From: Melissa Ball <Melissa.Ball@coag.gov>
Sent: Thursday, August 9, 2018 5:15 PM
To: Riemer, Jeffrey (Justin)
Cc: Styles, Kathleen; Kang, Soo; 'jennifer.levy@kirkland.com'; Kilgarriff, Mike (mike.kilgarriff@kirkland.com); Alissa Gardenswartz; Jennifer Hunt; Jennifer Dethmers
Subject: Request for Records: In the Matter of Navient - Letter from Jennifer Miner Dethmers
Attachments: 2018-08-09 Letter to J Riemer Dept of Ed re req for records.pdf

Good afternoon.

Please find attached a letter from Jennifer Miner Dethmers re: the Colorado Attorney General's request for records sent to the U.S. Department of Education on June 1, 2018. A hard copy was also sent to you via U.S. Mail. Thank you.

Melissa Ball
Paralegal
Consumer Protection Section
Colorado Attorney General's Office
1300 Broadway, 7th Floor
Denver, CO 80203
(720) 508-6229
Melissa.Ball@coag.gov
FAX: (720) 508-6040

Please note my email address has changed to melissa.ball@coag.gov

CYNTHIA H. COFFMAN
Attorney General

MELANIE J. SNYDER
Chief Deputy Attorney General

LEORA JOSEPH
Chief of Staff

FREDERICK R. YARGER
Solicitor General

STATE OF COLORADO
DEPARTMENT OF LAW

RALPH L. CARR
COLORADO JUDICIAL CENTER
1300 Broadway, 10th Floor
Denver, Colorado 80203
Phone (720) 508-6000

Consumer Protection Section

August 9, 2018

J. Justin Riemer
Deputy General Counsel
Postsecondary Education
U.S. Department of Education
400 Maryland Ave., SW
Washington, DC 20202

VIA ELECTRONIC MAIL (jeffrey.riemer@ed.gov) and U.S. MAIL

RE: Request for Records: *In the Matter of Navient* (Matter #2017-LWCP-115960)

Dear Mr. Riemer:

I am writing to follow up on the Colorado Attorney General's request for records pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, sent to the U.S. Department of Education (the "Department") on June 1, 2018.

On January 29, 2018, our office issued a subpoena to Navient Solutions, LLC ("Navient Solutions"). Navient Solutions refused to provide information related to Department loans serviced by Navient Solutions based on, in part, the Department's December 24, 2017, directive. On April 18, 2018, Jennifer G. Levy, P.C., sent you a letter regarding to our request, which included a copy of our subpoena. I have attached a copy of this letter.

On May 14, Soo Kang sent us the Department's response, directing us to submit a request directly to the Department under the Privacy Act. I have also attached a copy of this letter (without attachments). Our June 1 request (attached) was our response to this directive. While the Department indicated that it would respond to our request as expeditiously as possible, we have not received any response in the two months since we sent our letter.

The lack of a response is hindering our investigation into the conduct of Navient Solutions in Colorado. Please let me know when the Department will respond to our request. Thank you.

Sincerely,

FOR THE ATTORNEY GENERAL

(b)(6)

JENNIFER MINER DETHMERS
Senior Assistant Attorney General
Antitrust, Tobacco, & Consumer Protection Unit
Consumer Protection Section
720-508-6216
720-508-6040 (FAX)
Email: jennifer.dethmers@coag.gov

Enclosure

cc: Kathleen Styles, Esq., Chief Privacy Officer
U.S. Department of Education
kathleen.styles@ed.gov

Soo Kang, Contracting Officer
U.S. Department of Education
soo.kang@ed.gov

Jennifer Levy, Esq.
Jennifer Levy, P.C.
Kirkland & Ellis LLP
jennifer.levy@kirkland.com

Mike Kilgarriff, Esq.
Kirkland & Ellis LLP
mike.kilgarriff@kirkland.com

Alissa H. Gardenswartz, Esq., Deputy Attorney General
Colorado Department of Law
alissa.gardenswartz@coag.gov

Jennifer H. Hunt, Esq., First Assistant Attorney General
Colorado Department of Law
jennifer.hunt@coag.gov

EXHIBIT A

KIRKLAND & ELLIS LLP
AND AFFILIATED PARTNERSHIPS

655 Fifteenth Street, N.W.
Washington, D.C. 20005

Jennifer Levy, P.C.
To Call Writer Directly:
(202) 879-5211
jennifer.levy@kirkland.com

(202) 879-5000

www.kirkland.com

Facsimile:
(202) 879-5200

April 18, 2018

Via E-Mail

Justin Riemer
Special Counsel
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

Re: Requests for Information Related to Department of Education Loans from Colorado Attorney General

Dear Justin:

On January 29, 2018, the Colorado Attorney General issued a subpoena to Navient Solutions. The subpoena is attached for your review. The subpoena seeks, among other things, the production of information related to Department of Education loans serviced by Navient Solutions. In accordance with the Department's directive from December 24, 2017, we have indicated to the State that Navient Solutions is not at liberty to produce such information, and that the request should be made directly to the Department. Colorado, copied here, has requested we make this request on their behalf.

Please let us know if you have any questions. We are happy to arrange a call if you would like to discuss further.

Sincerely,

(b)(6)

Jennifer G. Levy, P.C.

cc: Jennifer Miner Dethmers
Jennifer H. Hunt

STATE OF COLORADO ATTORNEY GENERAL	
IN THE MATTER OF NAVIENT (MATTER #2017-LWCP-115960)	
CYNTHIA H. COFFMAN, Attorney General JENNIFER H. HUNT, #29964* First Assistant Attorney General JENNIFER MINER DETHMERS, #32519* Senior Assistant Attorney General COLORADO DEPARTMENT OF LAW Consumer Protection Section Ralph L. Carr Colorado Judicial Center 1300 Broadway, 7th Floor Denver, CO 80203 Telephone: 720-508-6228 Facsimile: 720-508-6040 Emails: jennifer.hunt@coag.gov jennifer.dethmers@coag.gov *Counsel of Record	
SUBPOENA	

TO: Navient Solutions, LLC (fka Navient Solutions, Inc.)
2001 Edmund Halley Dr.
Reston, VA 20191

c/o Jennifer Levy
Kirkland & Ellis LLP
655 Fifteenth Street, NW
Washington, DC 20005-5793
Phone: 202-879-5211
Fax: 202-879-5200
Email: jennifer.levy@kirkland.com

YOU ARE HEREBY ORDERED to produce for inspection and copying for the Attorney General of the State of Colorado the documents described below to the Colorado Department of Law, Attn: Jennifer Miner Dethmers, Consumer Protection Section, Ralph. L. Carr Colorado Judicial Center, 1300 Broadway, 7th Floor, Denver, CO 80203, on or before **February 28, 2018, at 4:00 p.m. Mountain time.**

This subpoena is issued pursuant to the Colorado Consumer Protection Act, C.R.S. §§ 6-1-101, *et seq.* ("CCPA"), which grants the Attorney General the power to issue subpoenas and require production of documents when she has reasonable cause to believe that any person has engaged in or is engaging in any deceptive trade practice. *See* C.R.S. §§ 6-1-107 and -108.

Based upon investigative information, the Attorney General has reasonable cause to believe that Navient Solutions, LLC has information related to deceptive trade practices and potential violations of the CCPA, including but not limited to violations of C.R.S. § 6-1-105(1)(g), (e), (i), and (u).

PRESERVATION OF DOCUMENTS

You must preserve all documents, including electronically stored information ("ESI"), related to this investigation. Accordingly, you must take steps to inform your employees, officers, and agents to refrain from modifying, destroying, or otherwise rendering unreadable any relevant documents, including hard copies and ESI. A paper copy or an electronic image (e.g. TIFF or PDF file) of ESI is not an adequate preservation of ESI. ESI should be preserved in the document's native format to preserve metadata.

INSTRUCTIONS

1. Each document request within this subpoena requires a complete search of all documents in your possession, custody, or control (including all ESI, whether stored locally or remotely, and whether stored by you or by another person on your behalf). If there are documents that are not searchable, please contact the attorney signing this subpoena to explain.

2. If you or your agent desires to use software or technology to identify or eliminate potentially responsive documents and information produced in response to this subpoena, including but not limited to search terms, predictive coding or similar technology, deduplication, and email threading, you must provide a detailed description of the method(s) used to conduct any part of the search. If search terms will be used to identify documents responsive to this subpoena, provide the following: (a) a list of the proposed search terms, (b) a list of any proposed date and/or custodian restrictions, (c) a word dictionary or tally list of all the terms that appear in the collection and the frequency with which the terms appear in the collection (both the total number of appearances and the number of documents in which the words appear), (d) a glossary of industry and company terminology (including any slang, abbreviations, or code words related to the topics identified in this subpoena), (e) a description of the search methodology, and (f) a list and description of the software and technology that will be used to execute the search. **It is strongly recommended that you contact the attorney who signed this**

subpoena prior to using such technology to avoid situations that would cause your response to be deemed insufficient.

3. The response to this subpoena must be submitted in the following manner:

a. **Please contact the attorney who signed this subpoena to discuss the appropriate document production protocol.** ESI may not be printed and produced in paper copy, nor may ESI be converted or imaged into any other formats unless agreed to in writing by the attorney who signed this subpoena.
b. Documents must be complete and unredacted, submitted as found in your possession, custody, or control. Paper documents that in their original condition were stapled, clipped, or otherwise fastened together or maintained in separate file folders must be produced in such form.
c. Documents written in a language other than English must be translated into English. Submit the foreign language document with the English language translation attached.
d. PDF files or photocopies may be submitted in lieu of original paper documents (with color versions where necessary to preserve information in the documents).
e. An officer of the company must provide an affidavit stating that all ESI, PDF files, and photocopies produced in response to this request are true, correct, and complete copies of the original documents.
f. The response to each document request must be identified by document request number (and, if applicable, sub-document request number), and segregated from responses to other document requests. Each page of each paper document must be marked with a control number. Any pamphlets, books, or devices containing ESI must each be marked with a single control number. Within the response to a given document request, documents must be organized and identified according to the files (or electronic locations) in which they were kept, maintained or found.

4. Any documents that are withheld in whole or in part from production based on a claim of privilege must be assigned document control numbers (with unique consecutive numbers for each page of each document). You must also provide the reason that such document was withheld (including the specific privilege being claimed), all facts relied on in supporting that reason, and a complete description of each document including: the document control number of the document, the document control numbers of any attached documents (regardless of whether any privilege is claimed for the attached documents), the author(s), addressee(s), date, subject, all recipients (of the original and any copies), its present location(s), and the document request(s) of this subpoena to which the document is responsive. For each

document withheld under a claim that it constitutes or contains attorney work product, state whether you assert that the document was prepared in anticipation of litigation or for trial and, if so, identify the anticipated litigation or trial upon which the assertion is based.

5. If documents responsive to a particular document request no longer exist, but are known to have been in existence, state the circumstances under which they were lost or destroyed, describe the documents to the fullest extent possible, state the document request(s) to which they are responsive, and identify persons having knowledge of the content of such documents.

6. This subpoena is continuing in nature and requires the production of all documents during the relevant period.

7. Any questions you have relating to the scope or meaning of anything in this subpoena should be directed to the attorney who signed this subpoena.

DEFINITIONS

As used in this subpoena, the following terms have the following meanings:

1. The term "agreement" means any oral or written contract, arrangement, or understanding, whether formal or informal, between two or more persons, and shall include any responsive agreement as well as any and all drafts, addenda, corrections, exhibits, modifications, and/or appendixes thereto.

2. The terms "all," "each," and "any" mean "each and every."

3. The terms "and" and "or" have both conjunctive and disjunctive meanings.

4. The term "Colorado borrower or co-signer" means any person (a) who is or was a borrower or co-signer on a student loan originated, serviced, or collected by you; and (b) who has or had an address located in Colorado.

5. The term "communication" means any exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished.

6. The term "consolidation" means consolidating or combining multiple education loans into one loan.

7. The term "deferment" means a program that allows a borrower to temporarily stop making student loan payments or temporarily reduce the amount of student loan payments. During a deferment, the borrower may or may not be responsible for paying interest that accrues on his or her loans.

