U.S. Department of Labor

Office of Federal Contract Compliance Programs
200 Constitution Avenue, N.W.
Washington, D.C. 20210

April 7, 2020

Mr. David B. Cohen
Mr. David S. Fortney
Mr. Mickey Silberman
Institute for Workplace Equality
1920 I Street, NW
Washington, DC 20006

VIA EMAIL: Barbara.Kelly@theinstitute4workplaceequality.org

Dear Messrs. Cohen, Fortney, and Silberman:

Thank you for your March 27, 2020, correspondence to the U.S. Department of Labor's (US DOL) Office of Federal Contract Compliance Programs (OFCCP) inquiring as to how compliance officers and other OFCCP employees will handle federal contractors' data now that they are working remotely.

As you know, OFCCP administers and enforces three equal employment opportunity laws: Executive Order 11246, as amended (Executive Order); Section 503 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 793 (Section 503); and the Vietnam Era Veterans' Readjustment Assistance Act of 1974, as amended, 38 U.S.C. § 4212 (VEVRAA). Collectively, these laws make it illegal for contractors and subcontractors doing business with the federal government to discriminate in employment because of race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or status as a protected veteran. In addition, contractors and subcontractors are prohibited from discriminating against applicants or employees because they inquire about, discuss, or disclose their compensation or that of others, subject to certain limitations.

During the COVID-19 pandemic, while securely teleworking, OFCCP remains committed to safeguarding any nonpublic, confidential, and sensitive data it receives from contractors and complainants during compliance evaluations and complaint investigations.

OFCCP has had a long-standing policy that requires compliance officers, to store information received from contractors on the agency's secure network. The policy instructs staff that while on telework, nonpublic, confidential, and sensitive data should be accessed via OFCCP-furnished laptop, as this is considered OFCCP-controlled space and provides sufficient protections for data.

To further clarify, OFCCP data (including data submitted by contractors), are stored in the protected US DOL network or the Microsoft Azure federal platform. These environments are

secure and accessible only to authorized US DOL staff, enforced by access-control permissions. Staff access the network using either a Virtual Private Network (VPN) or Hypertext Transfer Protocol Secure (HTTPS) connection, both protected by TLS using 256-bit Advanced Encryption Standard (AES) protocols. Data stored locally on the workstation are protected with 256-bit AES full-disk encryption. US DOL staff issued workstations must provide a Personal Identity Verification (PIV) card and password to sign in. The US DOL network, including workstation system settings, have all been independently tested to meet the Federal Information Security Modernization Act of 2014 (FISMA) requirements and National Institute of Standards and Technology (NIST) guidance.

The policy also requires that monitors or computer screens be turned away from windows or doors such that unauthorized individuals cannot read the display. When idle, monitors and screens must transition to a password-locked screensaver to prevent unauthorized reading of data or system manipulation.

In addition, all OFCCP staff, including compliance officers, are required to complete annual training from US DOL and OFCCP on safeguarding data.

Contractors also have the option of sending their data to OFCCP via their secure data or email portals. OFCCP is now able to transfer data back to the contractors via a secure file sharing portal.

Thank you again for your correspondence. If you have further questions, please contact Lissette Geán at (202) 693-1049 or via email at Gean.Lissette@dol.gov.

Sincerely,

Craig E. Leen
Director

cc: Barbara Kelly