Consumer Financial Protection Bureau
1700 G Street NW, Washington, D.C. 20552

RE: FOIA Request #CFPB-2019-0458-REM

November 24, 2021

Mr. Austin Evers

American Oversight
1030 15th Street NW, Suite B255
Washington, DC 20005

Via email: foia@americanoversight.org

Dear Mr. Evers:

This letter is in final response to your Freedom of Information Act (FOIA) request, on remand, dated November 3, 2021. Your request was remanded to:

- with respect to the document found on page 3, and the FOIA Office is directed to release that document to you in full.
- with respect to the documents found on pages 4, 144, 152, 286, 287-295, and 300. For those documents, your Request is remanded to the FOIA Office for it to determine whether releasing the documents would foreseeably cause harm.

Of the 15 pages on remand, I have determined that 13 pages of the records are granted in full and 2 pages are granted in part, pursuant to Title 5 U.S.C. § 552 (b)(5).

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I determined that portions of the responsive documents qualify for protection under the

- Deliberative Process Privilege
  The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

You may appeal any of the responses or decisions set forth above. If you choose to file an appeal, you must do so within 90 calendar days from the date of this letter. Your appeal must be in writing, signed by you or your representative, and should contain the rationale for the appeal. You may send your appeal via the mail (address below) or email (foia@consumerfinance.gov).

Your appeal should be addressed to:

Consumer Financial Protection Bureau
Chief FOIA Officer
Freedom of Information Appeal
1700 G Street, NW
Washington, DC 20552

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, we have waived all fees related to the processing of your request.
reference your FOIA request number above and contact our FOIA Public Liaison via email at FOIA@consumerfinance.gov or by phone at 1-855-444-FOIA (3642).

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Danielle Duvall Adams
FOIA Manager
Office of the Chief Data Officer

1700 G Street NW,
Washington, DC 20552

Decision Memorandum from the Acting Director

FROM	Mick Mulvaney
TO	Kate Fulton, Acting Chief Operating Officer
SUBJECT	Use of logo in implementation of the name correction

I approve the use of a two-mark solution to identify the Bureau: a corrected logo and a seal. The corrected logo will be used in select Bureau materials and on consumerfinance.gov. The seal will be used on official correspondence, legal actions, and reports.

Mick Mulvaney
Acting Director
Bureau of Consumer Financial Protection

6-19-18
Date

* Can we change the color of the beta logo from green to black/grey/whatever (similar to the caps + the words)? Also am wondering if we can drop the "search" part."

cfpb Consumer Financia Protection Bureau
1700 G Street, N.W., Washington, DC 20552

Decision Memorandum from the Acting Director

FROM	Mick Mulvaney
TO	Dana James, Acting Chief Financial Officer
SUBJECT	Anticipated Contract Actions for December and January

Please proceed with executing the anticipated contract actions for December and January.

CFPB

Mick Mulvaney
Acting Director
Consumer Financial Protection Bureau

12-14-17
Date

Approved as to all except

CEE / Procurement Admin. Action / $1,145,546.09

· CEE / Training & Tech Assistance / TBD

Operations / Info. Tech. Serv. Mgmt Software / $1,092,430

Please see sheet for more info on these 3. TX. Mick

cfpb Consumer Financia Protection Bureau
1700 G Street, N.W., Washington, DC 20552

Decision Memorandum from the Acting Director

FROM	Mick Mulvaney
TO	Dana James, Acting Chief Financial Officer
SUBJECT	Anticipated Contract Actions for December and January

Please proceed with executing the anticipated contract actions for December and January.