8. The term "discharge" means the cancellation of a borrower's obligation to repay some or all of the amount owed on a student loan due to certain circumstances and includes, but is not limited to, the following types of discharges: Closed School Discharge, Perkins Loan Cancellation and Discharge, Total and Permanent Disability Discharge, Discharge Due to Death, Discharge in Bankruptcy, False Certification of Student Eligibility or Unauthorized Payment Discharge, Unpaid Refund Discharge, and Borrower Defense Discharge.

9. The term "document" means all written, recorded or graphic materials of every kind,[1] including all ESI. The term "document" includes metadata, embedded, hidden, and other bibliographic or historical data describing or relating to other documents, drafts of documents, copies of documents that are not identical duplicates of the originals, and copies of documents the originals of which are not in your possession, custody, or control.

10. The term "electronically stored information," or "ESI," means all information stored electronically[2] on a computer or any other device,[3] whether on or off your premises (including websites or web services operated by any person, such as web-based email (e.g. Gmail), posts to online services or websites (e.g.

---

[1] "Document" includes but is not limited to address and telephone records, advertisements, appointment books, articles, books, bills, calendars, charts, circulars, checks, contracts, customer lists, diaries, facsimiles, films, financial statements, graphs, indices, invoices, letters, magazines, manuals, memoranda, microfilms, minutes, newspapers, notices, notes, pamphlets, photographs, presentations, press releases, price lists, purchase orders, receipts, reports, security logs, slides, statements of account, studies, surveys, tabulations, tapes, transcripts, records of, or that relate meetings, conferences, and telephone or other conversations or communications, and all other information fixed in a tangible medium of expression, now or at any time in your possession, custody, or control.

[2] "ESI" includes but is not limited to email; text messages; mobile app data; spreadsheets; databases; word processing; images; presentations; any content posted to, uploaded to, or downloaded from any websites or web services; application files; log files; and all other information present on any type of device capable of storing electronic information, including any information recorded automatically and/or surreptitiously by such devices, now or at any time in your possession, custody, or control.

[3] Devices capable of storing ESI include but are not limited to computers, servers, mobile devices, external drives, flash memory devices, telephones, cameras, media players, global positioning system devices, backup disks and tapes, archival storage mediums, and any other form of online or offline storage.

Twitter), social or professional networking sites (e.g. Facebook), document repositories (e.g. Dropbox), and other content repositories (e.g. YouTube)).

11. The term "federal student loan" means a loan funded by the federal government, including Direct Subsidized Loans, Direct Unsubsidized Loans, Direct PLUS Loans, and Federal Perkins Loans.

12. The term "forbearance" means a program that allows a borrower to temporarily stop making student loan payments or temporarily reduce the amount of student loan payments without the loan going into default. During a forbearance, the borrower is responsible for paying the interest that accrues on his or her loans.

13. The term "forgiveness" means the cancellation of a borrower's obligation to repay some or all of the remaining amount owed on a student loan. The term includes, but is not limited to, types of forgiveness where the borrower works full-time for a specified time period in certain occupations or for certain types of employers, including but not limited to, the Teacher Loan Forgiveness Program and Public Service Loan Forgiveness Program.

14. The term "identify" means to provide a person's full name, all current or last known addresses, telephone numbers, and email addresses. When used in the context of an individual, the term "identify" means to provide the individual's current or last known business affiliation and position.

15. The terms "Income-Driven Repayment Plan" and "IDR Plan" mean any repayment plan that sets a borrower's monthly student loan payment at an amount intended to be affordable based on income and family size, such as an Income-Based Repayment Plan ("IBR Plan"), Income-Contingent Repayment Plan ("ICR Plan"), Pay As You Earn Repayment Plan ("PAYE Plan"), or Revised Pay As You Earn Repayment Plan ("RPAYE Plan").

16. The terms "Income-Sensitive Repayment Plan" and "ISR Plan" mean a federal program available to low-income borrowers who have Federal Family Education Loan Program Loans. The payments under an ISR Plan increase or decrease based on a borrower's annual income.

17. The term "person" includes any natural person, proprietorship, corporation (public, municipal, for profit, or not for profit), governmental agency, political subdivision, partnership, association, cooperative, company, joint venture, trust, and any other legal entity. With respect to a business entity, the term "person" includes any natural person acting formally or informally as an employee, officer, agent, attorney, or other representative of the business entity.

18. The term "private student loan" means a non-federal student loan, made by a lender such as a bank, credit union, state agency, or school.

19. The term "rehabilitation" means a program where the borrower agrees to make payments toward a student loan subject to certain conditions during a specified period of time. Once the borrower has made the required payments, the default status will be removed from the student loan; collection activities through wage garnishment or Treasury offset will stop; benefits such as deferment, forbearance, choice of repayment plans, and loan forgiveness may be available; and the default record on the rehabilitated loan will be removed from the borrower's credit history.

20. The terms "relate to" and "relating to" mean in whole or in part constituting, containing, concerning, discussing, embodying, reflecting, mentioning, describing, analyzing, identifying, stating, referring, dealing with, or in any way pertaining to, and without limitation, in any way legally, logically, or factually connected with the matter discussed.

21. The term "repayment plan" means any plan for repaying a student loan, including but not limited to, a Standard Repayment Plan, a Graduated Repayment Plan, an Extended Repayment Plan, an Income-Driven Repayment Plan ("IDR Plan"), and an Income-Sensitive Repayment Plan ("ISR Plan").

22. The terms "you," "your," and "Navient" mean Navient Solutions, LLC fka Navient Solutions, Inc., including any other name pursuant to which Navient conducts business, and any of its parents (including but not limited to Navient Corporation), predecessors (including but not limited to SLM Corporation and Sallie Mae, Inc.), subsidiaries, or affiliates. The terms further comprise any officers, directors, managers, partners, employees, or owners, and any predecessors or successors in interest to such officers, directors, managers, partners, employees, owners, or affiliates. The terms further comprise any persons acting on behalf of or under the direction, authorization, or control of Navient.

23. The plural form of any word shall include the singular form and the singular form shall include the plural. Any reference to male or female pronouns shall constitute a reference to both male and female pronouns.

24. All definitions included within the CCPA are incorporated by this reference and any term defined in the CCPA has the same meaning when used in this subpoena.

25. Unless otherwise stated, this subpoena requests documents from January 1, 2013, to the date of the production of all responsive documents. Documents included in this relevant period are those which were prepared, sent,

dated, received, in effect, or came into existence at any time during the relevant period.

DOCUMENTS TO BE PRODUCED

1. All complaints you received from or about consumers relating to student loans of Colorado borrowers or co-signers, including but not limited to, any aspect of the student loan origination, servicing, and collection processes, and your response to those complaints or inquiries. This request includes documents referenced in or attached to the complaints and responses. This request also includes complaints or inquiries you received – either directly or indirectly – from the Consumer Financial Protection Bureau (the "Bureau") or other federal law enforcement or regulatory agency, any state law enforcement or regulatory agency, any elected or appointed governmental official, any consumer advocacy organization, any educational institution (whether public, private, non-profit, or for-profit), any attorney or other borrower representative, and the Better Business Bureau or similar organization relating to the student loan of a Colorado borrower or co-signer.

2. Documents you produced to the Bureau in response to any investigative subpoena, data request, civil investigative demand, discovery request, or other demand.

3. Transcripts of and exhibits to any deposition or other sworn testimony that you took of the Bureau or its representatives in connection with *Consumer Financial Protection Bureau v. Navient Corp., et al.*, Case No. 3:17-cv-00101-RDM (M.D. Pa.).

4. Documents reflecting the status of all student loans obtained by Colorado borrowers or co-signers who complained about the student loan process or who are delinquent or in default on their student loans. This request includes all Colorado borrowers and co-signers identified in your response to Request No. 1 as well as the following information:

   a. Identification of the borrower;
   b. Whether there is a co-signer and, if so, the identification of the co-signer;
   c. Loan amount;
   d. Date loan was originated;
   e. Type of loan, including whether the loan is a private or a federal student loan;
   f. All repayment, deferment, forbearance, discharge, forgiveness, and cancellation plans applied for by the Colorado borrower or co-signer, the date of the application, whether the application was granted or

denied, the date the application was granted or denied, and if denied, the reason(s) for denial;

g. All repayment, deferment, forbearance, discharge, forgiveness, and cancellation plans entered into by the Colorado borrower or co-signer, including the type and terms of the plan and the date the borrower or co-signer entered the plan;
h. All rehabilitation plans applied for by the Colorado borrower or co-signer, the date of the application, whether the application was granted or denied, the date the application was granted or denied, and if denied, the reason(s) for denial;
i. All rehabilitation plans entered into by the Colorado borrower or co-signer, including the type and terms of the rehabilitation plan and the date the borrower or co-signer entered the rehabilitation plan;
j. Payment history, including attempts to pay past due amounts;
k. Collection history;
l. Amount of interest charged;
m. Amount of fees assessed;
n. Consolidation history, if applicable; and
o. Current loan status, i.e., current, delinquent, default, paid in full, forbearance, etc.

5. Documents reflecting all written and oral communications – including but not limited to, call recordings, notes, logs, electronic mail, text or instant messages, and other correspondence – between you and the Colorado borrowers and co-signers identified in documents responsive to Request Nos. 1 and 4. This request includes, but is not limited to, communications about the Colorado borrower's or co-signer's financial situation, including his or her delinquency history and attempts to repay past due amounts; all repayment, forbearance, forgiveness, deferment, cancellation, discharge, or consolidation plans offered or presented to the borrower or co-signer; and all collection efforts, including attempts to collect the "present amount due."

6. For those student loans that had a Colorado co-signer, produce documents reflecting any communication relating to an request for information about the co-signer release, including but not limited to, documents describing the process and requirements to release a co-signer; whether a co-signer release application was filed and, if so, the date of application; the status of the application; whether the application was granted or denied, the date the application was granted or denied, and, if denied, the reason(s) for denial; and inquiries about any aspect of the co-signer release.

7. Documents reflecting all formal or informal training manuals, materials, policies, procedures, processes, guidelines, rules, scripts, and other documents providing instruction or guidance for servicing, processing, and

collecting payments for student loans that you service. This request specifically includes, but is not limited to, documents related to:

a. advising, responding to, and providing or recommending options to Colorado borrowers or co-signers whose student loans are delinquent or in default;
b. advising, responding to, and providing or recommending options to Colorado borrowers or co-signers who indicate they are having or may have difficulty making their student loan payments;
c. handling Colorado borrower or co-signer complaints about any aspect of their student loans, including any complaint escalation processes;
d. co-signer releases, including requirements to release a co-signer such as requirements concerning that the borrower make a certain number of consecutive, on-time principal and interest payments;
e. eligibility, requirements, application, review, and determination processes relating to repayment, forbearance, forgiveness, deferment, cancellation, discharge, and consolidation plans or programs;
f. allocating student loan payments, including allocating payments as requested by the Colorado borrower or co-signer;
g. handling payments between one or more student loans;
h. servicing student loans of Colorado borrowers or co-signers; and
i. collecting on student loans of Colorado borrowers or co-signers that are delinquent or in default, including but not limited to policies, procedures, and guidance regarding requests that you no longer contact the borrower or co-signer by telephone, the frequency of attempts to contact the borrower or co-signer, and the practice of attempting to collect the "present amount due."

8. All marketing, advertising, promotional, and outreach materials, including templates of correspondence to any Colorado borrower or co-signer, regarding the servicing, repayment, and collecting of student loans.

9. Information provided or otherwise generally available to Colorado borrowers and co-signers that you drafted, provided, sent, or authorized relating to or describing repayment, forbearance, forgiveness, deferment, cancellation, discharge, consolidation, and any other options for Colorado borrowers or co-signers who are having trouble making their student loan payments, are not making their student loan payments, or are otherwise in financial distress. This request includes, but is not limited to, information and representations on websites, advertisements, direct mailers, email messages, text messages, flyers, and documents reflecting oral representations by your representatives to Colorado borrowers or cosigners. This request also includes information about qualifying and applying for repayment, forbearance, forgiveness, deferment, cancellation, discharge, consolidation, and any other program; the recertification process; and any other program requirements.

10. Internal or external studies or analyses relating to call times with borrowers or co-signers, including Colorado borrowers or co-signers, who are delinquent, who are in default, or who indicate they are having or may have difficulty making student loan payments.

