POSTSEC DATA

October 23, 2020

Mark A. Brown, Chief Operating Officer
Office of Federal Student Aid
U.S. Department of Education

Dear Chief Operating Officer Brown,

This letter is submitted on behalf of these 14 undersigned members and partners of the Postsecondary Data Collaborative (PostsecData). PostsecData is a coalition of diverse organizations that recognize the power of high-quality data to ensure equitable access and success in higher education.

Our student-driven mission and unwavering commitment to putting the best information in the hands of students, families, and policymakers to inform decision-making also keeps issues of privacy and security at the forefront of postsecondary data policy conversations. Policy should address stakeholder needs for information as well as protect students' right to privacy and keep data secure from internal and external threats. It is for these reasons that we commend the Office of Federal Student Aid (FSA) for dedicating Strategic Goal 4 to strengthening data protection and cybersecurity safeguards and Strategic Goal 5 to enhancing transparency of the aid portfolio.[i]

In recent years, the U.S. Department of Education Office of Inspector General has raised concerns about gaps in existing security protections at FSA, including in the Fiscal Year 2019 Federal Information Security Modernization Act[ii] review and the audit of FSA's Contractor Personnel Security Clearance Process in 2018.[iii] We appreciate that Strategic Objective 4.1 ("Implement business partner and vendor systems, focused on oversight, enforcement, infrastructure, systems, and data") and 4.3 ("Build an effective cybersecurity culture through employee awareness, training and accountability focused on protecting systems and data") are focused squarely on these issues.

While Strategic Goal 4 concentrates on key topics like cybersecurity and the negative impact of breaches on processes and reputation, we would like to see additional emphasis given to issues of privacy, risk management, and data governance at both postsecondary institutions and FSA. Strategic Objective 4.2 mentions controls and communications with institutions to prevent breaches, but it does not outline the steps that FSA will take internally to ensure student privacy protection, like steps to strengthen and solidify controls and restrictions around data access, use, sharing, and processing. We encourage FSA to explore resources related to the "five safes" framework and National Institute of Standards and Technology's (NIST) Privacy Framework, to marry its work on prevention of cybersecurity risks with recognition of privacy risks.[iv]

PostsecData also recommends adding a new Strategic Objective 5.5: Improve Insights Into and Understanding of Variations in Student Aid by Race/Ethnicity and disaggregating Performance Metrics (B), (C), and (D) by race/ethnicity and institution sector (Strategic Objective 5.3). These disaggregated data would offer a more comprehensive understanding of disparate outcomes, especially critical for Black students. We also welcome the change to monthly reporting through the FSA Data Center to provide closer to real-time insights for the aid portfolio (Strategic Objective 5.1) and recommend that FSA couple the emphasis on transparency with increased access to data for researchers, through privacy-protected microdata or research partnerships (Strategic Objective 5.2).[v]

It is critically important to use high-quality data to understand inequitable outcomes among student groups and advance student success while also ensuring security and safeguarding students' privacy. We commend FSA for its commitment to creating a secure data environment and encourage you to consider ways to also overtly prioritize student privacy and continue to improve transparency. If you have any questions, please contact Mamie Voight, vice president of policy research at the Institute for Higher Education Policy (mvoight@ihep.org or 202-587-4967).

Sincerely,

AccuRounds

American Educational Research Association - AERA

Data Quality Campaign

Future of Privacy Forum

Georgetown University Center on Education and the Workforce

Higher Learning Advocates

Institute for Higher Education Policy

Manufacturers Education and Training Alliance

NASPA - NASPA - Student Affairs Administrators in Higher Education

National Association for College Admission Counseling

National Center for Higher Education Management Systems

New America Higher Education Program

The Institute for College Access and Success

uAspire

[i] Office of Federal Student Aid (2020). Draft Federal Student Aid Strategic Plan FY 2020-24. Retrieved from: https://studentaid.gov/sites/default/files/fy2024-strategic-plan-draft.pdf

[ii] U.S. Department of Education Office of Inspector General (2019, October 31). The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report. Retrieved from: https://www2.ed.gov/about/offices/list/oig/auditreports/fy2020/a11t0002.pdf

[iii] U.S. Department of Education Office of Inspector General (2018, April 17). Federal Student Aid's Contractor Personnel Security Clearance Process. Retrieved from: https://www2.ed.gov/about/offices/list/oig/auditreports/fy2018/a19r0003.pdf

[iv] O'Hara, A. (2019, June). Postsecondary Data Infrastructure: What is Possible Today. Retrieved from: http://www.ihep.org/research/publications/postsecondary-data-infrastructure-what-possible-today; National Institute of Standards and Technology (2020). The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Retrieved from: https://www.nist.gov/privacy-framework/privacy-framework

[v] "Letter from PostsecData, faculty, and others on Federal Student Aid transparency". (October 2016). Retrieved from: http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/finaldraftfsaletter.pdf