MM CFPB

Mick Mulvaney
Acting Director
Consumer Financial Protection Bureau

12-14-17
Date

Approved as to all except

CEE / Procurement Admin. Action / $1,145,546.09

· CEE / Training & Tech Assistance / TBD

Operations / Info. Tech. Serv. Mgmt Software / $1,092,430

Please see sheet for more info on these 3. TX. MM

Congress of the United States
Washington, DC 20515

June 19th, 2018

Acting Director Mick Mulvaney
Consumer Financial Protection Bureau
1700 G St. NW
Washington, D.C. 20552

Dear Acting Director Mulvaney,

We are deeply concerned about your recent decision to fire all 25 members of the Consumer Financial Protection Bureau's ("CFPB") Consumer Advisory Board. Your decision to hastily fire the members of the Consumer Advisory Board ("Board") are deeply concerning as the Board provides outside expertise on areas of consumer finance, trends in the financial sector that affect the everyday consumer and the impact of CFPB's regulations. The Dodd-Frank Wall Street Reform and Consumer Protection Act envisioned a consumer advisory board that encompasses well-informed professionals that focus on increasing financial inclusion, ensuring fair access to financial services products and provided valuable insight about the consumer finance industry.

Section 1014 of Dodd-Frank establishes the Consumer Advisory Board and sets forth the requirements for the Board's make-up, how of
providing travel expenses to board members. S
membership of the Advisory Board should ha
services, community development, fair lendin
representatives of depository institutions that
representatives of communities that have beer
loans. Congress identified these specific expe
CFPB on the best and safest practices in prote
fewer than 6 of the members shall be appointe
Reserve Bank Presidents, on a rotating basis.
regional Federal Reserve Banks that you wou
or if you requested that they provide you with
seats.

We do need to respond to this, so they leave directive it to the CBCFP instead of OMB.
—(W)

We would like clarification on why yo
plan for how you intend to fill the vacant seat
established by Dodd-Frank. Sources revealed that a CFPB Official, Anthony Welcher, reasoned the termination was to save costs by eliminating travel expenses. We would like to direct you to Section 1014(d)(2), which provides reimbursement for travel for Board members who are not employed by an agency of the federal government.

It is our hope that you understand the Dodd-Frank law in its entirety, especially when making major decisions that affect Americans' financial livelihood. The CFBP was created to protect American's from financial scams and unfair and deceptive practices that often prey on vulnerable populations and erode the financial health of hard-working families. To effectively ensure this mission, CFPB needs an Advisory Board that mirrors the provisions established in

1700 G Street NW,
Washington, DC 20552

August 7, 2018

Recommendation Memorandum for the Acting Director

FROM	Laura Hussain, Assistant General Counsel, 5-7789 Julia Szybala, Senior Counsel, 5-9874 Isabella More, Counsel, 5-7141
THROUGH	John Coleman, Deputy General Counsel Mary McLeod, General Counsel
SUBJECT	Response Letter to Senators Crapo and Brown regarding data collection

Recommendation(s)

We recommend that you review and sign the attached letter to Senators Crapo and Brown regarding the Bureau's data collection activities.

Background

On June 11, 2018, the Bureau of Consumer Financial Protection received letters from Senate Committee on Banking Housing and Urban Affairs Chairman Michael Crapo and Ranking Member Sherrod Brown requesting certain information regarding the Bureau's data collection activities. (b)(5)

(b)(5)

Attachment(s)

Tab 1: Draft Letter responding to Senators Crapo and Brown
Tab 2: Attachment A – (b)(5)
Tab 3: Letters from Senators Crapo and Brown

1700 G Street NW,
Washington, DC 20552

August 9, 2018

(b)(5)

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing and
Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Crapo: (b)(5)

I write in response to your June 11, 2018 letters regarding the data collection activities of the Bureau of Consumer Financial Protection (Bureau). The Bureau takes privacy and data security very seriously and is pleased to assist the Committee on Banking, Housing, and Urban Affairs with its review of this area. Please see below for responses to the questions presented in your letter.

As you may know, the Office of Management and Budget (OMB) defines personally identifiable information (PII) as any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[1] Therefore, PII includes both direct personal identifiers (DPIs), such as a person's name or account number, as well as any other information that, when combined with other data, could facilitate re-identification, such as zip code, date of birth, and gender.

Your letter references 15 U.S.C. § 6809, a provision of the Gramm-Leach-Bliley Act (GLBA) which pertains to Personally Identifiable Financial Information (PIFI). PIFI is defined in Regulation P as information obtained by a financial institution from or about a consumer, and it excludes information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers.[2] Though the Bureau does, at times, collect PIFI from financial institutions, PIFI possessed by the Bureau is a subcategory of PII, which is a much broader term.

