening peace officer candidates. The information should not be interpreted as compulsory, exhaustive, nor a substitute for competent legal advice. Departments are highly encouraged to work with their legal counsel to develop a comprehensive cyber vetting policy.

State and Federal Laws

- [Labor Code § 980](#)
- Federal Equal Employment Opportunity Commission (EEOC)
 - EEOC *Social Media in the Workplace: Examining Implications for Equal Employment Opportunity Law* (EEOC Meeting of March 12, 2014)
 - [Press Release](#)
 - <https://www.eeoc.gov/meetings/meeting-march-12-2014-social-media-workplace-examining-implications-equal-employment>
 - [Fair Employment and Discrimination Laws](#)
 - Prohibited Employment Policies and Practices:
<https://www.eeoc.gov/prohibited-employment-policiespractices>
- California Department of Fair Employment and Housing (DFEH)
 - [Employment Discrimination](#)
- State and Federal Fair Credit and Investigator Consumer Reporting Requirements
 - ICRAA (California [Civil Code §1786](#), et seq.)
 - FCRA ([5 U.S.C. §§ 1681](#))
- Article 1 of the California Constitution
- The First Amendment to the United States Constitution

- Case Law – regard should be given to cases specific to law enforcement employment, including First Amendment and relevant background issues

Social Media Content Considerations

- POST background investigation dimensions and bias screening requirements. Relevant content may include bias-relevant behaviors; behaviors indicative of misconduct or dishonesty, illegal acts, or activity; or other behaviors or evidence indicative of unsuitability for employment
- Publicly available, open-source information
- Seek legal counsel advice with regard to private social media accounts
- Careful consideration of protected information
- Restrict to information relevant to the candidate only
- Number of followers/friends etc. should not be considered

Searchable sites may include, but not be limited to:

- Social networking (e.g., Facebook, Instagram, LinkedIn)
- Blogs (e.g., Twitter, Tumblr)
- Video (e.g., YouTube, TikTok, Twitch)
- Forums (e.g., Quora, Reddit)

Reporting Limits and Considerations

- Report only information relevant to peace officer suitability
- Do not include information about others
- Redact irrelevant information
- Verify accuracy of information
- Provide sources – URLs, webpages
- Provide documentation – screenshots, printouts, etc.

Mandatory Background Investigation Training FAQs

Q1: Who must meet the mandatory background investigator training requirement?

A1: The requirement applies to those who conduct the background investigation, thus a staff member who merely collects information at the onset of the background would not necessarily be required to attend training. However, an officer being assigned to backgrounds (even if temporarily) would have to complete the training prior to being able to conduct background investigations.

Q2: Where do I find information about POST-certified background investigation course availability?

Q2: All POST-certified courses, including the background investigation course, can be found in the [Course Catalog](#).

Q3: Are all background investigation course presentations the same?

Q3: POST currently only provides recommended course curriculum; thus, content and instruction may vary by presenter. POST is in the process of identifying mandatory content requirements, and once identified, will pursue regulatory changes to that effect. In the interim, departments and investigators are encouraged to reach out to course presenters directly and/or access the [POST Open Data](#) resource to identify specific course content, curriculum, and learning objectives.

Q4: If the investigator has already attended background investigation training, will they need to repeat it and/or update the training?

A4: Once the training has been completed, it does NOT need to be repeated, regardless of when the course was completed. There is no current requirement for update training.

Q5: How do departments track completion of the training requirement (e.g., confirm that their investigator(s) have completed the mandatory training)?

A5: Departments can request the background investigator to provide a copy of their POST Profile (e.g., training record), which the investigator can easily access through the POST PASS system. The profile will include the completed training.