11. Internal or external studies or analyses relating to the effectiveness (or lack of effectiveness) of communications to borrowers or co-signers, including Colorado borrowers or co-signers. By way of example, this request includes any studies or analyses about whether certain communications are more or less likely to (a) solicit a response from a borrower or co-signer who is delinquent or in default, (b) ensure that borrowers correctly and timely complete any recertification process, (c) successfully obtain a co-signer release, or (d) collect past due amounts or the "present amount due," a figure which includes the next month's payment.

12. Documents describing compensation policies and plans for your customer service representatives, call center representatives, and similar employees who interact with student loan borrowers and co-signers, including any incentive and bonus plans.

13. Documents describing compensation policies and plans for your employees who – either directly or indirectly – supervise, manage, or otherwise have responsibility for employees who interact with student loan borrowers and co-signers, as described above in Request No. 12, including any incentive and bonus plans.

14. State the number of Colorado borrowers or co-signers who were placed into one or more consecutive non-administrative forbearances within the 12 months prior to entering an IDR. As part of your response, provide information about the situation causing the borrower to be placed in the forbearance(s); the number of forbearance(s); the terms of each forbearance, including any fees; the amount of interest capitalized to the loan while in each forbearance; the date the borrower entered into the IDR; and the terms of the IDR, including the interest rate of the IDR and the monthly payment amounts.

15. Documents relating to every time you demanded or requested the "present amount due," which included the following month's payment, from a Colorado borrower or co-signer.

16. Documents relating to compensation you received for originating, servicing, and collecting student loans for Colorado borrowers and co-signers. This request includes, but is not limited to, how your compensation is calculated for originating, servicing, and collecting student loans.

17. Documents between you and the United States Department of Education relating to the servicing or collection of federal student loans, including any guidance, policies, or procedures.

18. Documents relating to the relationship between Navient Solutions, LLC and Navient Corporation.

19. Documents relating to the relationship between Navient Solutions, LLC or Navient Corporation and SLM Corporation or Sallie Mae, Inc.

20. Documents relating to the relationship between Navient and Pioneer Credit Recovery, Inc.

21. Documents relating to the relationship between Navient and General Revenue Corporation.

22. Documents that Navient provided to any educational institution in Colorado, including but not limited to, public, private, and for-profit colleges, universities, and trade schools. This request includes, but is not limited to, materials intended for distribution to students or potential students interested in obtaining or who had obtained student loans.

23. Documents reflecting communications between Navient and any educational institution in Colorado, including but not limited to, public, private, and for-profit colleges, universities, and trade schools relating to Navient's origination, servicing, and collecting of student loans.

DATED this 29th day of January, 2018.

FOR THE ATTORNEY GENERAL
CYNTHIA H. COFFMAN

s/ Jennifer Miner Dethmers

JENNIFER MINER DETHMERS
Senior Assistant Attorney General
jennifer.dethmers@coag.gov
720-508-6216

JENNIFER H. HUNT
First Assistant Attorney General
jennifer.hunt@coag.gov
720-508-6215

EXHIBIT B

May 14, 2018

Via Email

Jennifer H. Hunt
First Assistant Attorney General
Colorado Department of Law
Consumer Protection Section
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 7th Floor
Denver, CO 80203

Re: Colorado Attorney General's Request for Department of Education Records in *In the Matter of Navient,* Matter # 2017-LWCP-115960

Dear Ms. Hunt:

On April 18, 208, Navient forwarded the subpoena in the matter referenced above, issued on January 29, 2018, to the U.S. Department of Education ("Department"), as you requested they do. The Department has instructed its Federal Loan Servicers, such as Navient, that have received third-party requests for Department records subject to the Privacy Act of 1974, as amended, ("Privacy Act") to inform the requesters they need to come to the Department directly with their requests. *See* Letter from Patrick A. Bradfield, Director, Federal Student Aid Acquisitions, Ownership of and Access to U.S Department of Education Records and Data Department of Education Memorandum (Dec. 27, 2017).

In addition, Navient's contract with the Department makes clear that the Department "owns the rights to all data/records produced as part of th[e] contract." Number: FSA-TitleIV-09, Attachment A-2, https://www2.ed.gov/policy/gen/leg/foia/contract/salliemae-061709.pdf. The contract states Navient is to "treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest." *Id.*

Additional provisions of the contract related to records management state that the records produced pursuant to this contract are subject to the Privacy Act. *See id.* ("All data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records and shall be managed in accordance with the Privacy Act (5 U.S.C. 552a).")

Consistent with the Department's earlier instructions and Navient's contract with the Department, Navient asked that you make the request directly with the Department. The Department therefore asks that your organization submit any request for Department data and/or records to the Department directly. In making the request directly to the Department, please

provide the legal basis on which you believe access to the records of the Department can be granted with as much specificity as possible. For example, if you believe the system of records (SOR) from which you seek records has a routine use permitting disclosure of the records, please specify (a) the System of Records from which data access is sought, (b) the routine use upon which you are making the request, and (c) how the request per that routine use is compatible with one or more of the purposes for which the data was collected.

In general, requests made for access to Department data used and/or accessed by ED's Federal Loan Servicers would come from the Common Services for Borrowers (CSB) system (18-11-16). The most recent System of Records Notice (SORN) for the CSB system was published at 81 Fed. Reg. 60683 (Sept. 2, 2016). Your request also seems to request information maintained by the Department's Student Loan Ombudsman. The most recent SORN for the Office of the Student Loan Ombudsman Records (18–11–11) was published at 81 Fed. Reg. 12081 (March 8, 2016).[1] Each SORN lists all routine uses and program purposes. A full list of all SOR/SORN for the Department can be found at https://www2.ed.gov/notices/ed-pia.html.

If your organization believes that CSB Routine use 1(r) is appropriate, please be sure to state specifically the "debt collection, financial, and other applicable statutory, regulatory, or local requirement" on which your request is based, how provision of or access to data/documents under this routine use is compatible with one or more purposes for which the information was collected, as set out in the "Purposes" section of the SORN, and how your organization will maintain Privacy Act safeguards to protect the security and confidentiality of the disclosed records. For any other SOR/SORN, please be as specific as possible in identifying the routine use upon which you are making the request, and how the request per that routine use is compatible with one or more of the purposes for which the data was collected.

If your office believes another Privacy Act exception or routine use from any other SOR/SORN would apply to your request, you may certainly rely on either of those options as well. There is no prohibition on requesting access to Privacy Act protected data by any legally available means.

Once you make the request(s) directly to the Department, the Department can then evaluate the request based on the requirements of the Privacy Act and the Freedom of Information Act, as applicable. The Department will do so as expeditiously as possible, and will notify both the Federal Loan Servicer and your organization of its decision to approve or deny access to the data, or to request additional clarification regarding the request. If you have any questions, please feel free to contact the undersigned.

Sincerely,

(b)(6)

Soo Kang
Contracting Officer

[1] The Ombudsman SORN is due to be published with modifications in the very near future so any requests under that SOR/SORN will need to reference the most recent version.

CC: Jennifer Levy, P.C., Kirkland & Ellis LLP

EXHIBIT C

CYNTHIA H. COFFMAN
Attorney General

MELANIE J. SNYDER
Chief Deputy Attorney General

LEORA JOSEPH
Chief of Staff

FREDERICK R. YARGER
Solicitor General

STATE OF COLORADO
DEPARTMENT OF LAW

RALPH L. CARR
COLORADO JUDICIAL CENTER
1300 Broadway, 10th Floor
Denver, Colorado 80203
Phone (720) 508-6000

Consumer Protection Section

May 31, 2018

Kathleen Styles
Chief Privacy Officer
U.S. Department of Education
Office of the Chief Privacy Officer
400 Maryland Avenue, SW LBJ 2E320
Washington, DC 20202-4536

VIA FACSIMILE (202-401-0920), ELECTRONIC MAIL (kathleen.styles@ed.gov), and U.S. MAIL, FIRST-CLASS, POSTAGE PREPAID

RE: Law Enforcement Agency Request: *In the Matter of Navient* (Matter #2017-LWCP-115960)

Dear Ms. Styles:

Pursuant to the Colorado Consumer Protection Act, C.R.S. § 6-1-101, *et seq.* (CCPA), the Colorado Department of Law is conducting a civil law enforcement investigation into whether Navient Corporation ("Navient Corp."), Navient Solutions, LLC ("Navient Solutions"), Pioneer Credit Recovery, Inc. ("Pioneer"), and General Revenue Corp. ("GRC") engaged in deceptive trade practices. In connection with this investigation, the Consumer Protection Section issued a subpoena to Navient Solutions on January 29, 2018 (the "Subpoena"), a copy of which is attached as Exhibit A.

Navient Solutions objected to the Subpoena in part because several requests purported to seek information from the U.S. Department of Education (the "Department") systems of records regarding borrowers with Federal Direct Loans. Navient Solutions claimed that such information was protected by the Privacy Act of 1974, 5 U.S.C. § 552a (the "Privacy Act"), and governed by Department regulations, policies, and guidelines; therefore, it was unable to produce the all of the responsive information. Navient offered to reach out to the Department on our behalf and sent a letter to the Department on April 18.

We received the Department's response to Navient's letter on May 14. The response instructs us to submit requests for information that may come from Department systems of records directly to the Department. The response further explains that information and records responsive to the Subpoena may come from the Common

Services for Borrowers (CSB) system as well as records maintained by the Department's Student Loan Ombudsman (the "Ombudsman"). In accordance with the Department's directive, I am the Deputy Attorney General for the Consumer Protection Section in the Colorado Department of Law, and am authorized by Colorado Attorney General Cynthia H. Coffman (the "Attorney General") to request that the Department either produce, or authorize Navient Corp. and Navient Solutions (collectively, "Navient") to produce, information and records responsive to the Subpoena pursuant to a law enforcement agency request and applicable routine use exceptions.

The Department asked that we "provide the legal basis on which [we] believe access to the records of the Department can be granted with as much specificity as possible." The Colorado Department of Law believes that providing it with access to the requested records and information is not only permissible pursuant to this law enforcement agency request and routine use exceptions, but that doing so will further the stated purposes for which the Department maintains the records relating to student loan borrowers.

A. Law Enforcement Agency Request

Under 34 C.F.R. § 5b.9(b)(7), the Department may make disclosures without the consent of the subject individual

> [t]o another government agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of such government agency or instrumentality has submitted a written request to the Department specifying the record desired and the law enforcement activity for which the record is sought.[1]

See also 5 U.S.C. § 552a(b)(7). As part of her civil law enforcement authority under the CCPA, the Attorney General seeks the information and records requested in the Subpoena to investigate whether Navient, Pioneer, or GRC engaged in unfair, deceptive, or abusive trade practices.

The Attorney General is responsible for enforcing the CCPA, which prohibits deceptive trade practices. C.R.S. §§ 6-1-103 & 6-1-105. When the Attorney General has cause to believe that any person has engaged or is engaging in any deceptive trade practice, she may (1) examine any property, record, document, account, or

[1] The head of the government agency may delegate the task of requesting documents to other officials, but never below that of a section chief. 40 Fed. Reg. 28949, 28955 (July 9, 1975). The Deputy Attorney General position is akin to a section chief in other state attorneys general offices.

paper she deems necessary, and (2) issue subpoenas to require the attendance of witnesses or the production of documents in aid of any investigation. C.R.S. §§ 6-1-107(1) & 6-1-108(1). Unlike private causes of action, the Attorney General may seek civil penalties in addition to restitution, disgorgement of unjust enrichment, and injunctive relief in any civil law enforcement action. C.R.S. §§ 6-1-110(1) & 6-1-112. Additionally, the Attorney General may bring a civil action to enforce and secure remedies under the Consumer Financial Protection Act of 2010 (the "CFPA"), including 12 U.S.C. §§ 5531 & 5536(a)(1). 12 U.S.C. § 5552(a)(1).

The CCPA is a broad remedial statute designed "to provide prompt, economical, and readily available remedies against consumer fraud." *Western Food Plan, Inc. v. District Court*, 598 P.2d 1038, 1041 (Colo. 1979). The use of deceptive trade practices not only injuriously affects honest businesses and consumers, but it also impacts the general and financial welfare of the state. *People ex rel. Dunbar v. Gym of Am., Inc.*, 493 P.2d 660, 667-68 (Colo. 1972); *see also* C.R.S. § 6-1-105(2) (providing that evidence a person has engaged in deceptive trade practices is prima facie evidence of "intent to injure competitors and to destroy or substantially lessen competition").