---

[1] OMB Circular No. A-130, App. II; *see also* OMB Memorandum M-17-12.

[2] 12 C.F.R. § 1016.3(q)(1).

For purposes of responding to your questions in an efficient and expedient manner, the Bureau's responses focus on PII collected from or relating to consumers pursuant to the Bureau's authorities under consumer financial protection law.[3]

1. Describe what types of and how much PII your organization collects on individuals.

Most of the Bureau's mission-related work is conducted by three divisions: (1) the Division of Supervision, Enforcement, and Fair Lending, which is responsible for conducting supervisory, fair lending, and enforcement activities; (2) the Division of Research, Markets, and Regulations, which is responsible for conducting research, for monitoring the consumer financial products and services markets, and for developing, implementing, and assessing regulations; and (3) the Division of Consumer Education and Engagement, which is responsible for providing financial education to consumers and for collecting, monitoring, and responding to consumer complaints regarding consumer financial products or services. All of this work is informed by the use of data, including PII, as discussed in more detail below.

Though collection of PII is necessary for much of the Bureau's mission-related work, the Bureau seeks to minimize the use of DPIs. The Bureau does not monitor the accounts of particular consumers and does not track the financial habits or activities of any individual consumer. Instead, in the normal course of fulfilling its statutory obligations, the Bureau:

- Collects information about accounts from consumers who seek the Bureau's help through the consumer response function and from the institution involved in the complaint;
- Collects information in connection with supervisory examinations or enforcement activity, as well as from whistleblowers;
- Performs market monitoring activities, which involve the analysis of market trends and risks to consumers;
- Assesses the effectiveness of its significant rules; and
- Conducts consumer surveys, focus groups, and interviews of consumers as part of its research function, including research to inform rulemaking and consumer financial education activities.

[3] Other collections of PII that the Bureau may hold are therefore not addressed in this response; for example, human capital data related to Bureau employees, or PII provided by individuals making Freedom of Information Act requests.

2. Describe how many individuals' PII your organization possesses.

As noted above, the Bureau does not monitor the accounts of particular consumers and does not track the financial habits or activities of any individual consumer. Since much of the data collected by the Bureau does not contain DPIs, the Bureau cannot link these records to individual consumers. It is therefore not possible for the Bureau to determine how many consumers' PII the Bureau possesses across various de-identified datasets. Furthermore, PIFI obtained through supervisory and enforcement activities is maintained separately by activity rather than by individual.

3. Explain what your organization does with the PII it collects and possesses.

In the normal course of carrying out its statutory functions and obligations, the Bureau collects PII for purposes of writing rules, supervising financial institutions, and enforcing the law; taking consumer complaints; providing financial education; researching the consumer experience of using financial products; and monitoring financial markets for new risks to consumers; and conducting assessments of significant rules. The Bureau minimizes privacy risk by de-identifying data when possible or when required by law, by restricting access to PII, by providing training to personnel on the appropriate use and disclosure of information, and by maintaining information in secure environments.

4. Describe how your organization protects PII it possesses.

The Bureau protects PII through a combination of internal controls, policies and procedures, and technologies that are designed to minimize the risk of an accidental disclosure or an intentional breach by a malicious actor and, should either of those events occur, to minimize the damage to an individual's privacy interests.

Following industry and government best practices, the Bureau has robust data governance processes and policies for each stage of the data lifecycle. These processes and policies govern, among other things, how information and data are: (1) brought into the Bureau (*e.g.*, the types of data that can be collected, how the data may be used), (2) securely stored, classified, and accessed, (3) shared internally across Divisions, and (4) publicly disclosed. Additional information on these categories is provided below.

At the collection stage, the Bureau has a Data Intake Group (DIG), which includes representatives from the privacy team and is responsible for vetting and approving proposed data intakes prior to collection. The DIG reviews proposed data collections for compliance with applicable laws and policies and makes recommendations to the Chief Data Officer (CDO) regarding whether to approve a proposed collection.

