PARENT COALITION FOR
STUDENT PRIVACY

www.studentprivacymatters.org
info@studentprivacymatters.org
@parents4privacy

124 Waverly Place
New York, NY 10011
303.204.1272

November 14, 2016

Docket ID: USBC-2016-0003-0001
The Commission on Evidence-Based Policymaking (CEP)

To the Commission:

We, the undersigned organizations, respectfully submit the following comments to the Commission on Evidence-Based Policymaking. While we applaud the ambitious charge of the Commission to examine "*strategies to increase the availability and use of government data, in order to build evidence related to government programs and policies, while protecting the privacy and confidentiality of the data,*" we strongly oppose any proposal that would lead to the creation of a central federal clearinghouse or linked data sets containing the personally identifiable information ("PII") of all students, commonly referred to as a federal student unit-record system or national database.

We cannot overstate the threat to student privacy that would be posed by the development of such a database, including breach, malicious attack, or use of student PII for purposes not initially intended. Ever since a federal student unit-record system was first proposed by the Bush administration in 2005, and banned by the Higher Education Act in 2008, the reasons against creating it have only become more persuasive in recent years.

First, we are gravely concerned about the high probability of breaches and unauthorized access to the data. As a 2015 report by the U.S. Government Accountability Office ("GAO") revealed, reports of security incidents involving breaches of personal information held by federal agencies rose from 10,481 in 2009 to 27,624 in 2014 – an increase of 164 percent over five years -- for a total of 144,439 reported instances. [1] The report also noted that these events can *"adversely affect national security; [and] damage public health and safety*" and yet federal agencies have failed to implement approximately nearly half of the recommendations made to them to improve security of their systems over the last six years*.*

In addition to system breaches documented by the GAO, the Office of Personnel Management announced in June 2015 that the personnel records of about 22.1 million people had been maliciously hacked by foreign interests -- not only federal employees and contractors but also their families and friends, including highly sensitive information gathered for the purposes of security clearance.[2]

The US Department of Education has been found to have especially weak security standards in its collection and storage of student information, as reported by an audit released in November 2015 by the department's Inspector General. This puts at risk the huge amount of data that the agency already holds, including student loan information involving information on more than 100 million individuals and

[1] http://www.gao.gov/assets/680/673678.pdf
[2] https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

at least 39 million unique Social Security numbers.[3] A reported by the audit, staff in the IG office hacked into the Department's main IT system and gained unfettered access to personal data without anyone noticing. Overall, the audit found significant weaknesses in four out of the five security categories.[4] In May 2016, the government scorecard created to assess how well federal agencies were implementing data security measures awarded the Education Department an overall grade of D.[5]

Second, K-12 student data currently collected by state departments of education in statewide longitudinal data systems (SLDS) that would potentially be shared with the federal database generally extend well beyond traditional administrative data to include upwards of 700 specific personal data elements, including students' immigrant status, disabilities, disciplinary incidents, and homelessness status.[6]

Data collected ostensibly for the sole purpose of research but without the individual's consent or knowledge would likely be merged with other federal agency data sets, to follow students into the workplace and beyond, and could include data from their military service, tax returns, criminal and health records. If this granular level of sensitive information were available in a universal U.S. student record database, it could quickly become a go-to repository for purposes that should never be allowed.

A real-life example of the potential misuse of a system of this nature has just been reported in England. There, a similar student data repository called the National Pupil Database ("NPD") was intended to be maintained "solely for internal departmental use for the analytical, statistical and research purposes." But as Freedom of Information requests[7] recently revealed, the names and home addresses of thousands of students[8] in the NPD have been requested by police and the Home Office for various purposes over the last 15 months, including to curb "abuse of immigration control."[9] A group of parents, teachers, and human rights campaigners has launched a national boycott to urge parents and schools to withhold their children's country of birth and nationality, data which is being collected at national level for the first time.[10]

Finally, we are very concerned about recent revelations of the widespread surveillance on ordinary citizens by the federal government, and the way in which a national unit-record system could be used to expand tracking of students. While data holds promise to solve complex problems and may be used to improve our nation's policies, we have a responsibility to our nation's citizens to protect the privacy of their most personal information, especially that of vulnerable children.

[3] https://www2.ed.gov/about/offices/list/oig/auditreports/fy2015/a11o0001.pdf

[4] http://federalnewsradio.com/cybersecurity/2015/11/government-testers-easily-bypassed-education-defenses-recent-cyber-audit/

[5] http://www.nextgov.com/cio-briefing/2016/05/fitara-scorecard-fewer-agencies-get-failing-scores/128410/

[6] See NYS for example at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

[7] https://www.whatdotheyknow.com/request/sharing_national_pupil_database?nocache=incoming-878444#incoming-878444

[8] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-10-13/48635/

[9]http://www.theregister.co.uk/2016/10/12/national_pupil_database_has_been_used_to_control_immigration/?mt=1476378123415

[10] https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-facing-lords-opposition-over-widely-condemned-"foreign

Any recommendation by the Commission to establish a federal data clearinghouse of student PII could effectively create life-long dossiers on nearly every individual in the nation. Instead, we strongly believe that the federal government should use aggregate, de-identified student information already maintained by states or districts for research or policy decisions.

We strongly urge that members of the Commission to consider the threats to privacy that overturning the ban on a federal student unit-record clearinghouse would create. Once privacy is lost it is nearly impossible to restore, and we hold a moral and ethical obligation to our children – and our citizens -- to minimize this risk in any way possible.

Yours,

Parent Coalition for Student Privacy
American Civil Liberties Union
Network for Public Education and NPE Action
Parents Across America
Badass Teachers Association
New York State Allies for Public Education