The information and records requested in the Subpoena are an important part of the Attorney General's investigation into whether these entities engaged in unfair, deceptive, or abusive practices. One purpose of the CCPA is to "deter the dissemination of misleading information," and the information and records sought will help determine whether Navient disseminated misleading information or engaged in other deceptive trade practices in violation of the CCPA and other laws. *May Dep't Stores Co. v. State*, 863 P.2d 967, 977 n.18 (Colo. 1993). Moreover, because the total outstanding student loan balance in Colorado was $24.75 billion at the end of 2016,[2] if Navient, Pioneer, or GRC have used or are using deceptive trade practices in connection with its student loan servicing and collection practices, such conduct impacts not only individuals but also the general and financial welfare of Colorado.

To the extent that any information or record requested in the Subpoena is subject to the Privacy Act – including but not limited to information regarding borrowers with Federal Direct Loans contained in the CSB, the Ombudsman's system of records, other system of records, or in Subpoena Request Nos. 1, 2, 4, 5, or 14 – the Attorney General respectfully requests that the Department either produce or authorize Navient to produce the requested information and records.

[2] Consumer Financial Protection Bureau, *50 state snapshot of student debt: A nationwide look at complaints about student loans*, Oct. 2017. The Bureau has indicated that, similar to the national average, nearly one in four Colorado borrowers is delinquent.

B. Routine Use Exceptions

The requested information and records also should be disclosed to the Attorney General for routine law enforcement uses. 34 C.F.R. § 5b.9(b)(3); *see also* 5 U.S.C. §552a(b)(3). Disclosure is consistent with the Department's decades-long policy to allow disclosure for routine uses and promotes the reasons for which the Department collects and maintains the information and records.

Appendix B to Title 34, Part 5b sets forth routine uses for the Department's systems of records:

> In the event that a system of records maintained by the Department to carry out its function indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether state or local charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

34 C.F.R. Pt. 5b, App. B, (5); *see also* 40 Fed. Reg. at 28955 (recognizing that disclosures to state and local law enforcement agencies may be established as routine uses). For nearly 20 years, the Department has recognized at least two routine uses for law enforcement purposes that apply to the vast majority of its systems of records:

> (3) **Disclosure for Use by Other Law Enforcement Agencies.** The Department may disclose information to any Federal, State, local, tribal, or foreign agency or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation if that information is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility within the receiving entity's jurisdiction.

> (4) **Enforcement Disclosure.** In the event that information in this system of records indicates, either alone or in connection with other information, a violation or potential violation of any applicable statutory, regulatory, or legally binding requirement, the Department may disclose the relevant records to an entity charged with the responsibility for investigating or enforcing those violations or potential violations.

81 Fed. Reg. 630683, 60687 (Sept. 2, 2016) (stating that law enforcement disclosures are routine uses for CSB system of records).[3]

Moreover, the Department's disclosure of the requested information and records will promote its stated objectives. In September 2016, the Department added a routine use to its CSB system of records that specifically addresses the situation where, as here, one of its contractors receives a subpoena seeking "to verify Department contractors' compliance with consumer protection, debt collection, financial, and other applicable statutory, regulatory, or local requirements." 81 Fed. Reg. at 60683. The Department collects information in the CSB system of records for the following purposes:

> (3) To facilitate default reduction efforts by program participants;
>
> * * *

[3] The Department has determined that the Disclosure for Use by Other Law Enforcement Agencies and Enforcement Disclosure routine uses apply to the following systems of records: **Common Services for Borrowers (CSB)**, 81 Fed. Reg. 630683, 60687 (Sept. 2, 2016); **Office of Student Loan Ombudsman Records**, 81 Fed. Reg. 12081, 12802-03 (Mar. 8, 2016); **Data Challenges and Appeals Solutions System (DCAS)**, 80 Fed. Reg. 56969, 56971 (Sept. 21, 2015); **Person Authentication Service (PAS)**, 80 Fed. Reg. 14981, 14983 (Mar. 20, 2015); **CSB**, 79 Fed. Reg. 54685, 54691 (Sept. 12, 2014); **National Student Loan Data System (NSLDS)**, 78 Fed. Reg. 38963, 38967 (June 28, 2013); **School Participation Division Complaints Tracking System (SPD-CTS)**, 78 Fed. Reg. 12298, 12299 (Feb. 22, 2013; **Federal Student Aid Application File**, 76 Fed. Reg. 46774, 46778 (Aug. 3, 2011); **NSLDS**, 76 Fed. Reg. 37095, 37099 (June 24, 2011); **Common Origination and Disbursement (COD) System**, 75 Fed. Reg. 59242, 59244-45 (Sept. 27, 2010); **Financial Management System (FMS)**, 73 Fed. Reg. 177, 178 (Jan. 2, 2008); **CSB**, 71 Fed. Reg. 3503, 3505 (Jan. 23, 2006); **Return of Title IV Funds on the Web (R2T4OTW)**, 69 Fed. Reg. 44521, 44523 (July 26, 2004); **Federal Student Aid (FSA) Students Portal**, 68 Fed. Reg. 23113, 23115 (Apr. 30, 2003); **Student Authentication Network Audit File**, 66 Fed. Reg. 29420, 29421 (May 30, 2001); **Office of Student Loan Ombudsman Records**, 64 Fed. Reg. 72384, 72399 (Dec. 27, 1999); **Student Account Manager System**, 64 Fed. Reg. 30169, 30169-70 (June 4, 1999). *See also* **Health Education Assistance On-Line Processing System (HOPS)**, 79 Fed. Reg. 36299, 36300-01 (June 26, 2014) (describing similar enforcement routine uses). The Enforcement Disclosure routine use also applies to the Department's **Student Aid Internet Gateway (SAIG), Participation Management System**, 83 Fed. Reg. 8855, (Mar. 1, 2018), and **Integrated Partner Management (IPM) System**. 82 Fed. Reg. 37089, 37092 (Aug. 8, 2017).

> (5) To make, service, collect, assign, adjust, transfer, refer, or discharge a loan or collect a grant obligation;
> (6) To counsel a debtor in repayment efforts;
> *(7) To investigate possible fraud or abuse or verify compliance with program regulations;*
>
> * * *
>
> (12) To verify whether a debt qualifies for discharge, cancellation, or forgiveness;
> (13) To conduct credit checks or respond to inquiries or disputes arising from information on the debt already furnished to a credit-reporting agency;
> (14) To investigate complaints, update information, or correct errors contained in Department records.

Id. at 60685-86 (emphasis added). In response to requests from Federal, State, local, and/or tribal governmental entities, the Department added a new programmatic routine use to more easily accommodate such requests. *Id.* at 60683. This CSB routine use 1(r) allows the Department

> to make disclosures to governmental entities at the Federal, State, local, or tribal levels regarding the practices of Department contractors who have been provided with access to the CSB system (*e.g.*, Federal Loan servicers, including not-for-profit servicers, the Federal Perkins Loan servicer, and private collection agencies) with regards to all aspects of loans and grants made under title IV of the HEA, in order to permit these governmental entities to verify the contractor's compliance with debt collection, financial, and other applicable statutory, regulatory, or local requirements. Before making a disclosure to these Federal, State, local, or tribal governmental entities, the Department will require them to maintain Privacy Act safeguards to protect the security and confidentiality of the disclosed records.[4]

Id. at 60687. Again, the Attorney General's investigation of Navient's compliance with the CCPA falls squarely within the routine use verifying compliance with debt collection or other statutory requirements.

[4] Navient Corp. has access to the CSB system of records. 81 Fed. Reg. at 600685.

Additionally, the Department collects information in the Ombudsman system of records to record complaints and comments, track individual cases through resolution, and assist in resolving disputes, among other things. 81 Fed. Reg. at 12083. In 2016 the Department modified routine uses (2), Disclosure for Use by Other Law Enforcement Agencies, and (3), Enforcement Disclosure, to permit disclosures of information and records for violations of civil or administrative law in addition to violations of criminal law and civil fraud. *Id.* at 12082-83. The current routine uses include the following:

> (3) **Disclosure for Use by Other Law Enforcement Agencies.** The Department may disclose information to any Federal, State, local, or foreign agency or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation if that information is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility within the receiving entity's jurisdiction.
>
> (4) **Enforcement Disclosure.** In the event that information in this system of records indicates, either on its face or in connection with other information, a violation or potential violation of any applicable statutory, regulatory, or order of a competent authority, the Department may disclose the relevant records to the appropriate agency, whether foreign, federal, State, tribal, or local, charged with the responsibility of investigating or prosecuting that violation or charged with enforcing or implementing the statute, Executive order, rule, regulation, or order issued pursuant thereto.

Id. at 12083.

As previously set forth, the Attorney General has responsibility for investigating and enforcing state consumer fraud statutes as well as other state and federal statutes. Thus, disclosing the information and records requested in the Subpoena to the Attorney General are routine uses that advance and promote the purposes for which the Department collected the information.

C. Privacy Act Safeguards

The Department's letter also requests that the Colorado Department of Law explain how it will "maintain Privacy Act safeguards to protect the security and confidentiality of the disclosed records." The Colorado Department of Law takes the position that all investigative information is confidential and exempt from the Colorado Open Records Act pursuant to C.R.S. § 24-72-204(2)(a)(I) & -(IX). *See also* C.R.S. § 24-72-204(1)(b) (noting that records are not allowed for inspection if "inspection would be contrary to any federal statute or regulation"). In the course of our investigations and litigation, our office routinely handles confidential and sensitive information and records involving personally identifiable information, federal tax information, the Health Insurance Portability and Accountability Act (HIPAA), the payment card industry, the Social Security Administration (SSA), and trade secrets.

Our office strictly adheres to robust policies to ensure the security of confidential information. I have attached relevant policies from our Information Technology Unit as Exhibit B and our background check policy as Exhibit C.[5] Moreover, our office is in a secure facility, which only allows access to current employees with valid credentials or to those who pass through a security checkpoint and are escorted throughout the building. Additionally, no person is able to enter any floor without a valid badge or an escort.

In addition, we are able to set up precautions so that any data, information, or record from a Department system of record is accessible only to employees working on the above-referenced investigation. Indeed, we anticipate that we will upload any Department information or record into a secure database, access to which is limited only to those attorneys, investigators, and legal assistants actively working on the investigation as well as those employees in our Information Technology Unit who provide litigation support services. We have contracted with a vendor to oversee the database, which is required to comply with strict security protocols. Of course, we are happy to provide the Department with additional information or discuss implementing additional safeguards to ensure that information and records from any Department system of records are kept in accordance with Privacy Act safeguards.

[5] The policies provided in Exhibit B include the Identification and Authentication Policy, Personnel Security Policy, Physical and Environmental Protection Policy, and Security Awareness and Training Policy.

If the Department would prefer that our office serve a formal subpoena for the requested information and records, we are happy to do so.

Please let me know if you have any questions. You may also contact the attorneys who are leading the investigation, Jennifer Dethmers and Jennifer Hunt, both of whom are copied on this letter. We look forward to your response. Thank you.