For some routine data intakes that are a normal part of the Bureau's work and operation, the CDO has granted the relevant operational office independent authority for each individual intake within the governance framework. For example, Consumer Response has been delegated data governance responsibilities for consumer complaints, and Supervision and Enforcement have been delegated data governance responsibilities for data specific to their supervisory and

enforcement activities, respectively. Each office creates an annual report on its policies, procedures, and activities pertaining to data governance. The CDO conducts an annual review of each office's data governance.

While PII resides on or traverses systems under the Bureau's custody or control, the Bureau adheres to the Risk Management Framework (RMF) prescribed by the National Institute of Standards and Technology (NIST) to determine the appropriate protections, assessment techniques, and authorization decisions necessary to operate Bureau systems within acceptable levels of risk. Generally, when evaluating systems and services for use, the Bureau adopts an approach to validate and leverage multiple layers of security services and protections, which include technologies and procedures as necessary. Technologies include, but are not limited to, firewalls, encryption, intrusion detection, identity management, access restrictions, threat intelligence feeds, antivirus, vulnerability scanning, and log analysis. If residual risks or control gaps exceed an acceptable level of risk to the Bureau, the Bureau implements supplemental controls or usage restrictions to further mitigate risk.

As additional validation of the effectiveness of security controls, in January of 2018, the Bureau signed an Interagency Agreement with the Department of Defense to leverage Risk and Vulnerability Assessment (RVA) services as a mechanism to identify potential gaps in cybersecurity controls. This is the same service the Department of Homeland Security (DHS) provides to other Federal agencies to assess technical vulnerabilities beyond those identified in their Cyber Hygiene program, in which the Bureau also participates. RVA testing has been completed with no "Critical" findings identified by the assessors, and only three technical recommendations. Of the three recommendations made by the assessors, the Bureau is already actively remediating all three.

The Bureau also protects PII through processes designed to minimize privacy risks for released data. The Bureau has a Data Release Group (DRG) that coordinates the review of potential data disclosures to the public. Among other things, the DRG assesses whether disclosures of data are legally permissible and sufficiently secure, and it minimizes re-identification risk that may be associated with the data.

The Bureau's Office of the Inspector General (OIG) completed an audit of the Bureau's privacy program in February 2018. In the report, the OIG determined that the Bureau has substantially developed, documented, and implemented a privacy program that addresses applicable federal privacy requirements and security risks related to collecting, processing, handling, storing, and disseminating sensitive privacy data.[4]

5. Describe your organization's policies for (a) data security, (b) data retention, and (c) data destruction.

Attached are the Bureau's Information Governance Policy, Information Security Program Policy, Records and Email Management Policy, and Data Destruction Policy. Federal records,

[4] https://oig.federalreserve.gov/reports/cfpb-privacy-program-feb2018.pdf

which include data collected by the Bureau, are subject to the Bureau's Records Retention Policy, which is also attached.

The Bureau's Information Security Program Policy is derived from the controls described in NIST Special Publication 800-53 Revision 4, titled "Security and Privacy Controls for Federal Information Systems and Organizations," as well as other relevant standards and requirements, including NIST Federal Information Process Standards, NIST Special Publications, OMB memoranda, executive orders, and DHS Binding Operational Directives. In addition, the program executing the Information Security Program Policy is aligned to the NIST Cybersecurity Framework as directed by Executive Order 13800.

6. Identify all sources from which your organization obtains PII, and, for each source, the statutory authority under which PII is collected.

The Bureau has five main external sources of data: the public domain, other agencies, commercial vendors, financial institutions, and consumers.

Below is a chart listing the most commonly used authorities under which the Bureau collects data, which may include PII.

Category of Data	Sub-Category	Dodd-Frank Act Authority
Consumer Complaints		1013(b)(3), 1034
Confidential Investigative Information (CII)	Civil Investigative Demand Material	1052
	Memoranda of Understanding (MOUs)/Access requests	1022(c)(6), 1052
	Other CII	1052, 1053
Confidential Supervisory Information	Supervisory requests	1024, 1025, 1026
	MOUs/Access requests	1022(c)(6), 1024, 1025, 1026
Market Monitoring Orders		1022(c)(1), 1022(c)(4)(b)(ii)
Market Monitoring	General	1022(c)(1), 1022(c)(4)(b)(i)
	Procurements	1022(c)(1), 1022(c)(4)(b)(i)
Assessment Orders		1022(d), 1022(c)(4)(b)(ii)
Assessment		1022(d), 1022(c)(4)(b)(i)

7. Identify your organization's outstanding contracts with third party vendors as it pertains to data collection.

The Bureau sometimes purchases commercially available data from third-party vendors. This approach can help reduce industry burden and is generally more cost effective than conducting a new survey or collection. Some of the datasets are "off the shelf" products that are available for purchase by anyone in the private sector or government. Other products are customized for the Bureau. Access to, and reuse of, these datasets is restricted in accordance with applicable license agreements.

