CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

RANDEL K. JOHNSON
SENIOR VICE PRESIDENT
LABOR, IMMIGRATION & EMPLOYEE
BENEFITS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062
202/463-5448 · 202/463-3194 FAX
RJOHNSON@USCHAMBER.COM

September 23, 2016

The Honorable Howard Shelanski
Administrator, Office of Information and Regulatory Affairs
Office of Management and Budget
1650 Pennsylvania Avenue NW, Room 262
Washington, DC 20503

Re: EEO-1 Data and Cybersecurity

Dear Administrator Shelanski:

I am writing to call your attention to two important developments this week relating to cybersecurity that should be considered as your office continues to deliberate the Equal Employment Opportunity Commission's (EEOC or Commission) proposed changes to its EEO-1 form. As we noted in both our written comments as well as our meeting on September 7, EEOC failed to set forth – as required by the Paperwork Reduction Act (PRA) – appropriate steps or protocols to ensure the privacy and confidentiality of EEO-1 data. These two recent incidents further underscore the risk in allowing the EEOC to collect massive amounts of sensitive, proprietary pay information without an express process and protocol to ensure the confidentiality of that information as required by the PRA. The EEOC's failure to include such protocols is significant and fatal to its proposal. As a result, the Office of Information and Regulatory Affairs (OIRA) should return the proposal to EEOC so the Commission can take the necessary steps to ensure that EEO-1 data remains confidential.

First, the Washington Post reported yesterday on a cyber breach at Yahoo!, in which the account information of at least 500 million users was stolen. According to the story, "[t]he Yahoo theft represents the most accounts ever stolen from a single email provider." Although the compensation and work hours data that would be contained in the proposed EEO-1 is obviously different than the personally identifiable information stolen from an email account, this breach is just the latest example of the continuing and growing cybersecurity threat that both private and public institutions face. EEOC must consider and appropriately address the growing size and scope of these cyber attacks if it is going to collect sensitive and proprietary data from employers. It has not done so.

Second, and more importantly, on September 19 the GAO released a study entitled, "Federal Information Security: Actions Needed to Address Challenges." Perhaps all you need to know is contained in the very first sentence of the report: "Cyber incidents affecting federal agencies have continued to grow, increasing about 1,300 percent from fiscal year 2006 to fiscal year 2015." Although the report does not specifically mention EEOC, it does note that despite the growing frequency of cyber incidents, "many agencies continue to have weaknesses in implementing [information security] controls, in part because many of these recommendations remain unimplemented."

As we set forth in our comments and in our meeting, the EEOC is proposing to collect highly sensitive personal data regarding compensation at thousands of American companies in a format which will not serve any of its statutory purposes and with an almost disdainful disregard of the obligation it and OIRA have to insure that the information submitted be kept confidential. While the compensation information will be of little or no legal use for the EEOC, it will certainly be of great use to any hacker who is interested in the compensation practices of most United States employers.

Thus, just two months after your receipt of EEOC's proposal to collect an unprecedented amount of sensitive and proprietary data from employers, GAO has sounded the alarm (again) about the cyber threats facing federal agencies, particularly as it relates to "[s]ensitive information, such as intellectual property." The GAO report brings EEOC's failure to ensure privacy and confidentiality of EEO-1 data into even greater relief. Fortunately, the GAO report provides a number of recommendations for agencies to undertake in order to improve their approach to cybersecurity (see GAO report at pages 8 through 10). Accordingly, the EEO-1 proposal should be returned to EEOC so the Commission can review the privacy and confidentiality provisions contained therein in accordance with GAO recommendations.

Thank you for your attention to this matter.

Sincerely,

Randel Johnson
Senior Vice President
Labor, Immigration and Employee Benefits