Sincerely,

FOR THE ATTORNEY GENERAL

(b)(6)

ALISSA H. GARDENSWARTZ
Deputy Attorney General
Consumer Protection Section
720-508-6204
720-508-6040 (FAX)
Email: alissa.gardenswartz@coag.gov

Enclosures

cc: Soo Kang, Contracting Officer
soo.kang@ed.gov

Jennifer H. Hunt, First Assistant Attorney General
720-508-6215
jennifer.hunt@coag.gov

Jennifer Miner Dethmers, Senior Assistant Attorney General
720-508-6216
jennifer.dethmers@coag.gov

Jennifer Levy, Esq.
Jennifer Levy, P.C.
Kirkland & Ellis LLP
202-879-5211
jennifer.levy@kirkland.com

Mike Kilgarriff, Esq.
Kirkland & Ellis LLP
202-879-5149
mike.kilgarriff@kirkland.com

EXHIBIT A

STATE OF COLORADO ATTORNEY GENERAL	
IN THE MATTER OF NAVIENT (MATTER #2017-LWCP-115960)	
CYNTHIA H. COFFMAN, Attorney General JENNIFER H. HUNT, #29964* First Assistant Attorney General JENNIFER MINER DETHMERS, #32519* Senior Assistant Attorney General COLORADO DEPARTMENT OF LAW Consumer Protection Section Ralph L. Carr Colorado Judicial Center 1300 Broadway, 7th Floor Denver, CO 80203 Telephone: 720-508-6228 Facsimile: 720-508-6040 Emails: jennifer.hunt@coag.gov jennifer.dethmers@coag.gov *Counsel of Record	

SUBPOENA

TO: Navient Solutions, LLC (fka Navient Solutions, Inc.)
2001 Edmund Halley Dr.
Reston, VA 20191

c/o Jennifer Levy
Kirkland & Ellis LLP
655 Fifteenth Street, NW
Washington, DC 20005-5793
Phone: 202-879-5211
Fax: 202-879-5200
Email: jennifer.levy@kirkland.com

YOU ARE HEREBY ORDERED to produce for inspection and copying for the Attorney General of the State of Colorado the documents described below to the Colorado Department of Law, Attn: Jennifer Miner Dethmers, Consumer Protection Section, Ralph. L. Carr Colorado Judicial Center, 1300 Broadway, 7th Floor, Denver, CO 80203, on or before **February 28, 2018, at 4:00 p.m. Mountain time.**

This subpoena is issued pursuant to the Colorado Consumer Protection Act, C.R.S. §§ 6-1-101, *et seq.* ("CCPA"), which grants the Attorney General the power to issue subpoenas and require production of documents when she has reasonable cause to believe that any person has engaged in or is engaging in any deceptive trade practice. *See* C.R.S. §§ 6-1-107 and -108.

Based upon investigative information, the Attorney General has reasonable cause to believe that Navient Solutions, LLC has information related to deceptive trade practices and potential violations of the CCPA, including but not limited to violations of C.R.S. § 6-1-105(1)(g), (e), (i), and (u).

PRESERVATION OF DOCUMENTS

You must preserve all documents, including electronically stored information ("ESI"), related to this investigation. Accordingly, you must take steps to inform your employees, officers, and agents to refrain from modifying, destroying, or otherwise rendering unreadable any relevant documents, including hard copies and ESI. A paper copy or an electronic image (e.g. TIFF or PDF file) of ESI is not an adequate preservation of ESI. ESI should be preserved in the document's native format to preserve metadata.

INSTRUCTIONS

1. Each document request within this subpoena requires a complete search of all documents in your possession, custody, or control (including all ESI, whether stored locally or remotely, and whether stored by you or by another person on your behalf). If there are documents that are not searchable, please contact the attorney signing this subpoena to explain.

2. If you or your agent desires to use software or technology to identify or eliminate potentially responsive documents and information produced in response to this subpoena, including but not limited to search terms, predictive coding or similar technology, deduplication, and email threading, you must provide a detailed description of the method(s) used to conduct any part of the search. If search terms will be used to identify documents responsive to this subpoena, provide the following: (a) a list of the proposed search terms, (b) a list of any proposed date and/or custodian restrictions, (c) a word dictionary or tally list of all the terms that appear in the collection and the frequency with which the terms appear in the collection (both the total number of appearances and the number of documents in which the words appear), (d) a glossary of industry and company terminology (including any slang, abbreviations, or code words related to the topics identified in this subpoena), (e) a description of the search methodology, and (f) a list and description of the software and technology that will be used to execute the search. It is **strongly recommended that you contact the attorney who signed this**

subpoena prior to using such technology to avoid situations that would cause your response to be deemed insufficient.

3. The response to this subpoena must be submitted in the following manner:

a. **Please contact the attorney who signed this subpoena to discuss the appropriate document production protocol.** ESI may not be printed and produced in paper copy, nor may ESI be converted or imaged into any other formats unless agreed to in writing by the attorney who signed this subpoena.
b. Documents must be complete and unredacted, submitted as found in your possession, custody, or control. Paper documents that in their original condition were stapled, clipped, or otherwise fastened together or maintained in separate file folders must be produced in such form.
c. Documents written in a language other than English must be translated into English. Submit the foreign language document with the English language translation attached.
d. PDF files or photocopies may be submitted in lieu of original paper documents (with color versions where necessary to preserve information in the documents).
e. An officer of the company must provide an affidavit stating that all ESI, PDF files, and photocopies produced in response to this request are true, correct, and complete copies of the original documents.
f. The response to each document request must be identified by document request number (and, if applicable, sub-document request number), and segregated from responses to other document requests. Each page of each paper document must be marked with a control number. Any pamphlets, books, or devices containing ESI must each be marked with a single control number. Within the response to a given document request, documents must be organized and identified according to the files (or electronic locations) in which they were kept, maintained or found.

4. Any documents that are withheld in whole or in part from production based on a claim of privilege must be assigned document control numbers (with unique consecutive numbers for each page of each document). You must also provide the reason that such document was withheld (including the specific privilege being claimed), all facts relied on in supporting that reason, and a complete description of each document including: the document control number of the document, the document control numbers of any attached documents (regardless of whether any privilege is claimed for the attached documents), the author(s), addressee(s), date, subject, all recipients (of the original and any copies), its present location(s), and the document request(s) of this subpoena to which the document is responsive. For each

document withheld under a claim that it constitutes or contains attorney work product, state whether you assert that the document was prepared in anticipation of litigation or for trial and, if so, identify the anticipated litigation or trial upon which the assertion is based.

5. If documents responsive to a particular document request no longer exist, but are known to have been in existence, state the circumstances under which they were lost or destroyed, describe the documents to the fullest extent possible, state the document request(s) to which they are responsive, and identify persons having knowledge of the content of such documents.

6. This subpoena is continuing in nature and requires the production of all documents during the relevant period.

7. Any questions you have relating to the scope or meaning of anything in this subpoena should be directed to the attorney who signed this subpoena.

DEFINITIONS

As used in this subpoena, the following terms have the following meanings:

1. The term "agreement" means any oral or written contract, arrangement, or understanding, whether formal or informal, between two or more persons, and shall include any responsive agreement as well as any and all drafts, addenda, corrections, exhibits, modifications, and/or appendixes thereto.

2. The terms "all," "each," and "any" mean "each and every."

3. The terms "and" and "or" have both conjunctive and disjunctive meanings.

4. The term "Colorado borrower or co-signer" means any person (a) who is or was a borrower or co-signer on a student loan originated, serviced, or collected by you; and (b) who has or had an address located in Colorado.

5. The term "communication" means any exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished.

6. The term "consolidation" means consolidating or combining multiple education loans into one loan.

7. The term "deferment" means a program that allows a borrower to temporarily stop making student loan payments or temporarily reduce the amount of student loan payments. During a deferment, the borrower may or may not be responsible for paying interest that accrues on his or her loans.

8. The term "discharge" means the cancellation of a borrower's obligation to repay some or all of the amount owed on a student loan due to certain circumstances and includes, but is not limited to, the following types of discharges: Closed School Discharge, Perkins Loan Cancellation and Discharge, Total and Permanent Disability Discharge, Discharge Due to Death, Discharge in Bankruptcy, False Certification of Student Eligibility or Unauthorized Payment Discharge, Unpaid Refund Discharge, and Borrower Defense Discharge.

9. The term "document" means all written, recorded or graphic materials of every kind,[1] including all ESI. The term "document" includes metadata, embedded, hidden, and other bibliographic or historical data describing or relating to other documents, drafts of documents, copies of documents that are not identical duplicates of the originals, and copies of documents the originals of which are not in your possession, custody, or control.

10. The term "electronically stored information," or "ESI," means all information stored electronically[2] on a computer or any other device,[3] whether on or off your premises (including websites or web services operated by any person, such as web-based email (e.g. Gmail), posts to online services or websites (e.g.

[1] "Document" includes but is not limited to address and telephone records, advertisements, appointment books, articles, books, bills, calendars, charts, circulars, checks, contracts, customer lists, diaries, facsimiles, films, financial statements, graphs, indices, invoices, letters, magazines, manuals, memoranda, microfilms, minutes, newspapers, notices, notes, pamphlets, photographs, presentations, press releases, price lists, purchase orders, receipts, reports, security logs, slides, statements of account, studies, surveys, tabulations, tapes, transcripts, records of, or that relate meetings, conferences, and telephone or other conversations or communications, and all other information fixed in a tangible medium of expression, now or at any time in your possession, custody, or control.

[2] "ESI" includes but is not limited to email; text messages; mobile app data; spreadsheets; databases; word processing; images; presentations; any content posted to, uploaded to, or downloaded from any websites or web services; application files; log files; and all other information present on any type of device capable of storing electronic information, including any information recorded automatically and/or surreptitiously by such devices, now or at any time in your possession, custody, or control.

[3] Devices capable of storing ESI include but are not limited to computers, servers, mobile devices, external drives, flash memory devices, telephones, cameras, media players, global positioning system devices, backup disks and tapes, archival storage mediums, and any other form of online or offline storage.

Twitter), social or professional networking sites (e.g. Facebook), document repositories (e.g. Dropbox), and other content repositories (e.g. YouTube)).

11. The term "federal student loan" means a loan funded by the federal government, including Direct Subsidized Loans, Direct Unsubsidized Loans, Direct PLUS Loans, and Federal Perkins Loans.

12. The term "forbearance" means a program that allows a borrower to temporarily stop making student loan payments or temporarily reduce the amount of student loan payments without the loan going into default. During a forbearance, the borrower is responsible for paying the interest that accrues on his or her loans.

13. The term "forgiveness" means the cancellation of a borrower's obligation to repay some or all of the remaining amount owed on a student loan. The term includes, but is not limited to, types of forgiveness where the borrower works full-time for a specified time period in certain occupations or for certain types of employers, including but not limited to, the Teacher Loan Forgiveness Program and Public Service Loan Forgiveness Program.

14. The term "identify" means to provide a person's full name, all current or last known addresses, telephone numbers, and email addresses. When used in the context of an individual, the term "identify" means to provide the individual's current or last known business affiliation and position.

15. The terms "Income-Driven Repayment Plan" and "IDR Plan" mean any repayment plan that sets a borrower's monthly student loan payment at an amount intended to be affordable based on income and family size, such as an Income-Based Repayment Plan ("IBR Plan"), Income-Contingent Repayment Plan ("ICR Plan"), Pay As You Earn Repayment Plan ("PAYE Plan"), or Revised Pay As You Earn Repayment Plan ("RPAYE Plan").

16. The terms "Income-Sensitive Repayment Plan" and "ISR Plan" mean a federal program available to low-income borrowers who have Federal Family Education Loan Program Loans. The payments under an ISR Plan increase or decrease based on a borrower's annual income.

17. The term "person" includes any natural person, proprietorship, corporation (public, municipal, for profit, or not for profit), governmental agency, political subdivision, partnership, association, cooperative, company, joint venture, trust, and any other legal entity. With respect to a business entity, the term "person" includes any natural person acting formally or informally as an employee, officer, agent, attorney, or other representative of the business entity.

18. The term "private student loan" means a non-federal student loan, made by a lender such as a bank, credit union, state agency, or school.

19. The term "rehabilitation" means a program where the borrower agrees to make payments toward a student loan subject to certain conditions during a specified period of time. Once the borrower has made the required payments, the default status will be removed from the student loan; collection activities through wage garnishment or Treasury offset will stop; benefits such as deferment, forbearance, choice of repayment plans, and loan forgiveness may be available; and the default record on the rehabilitated loan will be removed from the borrower's credit history.

20. The terms "relate to" and "relating to" mean in whole or in part constituting, containing, concerning, discussing, embodying, reflecting, mentioning, describing, analyzing, identifying, stating, referring, dealing with, or in any way pertaining to, and without limitation, in any way legally, logically, or factually connected with the matter discussed.

21. The term "repayment plan" means any plan for repaying a student loan, including but not limited to, a Standard Repayment Plan, a Graduated Repayment Plan, an Extended Repayment Plan, an Income-Driven Repayment Plan ("IDR Plan"), and an Income-Sensitive Repayment Plan ("ISR Plan").

22. The terms "you," "your," and "Navient" mean Navient Solutions, LLC fka Navient Solutions, Inc., including any other name pursuant to which Navient conducts business, and any of its parents (including but not limited to Navient Corporation), predecessors (including but not limited to SLM Corporation and Sallie Mae, Inc.), subsidiaries, or affiliates. The terms further comprise any officers, directors, managers, partners, employees, or owners, and any predecessors or successors in interest to such officers, directors, managers, partners, employees, owners, or affiliates. The terms further comprise any persons acting on behalf of or under the direction, authorization, or control of Navient.