A list of vendors with which the Bureau has outstanding contracts involving the purchase and collection of relevant data is included in Attachment A.

8. Describe how your organization ensures that data it relies on that is collected or stored by third party vendors is protected.

The Bureau validates compliance with cybersecurity policy and processes through the Bureau's contracts with each third-party service provider for data collected on behalf of the Bureau. The Bureau includes both cybersecurity- and privacy-specific clauses in contracts that include or otherwise affect the creation, collection, maintenance, use, or transfer of PII. All IT products and services provided by the contractor must comply with applicable federal laws and standards addressing information security and privacy.

When considering the cybersecurity risk of a new third-party service provider, the Bureau first consults, and prefers to use, the offerings under the Federal Risk and Authorization Management Program (FedRAMP) that have received FedRAMP authorization. If necessary, the Bureau also reviews relevant, available, and comparable information (*e.g.*, FedRAMP security packages, assessment reports and findings, SSAE-18 reports, security monitoring results). The Bureau will also conduct technical testing where feasible to ensure security controls are commensurate with Bureau standards. If the combination of security controls is deemed appropriate for the level of system risk, the Bureau will authorize the system's operation for Bureau use. Once the Bureau has granted an Authorization to Operate for a third-party system, the Office of Cybersecurity applies the Bureau's Information Security Continuous Monitoring (ISCM) process to manage any changes to the risk profile of the system throughout the duration of its use by the Bureau. If new or unanticipated threats, vulnerabilities, or risks affecting security of the service are discovered, the findings are reviewed by the Bureau-assigned Information System Security Manager (ISSM), risks are documented, and appropriate protections are instituted.

9. How much does your organization spend on data collection and protection? Please share with us any reports or documentation that describe how much institutions and individuals that provide data to your organization spend on reporting and providing such data.

For FY 2018, the budget for the Office of Technology & Innovation included the following items, which account for much of what the Bureau spends on data collection and protection: (1)

$600,000, reflecting the non-personnel budget for collecting data associated with the Home Mortgage Disclosure Act (HMDA); (2) $8,250,000, reflecting the non-personnel budget for the Office of Cybersecurity plus the cost of the RVA described earlier; and (3) $9,900,000, reflecting the non-personnel budget for the Chief Data Office, which oversees data governance, privacy, compliance, processing, storage, distribution, and analytics. These numbers do not reflect the costs incurred by other Bureau offices that routinely collect data, such as the Office of Consumer Response. Nevertheless, those Offices adhere to the Bureau's cybersecurity and data governance controls with respect to the data they collect. These costs also do not include investments in technical areas (*e.g.*, network infrastructure, cloud services, personnel screenings) that enable layers of cybersecurity controls but are not directly operated by personnel in the Office of Cybersecurity.

When an information collection request is subject to the Paperwork Reduction Act (PRA), the cost to institutions and individuals for reporting data is documented as a burden estimate for each request. The burden associated with each request is documented in the PRA documentation, which can be found on OMB's public docket at https://www.reginfo.gov/public/do/PRAMain. The Bureau does not currently collect information on the cost of compliance with market monitoring or assessment requests that are not subject to the PRA. The Bureau also does not require entities or individuals to track or provide information on the cost of compliance with Bureau investigatory or supervisory requests. We did, however, recently seek potentially relevant information as part of a call for evidence in which the Bureau issued a series of Requests for Information (RFI) seeking comment on its enforcement, supervision, rulemaking, market monitoring, and education activities.[5] The Bureau is currently evaluating information received as a part of its comprehensive review of comments on the RFIs.