23. The plural form of any word shall include the singular form and the singular form shall include the plural. Any reference to male or female pronouns shall constitute a reference to both male and female pronouns.

24. All definitions included within the CCPA are incorporated by this reference and any term defined in the CCPA has the same meaning when used in this subpoena.

25. Unless otherwise stated, this subpoena requests documents from January 1, 2013, to the date of the production of all responsive documents. Documents included in this relevant period are those which were prepared, sent,

dated, received, in effect, or came into existence at any time during the relevant period.

DOCUMENTS TO BE PRODUCED

1. All complaints you received from or about consumers relating to student loans of Colorado borrowers or co-signers, including but not limited to, any aspect of the student loan origination, servicing, and collection processes, and your response to those complaints or inquiries. This request includes documents referenced in or attached to the complaints and responses. This request also includes complaints or inquiries you received – either directly or indirectly – from the Consumer Financial Protection Bureau (the "Bureau") or other federal law enforcement or regulatory agency, any state law enforcement or regulatory agency, any elected or appointed governmental official, any consumer advocacy organization, any educational institution (whether public, private, non-profit, or for-profit), any attorney or other borrower representative, and the Better Business Bureau or similar organization relating to the student loan of a Colorado borrower or co-signer.

2. Documents you produced to the Bureau in response to any investigative subpoena, data request, civil investigative demand, discovery request, or other demand.

3. Transcripts of and exhibits to any deposition or other sworn testimony that you took of the Bureau or its representatives in connection with *Consumer Financial Protection Bureau v. Navient Corp., et al.*, Case No. 3:17-cv-00101-RDM (M.D. Pa.).

4. Documents reflecting the status of all student loans obtained by Colorado borrowers or co-signers who complained about the student loan process or who are delinquent or in default on their student loans. This request includes all Colorado borrowers and co-signers identified in your response to Request No. 1 as well as the following information:

   a. Identification of the borrower;
   b. Whether there is a co-signer and, if so, the identification of the co-signer;
   c. Loan amount;
   d. Date loan was originated;
   e. Type of loan, including whether the loan is a private or a federal student loan;
   f. All repayment, deferment, forbearance, discharge, forgiveness, and cancellation plans applied for by the Colorado borrower or co-signer, the date of the application, whether the application was granted or

denied, the date the application was granted or denied, and if denied, the reason(s) for denial;

g. All repayment, deferment, forbearance, discharge, forgiveness, and cancellation plans entered into by the Colorado borrower or co-signer, including the type and terms of the plan and the date the borrower or co-signer entered the plan;
h. All rehabilitation plans applied for by the Colorado borrower or co-signer, the date of the application, whether the application was granted or denied, the date the application was granted or denied, and if denied, the reason(s) for denial;
i. All rehabilitation plans entered into by the Colorado borrower or co-signer, including the type and terms of the rehabilitation plan and the date the borrower or co-signer entered the rehabilitation plan;
j. Payment history, including attempts to pay past due amounts;
k. Collection history;
l. Amount of interest charged;
m. Amount of fees assessed;
n. Consolidation history, if applicable; and
o. Current loan status, i.e., current, delinquent, default, paid in full, forbearance, etc.

5. Documents reflecting all written and oral communications – including but not limited to, call recordings, notes, logs, electronic mail, text or instant messages, and other correspondence – between you and the Colorado borrowers and co-signers identified in documents responsive to Request Nos. 1 and 4. This request includes, but is not limited to, communications about the Colorado borrower's or co-signer's financial situation, including his or her delinquency history and attempts to repay past due amounts; all repayment, forbearance, forgiveness, deferment, cancellation, discharge, or consolidation plans offered or presented to the borrower or co-signer; and all collection efforts, including attempts to collect the "present amount due."

6. For those student loans that had a Colorado co-signer, produce documents reflecting any communication relating to an request for information about the co-signer release, including but not limited to, documents describing the process and requirements to release a co-signer; whether a co-signer release application was filed and, if so, the date of application; the status of the application; whether the application was granted or denied, the date the application was granted or denied, and, if denied, the reason(s) for denial; and inquiries about any aspect of the co-signer release.

7. Documents reflecting all formal or informal training manuals, materials, policies, procedures, processes, guidelines, rules, scripts, and other documents providing instruction or guidance for servicing, processing, and

collecting payments for student loans that you service. This request specifically includes, but is not limited to, documents related to:

a. advising, responding to, and providing or recommending options to Colorado borrowers or co-signers whose student loans are delinquent or in default;
b. advising, responding to, and providing or recommending options to Colorado borrowers or co-signers who indicate they are having or may have difficulty making their student loan payments;
c. handling Colorado borrower or co-signer complaints about any aspect of their student loans, including any complaint escalation processes;
d. co-signer releases, including requirements to release a co-signer such as requirements concerning that the borrower make a certain number of consecutive, on-time principal and interest payments;
e. eligibility, requirements, application, review, and determination processes relating to repayment, forbearance, forgiveness, deferment, cancellation, discharge, and consolidation plans or programs;
f. allocating student loan payments, including allocating payments as requested by the Colorado borrower or co-signer;
g. handling payments between one or more student loans;
h. servicing student loans of Colorado borrowers or co-signers; and
i. collecting on student loans of Colorado borrowers or co-signers that are delinquent or in default, including but not limited to policies, procedures, and guidance regarding requests that you no longer contact the borrower or co-signer by telephone, the frequency of attempts to contact the borrower or co-signer, and the practice of attempting to collect the "present amount due."

8. All marketing, advertising, promotional, and outreach materials, including templates of correspondence to any Colorado borrower or co-signer, regarding the servicing, repayment, and collecting of student loans.

9. Information provided or otherwise generally available to Colorado borrowers and co-signers that you drafted, provided, sent, or authorized relating to or describing repayment, forbearance, forgiveness, deferment, cancellation, discharge, consolidation, and any other options for Colorado borrowers or co-signers who are having trouble making their student loan payments, are not making their student loan payments, or are otherwise in financial distress. This request includes, but is not limited to, information and representations on websites, advertisements, direct mailers, email messages, text messages, flyers, and documents reflecting oral representations by your representatives to Colorado borrowers or cosigners. This request also includes information about qualifying and applying for repayment, forbearance, forgiveness, deferment, cancellation, discharge, consolidation, and any other program; the recertification process; and any other program requirements.

10. Internal or external studies or analyses relating to call times with borrowers or co-signers, including Colorado borrowers or co-signers, who are delinquent, who are in default, or who indicate they are having or may have difficulty making student loan payments.

11. Internal or external studies or analyses relating to the effectiveness (or lack of effectiveness) of communications to borrowers or co-signers, including Colorado borrowers or co-signers. By way of example, this request includes any studies or analyses about whether certain communications are more or less likely to (a) solicit a response from a borrower or co-signer who is delinquent or in default, (b) ensure that borrowers correctly and timely complete any recertification process, (c) successfully obtain a co-signer release, or (d) collect past due amounts or the "present amount due," a figure which includes the next month's payment.

12. Documents describing compensation policies and plans for your customer service representatives, call center representatives, and similar employees who interact with student loan borrowers and co-signers, including any incentive and bonus plans.

13. Documents describing compensation policies and plans for your employees who – either directly or indirectly – supervise, manage, or otherwise have responsibility for employees who interact with student loan borrowers and co-signers, as described above in Request No. 12, including any incentive and bonus plans.

14. State the number of Colorado borrowers or co-signers who were placed into one or more consecutive non-administrative forbearances within the 12 months prior to entering an IDR. As part of your response, provide information about the situation causing the borrower to be placed in the forbearance(s); the number of forbearance(s); the terms of each forbearance, including any fees; the amount of interest capitalized to the loan while in each forbearance; the date the borrower entered into the IDR; and the terms of the IDR, including the interest rate of the IDR and the monthly payment amounts.

15. Documents relating to every time you demanded or requested the "present amount due," which included the following month's payment, from a Colorado borrower or co-signer.

16. Documents relating to compensation you received for originating, servicing, and collecting student loans for Colorado borrowers and co-signers. This request includes, but is not limited to, how your compensation is calculated for originating, servicing, and collecting student loans.

17. Documents between you and the United States Department of Education relating to the servicing or collection of federal student loans, including any guidance, policies, or procedures.

18. Documents relating to the relationship between Navient Solutions, LLC and Navient Corporation.

19. Documents relating to the relationship between Navient Solutions, LLC or Navient Corporation and SLM Corporation or Sallie Mae, Inc.

20. Documents relating to the relationship between Navient and Pioneer Credit Recovery, Inc.

21. Documents relating to the relationship between Navient and General Revenue Corporation.

22. Documents that Navient provided to any educational institution in Colorado, including but not limited to, public, private, and for-profit colleges, universities, and trade schools. This request includes, but is not limited to, materials intended for distribution to students or potential students interested in obtaining or who had obtained student loans.

23. Documents reflecting communications between Navient and any educational institution in Colorado, including but not limited to, public, private, and for-profit colleges, universities, and trade schools relating to Navient's origination, servicing, and collecting of student loans.

DATED this 29th day of January, 2018.

FOR THE ATTORNEY GENERAL
CYNTHIA H. COFFMAN

s/ Jennifer Miner Dethmers

JENNIFER MINER DETHMERS
Senior Assistant Attorney General
jennifer.dethmers@coag.gov
720-508-6216

JENNIFER H. HUNT
First Assistant Attorney General
jennifer.hunt@coag.gov
720-508-6215

EXHIBIT B

1. TITLE: IDENTIFICATION AND AUTHENTICATION

2. PURPOSE:
This policy is created to document how the Information Technology Unit (ITU) meets the State of Colorado Information Security Policies which have been created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. § 24-37.5-101 et seq.). ITU maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. ITU documents the program details in the Agency Cyber Security Plan (ACSP).

3. POLICY
As part of its Information Security Program, ITU shall ensure each individual or system is assigned a unique identifier (user/system ID) and authenticator (password) for access to the Department of Law systems provided and/or managed by ITU.

4. ORGANIZATIONS AFFECTED
This policy applies to all classified and non-classified employees within the Department of Law's of Information Technology Unit, whether full or part-time and regardless of physical work location and status (e.g., permanent, probationary, trial service, etc.)

5. SCOPE
The scope of this policy covers the security of the Department of Law information technology systems provided and/or managed by the IT unit. It does not cover any other aspect of Department of Law business processes. There are requirements which are the responsibility of the Department of Law to implement; specific Department of Law responsibilities are defined in the Requirements section.

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS classification contained within the Data Classification Policy CYBER POL 118.

Further Guidance on the data and information system security categorization is located in the Data Classification Policy CYBER POL 118.

6. REFERENCES

6.1. C.R.S. § 24-37.5-401 et seq.
6.2. Senate Bill 08-155 as codified in C.R.S. § 24-37.5-101 et seq.
6.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
6.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
6.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
6.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

7. DEFINITIONS

For the purposes of this document, refer to C.R.S. § 24-37.5-102 et seq. and the CISP Information Security Glossary for any terms not specifically defined herein. The glossary is posted in the same location as the Colorado Information Security Policies - http://ITU.state.co.us/ois/policies.

7.1. **ITU:** Department of Law Information Technology Unit
7.2. **DOL:** Department of Law
7.3. **DOL User:** An DOL employee or an individual the Department of Law deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
7.4. **CISO:** Chief Information Security Officer.
7.5. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
7.6. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

7.7. **Security Category:** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Classification Policy.

8. REQUIREMENTS

8.1. Identification and Authentication [Department of Law Users] (LM)

8.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.1.2. The information system shall uniquely identify and authenticate DOL users and devices (or processes acting on behalf of DOL users).

8.1.3. ITU shall implement multifactor authentication for remote access to information system resources utilizing data classified with a security category of moderate or high.

8.1.4. ITU shall implement multifactor authentication where possible, for access to system administrative accounts for essential or critical systems or information systems that fall under federally mandated compliance laws or rules.

8.2. Device Identification and Authentication (LM)

8.2.1. This control is required for information systems with a Low or Moderate security categorization.

8.2.2. The information system shall uniquely identify and authenticate devices before establishing a remote network connection.