10. Does your organization sell any of the PII it possesses, to whom, and under what terms?

No.

11. Has your organization experienced any data breaches in the previous three years? If so, explain how many and provide details of the nature of each.

The Bureau is not aware of any attacks from outsiders that resulted in third parties gaining access to non-public data without appropriate authorization. The Bureau has also not experienced a "major incident" as that term is defined by FISMA and OMB Memorandum M-18-02.

---

[5] https://www.consumerfinance.gov/policy-compliance/notice-opportunities-comment/open-notices/call-for-evidence/

OMB defines "breach" broadly to, among other things, include instances in which a person other than an authorized user accesses or potentially accesses PII.[6] In total, as of March 2018, the Bureau had experienced 175 confirmed breaches of PII in fiscal years 2016, 2017, and 2018.[7] More than half of these breaches of PII have occurred in connection with the Bureau's consumer response function, through which the Bureau has handled more than 1.5 million complaints. Those confirmed breaches have generally occurred in one of three ways: (1) the Bureau fails to follow internal processes and provides an update to a consumer about their complaint prior to receiving three pieces of information that would validate the consumer's identity; (2) the Bureau attaches an incorrect document to a consumer's complaint; or (3) the Bureau sends an unencrypted email to the wrong consumer. Breaches occurring outside of the consumer response function typically occur when the Bureau sends an email including PII to the wrong individual, either inside or outside the Bureau.

Almost all breaches (approximately 90 percent) involved one or more of the following data elements: first name, last name, email address, phone number, or account number. For almost all of these breaches, the number of individuals potentially impacted by each breach is most likely one. This means that those breaches each involve separate pieces of information and no multiple data lapses occurred for any breach.

It is also important to note that, as stated above, the Bureau uses the broad definition of PII promulgated by OMB when referring to confirmed breaches (meaning that PII encompasses any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual).

***

Should you have any questions about this response, please have your staff contact Laura M. Hussain in the Bureau's Legal Division or Matthew Pippin in the Bureau's Office of Legislative Affairs. Ms. Hussain can be reached at (202) 435-7789, and Mr. Pippin can be reached at (202) 435-7552.

Sincerely,

Mick Mulvaney
Acting Director

---

[6] OMB Memorandum M-17-12.

[7] The most recent FY 2018 statistics cover a period ending March 2018.

Attachment A: Third Party Vendors

2M Research Services LLC
Argus Information and Advsy Srs LLC
Columbia University
Comperemedia Inc
Experian Information Solution Inc
Feshbach Advisory Partners LLC
Fors Marsh Group LLC
Gettysburg College
ICF Macro Inc
Informa Business Intelligence Inc.
Informa Research Services Inc
JD Power
Mathematica Policy Research Inc
McDash Analytics LLC
Mercator Advisory Group Inc
Middlebury College
Mortgage Bankers Association
National Opinion Research Center
OCLC Inc
Powerlytics Inc.
Rand Corporation
RELX Inc
Research Triangle Institute
S&P Global Market Intelligence Inc
State Regulatory Registry LLC
University of Pennsylvania

Hold
we are no longer responding, substantively, to letters addressed to me @ OMB.

1700 G Street NW,
Washington, DC 20552

June 22, 2018

Recommendation Memorandum for t

FROM	Dara Goodman, Counsel, 5-7490 Laura Hussain, Assistant General Counsel, 5-7789 John Coleman, Deputy General Counsel, 5-7254
THROUGH	Mary McLeod, General Counsel
SUBJECT	Letters to Senator Brown et al regarding Office for Students

Recommendation(s)

We recommend that you review, approve, and sign the attached letters, which respond to a letter from Ranking Member Brown, Senator Patty Murray, Senator Richard J. Durbin, Senator Elizabeth Warren, Senator Richard Blumenthal, Senator Kirsten Gillibrand, Senator Mazie K. Hirono, and Senator Jack Reed regarding the Office for Students.

Background

The Bureau recently received a letter on May 18, 2018 from Ranking Member Brown and others regarding the plan to fold the Office for Students in to the Office of Financial Education. The response letters and incoming letter are attached.

Attachments

Tab 1: 2018.06.22 MM to Brown_Office for Students