8.3. Identifier Management (LM)

8.3.1. This control is required for information systems with a Low or Moderate security categorization.

8.3.2. ITU shall obtain authorization from appropriate information system owners to assign or create an individual, group, role or device identifier or account.

8.3.3. ITU shall select an identifier that uniquely identifies an individual, group, role, or device.

8.3.4. ITU shall assign the identifier to the intended individual, group, role, or device.

8.3.5. ITU shall archive inactive or terminated user credentials.

8.3.6. ITU shall develop and document a process for validating system users who request reinstatement of user credentials for those suspended or revoked by the system.

8.3.7. ITU shall prevent reuse of identifiers.

8.3.8. ITU shall disable the identifier or account after employee transfer, termination, or other circumstances warranting disabling the account.

8.4. **Authenticator Management (LM)**

8.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.4.2. ITU shall verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

8.4.3. ITU shall establish initial authenticator content for authenticators defined by the organization.

8.4.4. Special Characters

- Where feasible, a minimum of five (5) changed characters when new passwords are created. Prohibit password reuse for six (6) generations.
- Minimum of 24 hours between password changes.
- ITU shall change/refresh authenticators every 90 days or as required by state and federal regulations, based on type of authenticator.
- ITU shall protect authenticator content from unauthorized disclosure and modification.
- ITU shall require individuals to follow, and have processes/systems implement, security safeguards to protect authenticators.
- ITU shall change authenticators for group/role accounts every 90 days or when membership to those accounts changes. ITU shall ensure that authenticators have sufficient strength of mechanism for their intended use and include the following.
- Minimum password complexity of at least nine (8) characters and must include three of the four following categories:
- Capital letters
- Lower case letters
- Numbers

8.4.5. ITU shall establish, document and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

8.4.6. ITU shall change default content of authenticators prior to information system installation.

8.4.7. ITU shall establish and document minimum and maximum lifetime restrictions and reuse conditions for authenticators.

8.4.8. ITU shall store and transmit only encrypted representations of passwords.

8.5. Authenticator Feedback (LM)

8.5.1. This control is required for information systems with a Low or Moderate security categorization.

8.5.2. The information system shall obscure feedback of authentication information during the authentication (logon) process to protect the information from possible exploitation/use by unauthorized individuals.

8.6. Re-authentication (M)

8.6.1. This control is required for information systems with a Moderate security categorization.

8.6.2. ITU shall require users and devices to re-authenticate in situations:

- when authenticators change;
- when roles change;
- when security categories of information systems change;
- when the execution of privileged functions occurs; and/or
- after 20 minutes of inactivity.

9. Roles and Responsibilities

9.1. State Chief Information Security Officer (CISO)

9.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to state agencies.

9.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9.2. Information System Owner

9.2.1. Identify appropriate system access, and approve access request forms.

9.3. Network Infrastructure Team

9.3.1. Assign unique identifiers to information system users, groups, roles or devices.

9.3.2. Follow information system requirements for authenticator management.

10. Compliance

All ITU employees identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in corrective and/or disciplinary action up to and including termination of employment.

11. Expiration

This policy remains in effect until the State CISO revises, changes, or terminates it.

PS - Personnel Security	Document ID:	CYBER POL 113
	Effective Date:	6/23/2015
	Revision Date:	
Version: 1.0	Document Type:	POLICY

1. TITLE: PERSONNEL SECURITY

2. PURPOSE:

This policy is created to document how the Information Technology Unit (ITU) meets the State of Colorado Information Security Policies which have been created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. § 24-37.5-101 et seq.). ITU maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. ITU documents the program details in the Agency Cyber Security Plan (ACSP).

3. POLICY

As part of its Information Security Program, ITU shall ensure information systems are effectively protected from physical threats including unauthorized access and environmental issues. The level of protection depends on the security category of the information residing on the information system.

4. ORGANIZATIONS AFFECTED

This policy applies to all classified and non-classified employees within the Department of Law's of Information Technology Unit, whether full or part-time and regardless of physical work location and status (e.g., permanent, probationary, trial service, etc.)

5. SCOPE

The scope of this policy covers the security of the Department of Law information technology systems provided and/or managed by the IT unit. It does not cover any other aspect of Department of Law business processes. There are requirements which are the responsibility of the Department of Law to implement; specific Department of Law responsibilities are defined in the Requirements section.

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII). Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS classification contained within the Data Classification Policy CYBER POL 118.

Further Guidance on the data and information system security categorization is located in the Data Classification Policy CYBER POL 118.

6. REFERENCES

6.1. C.R.S. § 24-37.5-401 et seq.
6.2. Senate Bill 08-155 as codified in C.R.S. § 24-37.5-101 et seq.
6.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
6.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
6.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
6.6. Enterprise Cyber Security Plan (ECSP) defined in CISP-017 SP-Security Planning Policy
6.7. ITU Background Screening Policy and Procedures (POL 100-18)

7. DEFINITIONS

For the purposes of this document, refer to C.R.S. § 24-37.5-102 et seq. and the CISP Information Security Glossary for any terms not specifically defined herein.

7.1. **CISO:** Chief Information Security Officer.
7.2. **ITU:** Department of Law Information Technology Unit
7.3. **DOL:** Department of Law
7.4. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
7.5. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
7.6. **Security Category:** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. For more detailed information see the Data Classification Policy 118.

8. REQUIREMENTS

8.1. Position Risk Designation (LM)

8.1.1. This control is required for information systems with a Low or Moderate security categorization.

8.1.2. ITU shall establish screening criteria for individuals filling ITU roles according to position risk.

8.1.3. ITU shall review and update position risk designations annually or as necessary for the position.

8.2. Personnel Screening (LM)

8.2.1. This control is required for information systems with a Low or Moderate security categorization.

8.2.2. ITU shall screen individuals prior to authorizing access to the information system.

8.2.3. ITU shall rescreen individuals every five (5) years or as necessary for the positions risk designation.

8.3. Personnel Termination (LM)

8.3.1. This control is required for information systems with a Low or Moderate security categorization.

8.3.2. Upon termination of individual employment:

- The DOL is required to notify ITU to modify or terminate DOL personnel access to agency information systems.
- ITU shall disable information system access immediately for personnel terminations.
- ITU shall terminate/revoke any authenticators/credentials associated with the individual.
- ITU shall conduct exit interviews for ITU personnel that includes a discussion surrendering resources and access information.
- ITU shall retrieve all security-related information system-related property from ITU personnel.
- ITU shall retain access to information and information systems formerly controlled by terminated ITU personnel.

8.4. Personnel Transfer (LM)

8.4.1. This control is required for information systems with a Low or Moderate security categorization.

8.4.2. ITU shall review and confirm ongoing operational need for current logical and physical access authorizations for ITU personnel to information systems/facilities when individuals are reassigned or transferred to other positions within the Colorado State Government.

8.5. Access Agreements (LM)
- 8.5.1. This control is required for information systems with a Low or Moderate security categorization.
- 8.5.2. ITU shall develop and document access agreements (acceptable use policies) for information systems.
- 8.5.3. ITU shall ensure ITU personnel requiring access to information and information systems sign appropriate access agreements prior to being granted access.
- 8.5.4. ITU shall review and update the ITU access agreements annually or as necessary for the position.

8.6. Third Party Personnel Security (LM)
- 8.6.1. This control is required for information systems with a Low or Moderate security categorization.
- 8.6.2. ITU shall establish personnel security requirements including security roles and responsibilities for third-party providers.
- 8.6.3. ITU shall require third-party providers to comply with personnel security policies and procedures established by ITU.

8.7. Personnel Sanctions (LM)
- 8.7.1. This control is required for information systems with a Low or Moderate security categorization.

9. Roles and Responsibilities

9.1. State Chief Information Security Officer (CISO)
- 9.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to state agencies.
- 9.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9.2. ITU and DOL Human Resources
- 9.2.1. Performs initial and periodic screening / background checks as needed.
- 9.2.2. Conducts exit interviews for departing employees.

9.3. ITU Supervisors
- 9.3.1. Notifies Infrastructure team of departing employees.
- 9.3.2. Conducts periodic position risk reviews.

10. Compliance

All ITU employees identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in corrective and/or disciplinary action up to and including termination of employment.

11. EXPIRATION

This policy remains in effect until the State CISO revises, changes, or terminates it.

PE - Physical and Environmental Protection	Document ID:	CYBER POL 112
	Effective Date:	
	Revision Date:	
Version: 1.1	Document Type:	POLICY

1. TITLE: PHYSICAL AND ENVIRONMENTAL PROTECTION

2. PURPOSE:
This policy is created to document how the Information Technology Unit (ITU) meets the State of Colorado Information Security Policies which have been created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. § 24-37.5-101 et seq.). ITU maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. ITU documents the program details in the Agency Cyber Security Plan (ACSP).

3. POLICY
As part of its Information Security Program, ITU shall ensure information systems are effectively protected from physical threats including unauthorized access and environmental issues. The level of protection depends on the security category of the information residing on the information system.

4. ORGANIZATIONS AFFECTED
The scope of this policy covers the security of the Department of Law information technology systems provided and/or managed by the IT unit. It does not cover any other aspect of Department of Law business processes. There are requirements which are the responsibility of the Department of Law to implement; specific Department of Law responsibilities are defined in the Requirements section.

5. SCOPE
The scope of this policy covers the security of the Department of Law information technology systems provided and/or managed by the IT unit. It does not cover any other aspect of Department of Law business processes. There are requirements which are the responsibility of the Department of Law to implement; specific Department of Law responsibilities are defined in the Requirements section.

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII). Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS classification contained within the Data Classification Policy CYBER POL 118.

Further Guidance on the data and information system security categorization is located in the Data Classification Policy CYBER POL 118.

6. REFERENCES

6.1. C.R.S. § 24-37.5-401 et seq.
6.2. Senate Bill 08-155 as codified in C.R.S. § 24-37.5-101 et seq.
6.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
6.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
6.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
6.6. Enterprise Cyber Security Plan (ECSP) defined in CISP-017 SP-Security Planning Policy

7. DEFINITIONS

For the purposes of this document, refer to C.R.S. § 24-37.5-102 et seq. and the CISP Information Security Glossary for any terms not specifically defined herein. The glossary is posted in the same location as the Colorado Information Security Policies - http://ITU.state.co.us/ois/policies.

7.1. **CISO:** Chief Information Security Officer.
7.2. **ITU:** Department of Law Information Technology Unit
7.3. **DOL:** Department of Law
7.4. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
7.5. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
7.6. **Security Category:** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations,

and the state. For more information see the Data Classification Policy CYBER POL 118.

8. Requirements

8.1. Physical Access Authorizations (LM)

8.1.1. This control is required for information systems with a Low or Moderate security categorization.

8.1.2. ITU shall develop, approve and maintain a list of individuals with authorized access to the facility where the information system resides.

8.1.3. ITU shall ensure that authorization credentials for facility access are properly issued.

8.1.4. ITU shall review the access list detailing authorized facility access by individuals annually.

8.1.5. ITU shall ensure that individuals are removed from the facility list when access is no longer required.

8.2. Physical Access Control (LM)

8.2.1. This control is required for information systems with a Low or Moderate security categorization.

8.2.2. ITU shall ensure the physical access authorizations at entry/exit points to the facility where the information system resides is enforced by validating the following:

- Verifying individual access authorizations before granting access to the facility; and
- Controlling ingress/egress to the facility using physical access control systems/devices or guards.

8.2.3. ITU shall maintain physical access audit logs for entry and exit points.

8.2.4. ITU shall provide security safeguards commensurate with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance as defined by the information system data security categorization to control access to areas within facilities officially designated as publicly accessible.

8.2.5. ITU shall escort visitors and monitor visitor activity in all secure areas.

8.2.6. ITU shall secure keys, combinations, and other physical access devices.

8.2.7. ITU shall inventory physical access devices annually.

8.2.8. ITU shall change combinations and keys annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

8.3. Access Control for Transmission Medium (M)

8.3.1. This control is required for information systems with a **Moderate** security categorization.

8.3.2. ITU shall control physical access to information system distribution and transmission lines within organizational facilities in accordance with state and federal requirements.

8.4. **Access Control for Output Devices (M)**

8.4.1. This control is required for information systems with a **Moderate** security categorization.

8.4.2. ITU shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

8.5. **Monitoring Physical Access (LM)**

8.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.5.2. ITU shall ensure that monitoring of physical access to the facility where the information system resides is in place to detect and respond to physical security incidents.

8.5.3. ITU shall ensure a review of physical access logs is conducted annually and upon occurrence of a physical security violation.

8.5.4. ITU shall coordinate results of reviews and investigations with the organizational incident response capability.

8.6. **Visitor Access Records (LM)**

8.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.6.2. ITU shall ensure that visitor access records are maintained to the facility where the information system resides to meet applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance as defined by the information system data security categorization.

8.6.3. ITU shall ensure a review of visitor access records is conducted quarterly.

8.7. **Power Equipment and Cabling (M)**

8.7.1. This control is required for information systems with a **Moderate** security categorization.

8.7.2. ITU shall ensure that proper protection of power equipment and power cabling for the information system from damage and destruction is provided.

8.8. **Emergency Shutoff (M)**

8.8.1. This control is required for information systems with a **Moderate** security categorization.

8.8.2. ITU shall ensure that the capability of shutting off power to the information system or individual system components in emergency situations is in place.

8.8.3. ITU shall ensure that emergency shutoff switches or devices to facilitate safe and easy access for personnel are provided.

8.8.4. ITU shall ensure that protection to emergency shutoff capability from unauthorized activation is in place and properly maintained.

8.9. Emergency Power (M)

8.9.1. This control is required for information systems with a **Moderate** security categorization.

8.9.2. ITU shall ensure that a short-term uninterruptible power supply is provided to facilitate an orderly shutdown of the information system, or transition of the information system to long-term alternate power in the event of a primary power source loss.

8.10. Emergency Lighting (LM)

8.10.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.10.2. ITU shall employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

8.11. Fire Protection (LM)

8.11.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.11.2. ITU shall employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

8.12. Temperature and Humidity Controls (LM)

8.12.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.12.2. ITU shall maintain appropriate temperature and humidity levels within the facility where the information system resides.

8.12.3. ITU shall monitor temperature and humidity levels.

8.13. Water Damage Protection (LM)

8.13.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

8.13.2. ITU shall protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

8.14. Delivery and Removal (LM)

8.14.1. This control is required for information systems with a Low or Moderate security categorization.

8.14.2. ITU shall authorize, monitor and control information system components entering and exiting the facility and maintain records of those items.

8.15. Alternate Work Site (M)

8.15.1. This control is required for information systems with a Moderate security categorization.

8.15.2. Remote access to information systems containing FTI or HIPAA data is prohibited on non-state controlled assets.

8.15.3. ITU shall employ appropriate security controls at alternate work sites.

8.15.4. ITU shall assess, as feasible, the effectiveness of security controls at alternate work sites.

8.15.5. ITU shall provide a means for employees to communicate with information security personnel in case of security incidents or problems.

9. Roles and Responsibilities

9.1. State Chief Information Security Officer (CISO)

9.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to state agencies.

9.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9.2. ITU Staff

9.2.1. Ensure due diligence is exercised when accessing secure areas and abide by specific agency rules and requirements above and beyond the scope of this policy.

10. Compliance

All ITU employees identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in corrective and/or disciplinary action up to and including termination of employment.

11. Expiration

This policy remains in effect until the State CISO revises, changes, or terminates it.

1. TITLE: SECURITY AWARENESS AND TRAINING

2. PURPOSE:
This policy is created to document how the Information Technology Unit (ITU) meets the State of Colorado Information Security Policies which have been created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. § 24-37.5-101 et seq.). ITU maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. ITU documents the program details in the Agency Cyber Security Plan (ACSP).

3. POLICY
As part of its Information Security Program for the Information technology Unit (ITU) shall ensure that the Department of Law personnel become aware of information security issues and their responsibilities to the data they protect by completing an annual Security Awareness Training. State personnel are required to read and be aware of policies, regulations, standards and guidance around protecting the State of Colorado information and information systems. Additional training is required for those users who utilize sensitive data such as Federal Tax Information (FTI), and Health Insurance Portability Accountability Act (HIPAA) data. Other training may be required based on the employee's roles and responsibilities.

4. ORGANIZATIONS AFFECTED
This policy applies to all classified and non-classified employees within the Department of Law's of Information Technology Unit, whether full or part-time and regardless of physical work location and status (e.g., permanent, probationary, trial service, etc.

5. SCOPE
The scope of this policy covers the security of the Department of Law information technology systems provided and/or managed by the IT unit. It does not cover any other aspect of Department of Law business processes. There are requirements which are the responsibility of the Department of Law to implement; specific Department of Law responsibilities are defined in the Requirements section.

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include

most data elements in state personnel records, building code violations, Personally Identifiable Information (PII). Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS classification contained within the Data Classification Policy CYBER POL 118.

Further Guidance on the data and information system security categorization is located in the Data Classification Policy CYBER POL 118.

6. REFERENCES

6.1. C.R.S. § 24-37.5-401 et seq.
6.2. Senate Bill 08-155 as codified in C.R.S. § 24-37.5-101 et seq.
6.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
6.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
6.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
6.6. Agency Cyber Security Plan (ACSP) defined in CISP-002 SP-Security Planning Policy

7. DEFINITIONS

For the purposes of this document, refer to C.R.S. § 24-37.5-102 et seq. and the CISP Information Security Glossary for any terms not specifically defined herein. The glossary is posted in the same location as the Colorado Information Security Policies - http://ITU.state.co.us/ois/policies.

7.1. **ITU:** Department of Law Information Technology Unit
7.2. **DOL:** Department of Law
7.3. **CISO:** Chief Information Security Officer
7.4. **Security Category:** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality,

integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. For more information see the Data Classification Policy 118.

8. REQUIREMENTS

8.1. Security Awareness Program (LM)

8.1.1. This control is required for information systems with a Low or Moderate security categorization.

8.1.2. ITU shall develop and document a security awareness and training program and disseminate the program to state agency personnel.

8.1.3. ITU shall review and update the security awareness and training program annually.

8.2. Security Awareness Training (LM)

8.2.1. This control is required for information systems with a Low or Moderate security categorization.

8.2.2. ITU shall provide basic security awareness training to information system users:

- As part of initial training for new users, and
- Annually thereafter.

8.3. Role Based Security Training (LM)

8.3.1. This control is required for information systems with a Low or Moderate security categorization

8.3.2. ITU shall provide role based security training to ITU personnel with assigned security roles and responsibilities:

- Before authorizing access to the information system or performing assigned duties,
- When required by information system changes, and
- Annually thereafter.

8.3.3. Role based security training shall include HIPAA and FTI specific training for ITU users whose job duties include working on HIPAA and/or FTI information systems.

8.4. Security Training Records (LM)

8.4.1. This control is required for information systems with a Low or Moderate security categorization

8.4.2. ITU shall document and monitor individual information system security training activities.

8.4.3. ITU shall retain individual training records for three (3) years or as required by applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
- ITU shall retain HIPAA training records for five (5) years.
- ITU shall retain FTI training records for seven (7) years.

9. Roles and Responsibilities

9.1. State Chief Information Security Officer (CISO)

9.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to state agencies.

9.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9.2. Human Resources

9.2.1. Document and retain individual training records?

9.3. Infrastructure Team

9.3.1. Develop and deliver annual security training to state agency personnel.

9.3.2. Develop and deliver role based security training curriculum for ITU personnel with assigned security roles and responsibilities.

10. Compliance

All ITU employees identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in corrective and/or disciplinary action up to and including termination of employment.

11. Expiration

This policy remains in effect until the State CISO revises, changes, or terminates it.

EXHIBIT C

COLORADO ATTORNEY GENERAL'S OFFICE POLICY

HUMAN RESOURCES

Policy Title	**Background Check**
Originator	Shelley Oxenreider, Human Resources Director
Reviewer	Melanie Snyder, Chief Deputy Attorney General
Approver	Cynthia H. Coffman, Attorney General
Original Effective Date	November 1, 2011
Effective Date This Revision	September 1, 2017

Purpose

The Colorado Department of Law is recognized as the lead law enforcement agency in the State of Colorado. As such, it is imperative that the department employs individuals of the highest ethical and moral standards and who have a background free of convictions for criminal offenses that could adversely affect the department or the performance of the employee's duties.

Policy

It is the policy of the Department of Law to conduct a thorough background check of all final candidates for employment. The background check shall include a criminal background check, reference and previous/current employer check, and (for attorney candidates) a check for professional sanctions in any state(s) where a license has been held.

The criminal background check shall include the department making an inquiry to the Colorado Bureau of Investigation (CBI) to ascertain whether the candidate has a criminal history. A hiring authority may extend a conditional offer of employment pending the results of this inquiry. Fingerprints will also be submitted for processing by both CBI and the Federal Bureau of Investigation (FBI). Employment shall be deemed conditional pending the results of the full criminal background check.

This policy applies to all permanent employees, temporary employees, contract employees, temporary agency employees, and interns. Vendors may be subject to the provisions of this policy as determined on a case-by-case basis by the Chief of Staff. The requirement to successfully pass a criminal background check as a condition of employment shall be placed on all vacancy announcements, as well as disclosed to candidates during the interview process.

As determined on a case-by-case basis, additional checks, such as a credit check or review of a candidate's motor vehicle record may also be conducted. Movement within the department to a different position may be cause for requiring additional background checks. The decision to conduct additional checks is made by the appointing authority with the concurrence of the Human Resources Director.

In determining whether a prospective employee is suitable for employment, primary consideration shall be given to the information found in the background check that relates specifically to the candidate's ability to successfully perform the duties of the position. Such determinations will be made on a case-by-case basis by the appointing authority, after full consideration of the circumstances.

When a candidate's background check contains any of the following listed offenses, additional review and full consideration of the circumstances by the Attorney General or Chief of Staff is required before an employment decision is made.

Offenses requiring secondary review include:

- A felony;
- A crime of violence as defined in CRS 16-1-104;
- Any offense where the underlying factual basis was one of domestic violence as defined in CRS 18-6-800.3(1);
- Any offense involving unlawful sexual behavior as defined under CRS 18-3-401;
- Any offense for child abuse as defined under CRS 18-6-401;
- Fraud, forgery, theft, false reporting, perjury or weapons offenses;
- Alcohol and/or drug offenses; and
- Ethics violations by attorneys that have resulted in professional sanctions and/or letters of admonition issued against attorneys.

Refusal to participate in the background check process will disqualify a person from employment with DOL. In addition, false, incomplete or inaccurate information, including failure to disclose a material fact during this process may be grounds for disqualification from employment.

In the event that information is revealed during the background check process that would disqualify a candidate from employment, the candidate will be notified in writing of the specific information and afforded an opportunity to provide evidence refuting the finding.

If a candidate believes the background information obtained via fingerprint search is inaccurate, the candidate may challenge such accuracy. It is the candidate's responsibility to correct such information as set forth in Title 42, U.S.C., Section

14616, Article IV(c); Title 28, C.F.R., Section 50.12(b); Title 5, U.S.C., Section 552a (e)(3). The procedure to correct this information is set forth in Title 28, C.F.R., Section 16.34. If the hiring authority is aware that the candidate is going to challenge the accuracy of the information, the hiring authority must afford the candidate a reasonable amount of time to correct the record, unless the candidate has declined to do so.

Evidence that a background check was conducted will be retained in an employee's personnel file. However, specific information obtained in conducting the background check will not be retained beyond its usefulness in approving an individual for employment.

Current employees are not subject to random background checks. However, when circumstances warrant, DOL reserves the right to conduct a background check on a current employee. In accordance with DOL's Criminal Misconduct of Employees Policy, all current employees are required to self-report the following to their supervisor on the next business day following the incident:

- All arrests, charges, or summons for any of the offenses set forth above;
- Any alcohol or drug related offenses;
- Any traffic offense(s) that results in the loss or suspension of a driver's license.

Employees are also required to self-report the disposition of any of the above offenses. Any employee who fails to self-report may be subject to corrective or disciplinary action up to and including termination. Further, conviction of any of the above offenses may result in disciplinary action up to and including termination.

The Human Resources Director serves as the department's background check coordinator, however, all hiring authorities are charged with following the published procedures for conducting background checks. The procedures to be followed in compliance with this policy are available on the Department of Law Intranet or by using the link below.

Attachment: DOL Background Check Procedures