THE CHANDRA LAW FIRM LLC

THE CHANDRA LAW BUILDING
1265 W. 6TH STREET, SUITE 400
CLEVELAND, OHIO 44113-1326
OFFICE 216.578.1700
FAX 216.578.1800

February 05, 2025

Via email

Thomas Wheeler
Acting General Counsel
U.S. Department of Education
Washington, DC 20202
Thomas.Wheeler@ed.gov

Candice Jackson
Deputy General Counsel
U.S. Department of Education
Washington, DC 20202
Candice.Jackson@ed.gov

Charles Ezell, Acting Director
Office of Personnel Management
The White House
Washington, DC 20500
hr@opm.gov

Re: Litigation-preservation demand

Dear Mr. Wheeler and Ms. Jackson:

We represent multiple U.S. Department of Education Office for Civil Rights–employee clients who have suffered retaliation made or directed by U.S. Department of Education, White House Office of Personnel Management, the Department of Government Efficiency (DOGE), other White House personnel, potentially in conspiracy with private citizens, in retaliation for our clients' participation in the Department of Education's diversity, equity, and inclusion programs and opposition to invidious discrimination—at the initial invitation of political appointees of Donald J. Trump. We are considering filing some form of legal action for equitable relief and damages to the federally protected interests of our clients.

Out of an abundance of caution to protect not only our clients' rights, but also against possible risks to the government if its employees were to inadvertently or intentionally spoliate evidence, **this is notice and request to immediately not delete, hide, or change in any way the relevant records, ensure that the government preserves the records, and ensure the records cannot be deleted, modified, or destroyed.**

Please confirm by email that you have complied with the requests in this preservation letter by **February 15, 2025.**

DEMAND FOR PRESERVATION OF ELECTRONICALLY STORED INFORMATION

We ask that you preserve all documents, tangible things (including handwritten notes), and electronically stored information ("ESI") potentially and broadly relevant to the actions

(including, but not limited to, placement on administrative leave) taken against our clients. As used in this document, "you" and "your" refers **all relevant personnel in your department, the White House, and across the federal government**, their respective agents, attorneys, accountants, employees, partners, or other persons occupying similar positions or performing similar functions, and all private citizens with whom they are working on concert. Much of the information subject to preservation is stored on your current and former computer systems, phones, online accounts, and other media and devices (including personal digital assistants, voice-messaging systems, online repositories, and cell phones).

ESI should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, or optically stored as:

- Digital communications (e.g., email, voice mail, instant messaging, social-media communications);
- Word-processed documents (e.g., Word, WordPerfect, or Google Docs documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting-application data (e.g., QuickBooks, Money, Peachtree data files);
- Image and facsimile files (e.g., .PDF, .TIFF, .JPG, .GIF, .PNG images, "memes");
- Sound recordings (e.g., .WAV and .MP3 files);
- Video and animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and relationship-management data (e.g., Outlook, ACT!);
- Calendar and diary application data (e.g., Google calendar, Outlook PST, Yahoo, blog tools);
- Online access data (e.g., temporary internet files, history, cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network access and server activity logs;
- Project-management application data;
- Computer-aided design/drawing files; and,
- Back-up, compressed, and archival files (e.g., .Zip, .GHO)

ESI resides not only in areas of electronic, magnetic, and optical-storage, and online media reasonably accessible to you, but also in areas you may deem *not* reasonably accessible. You are obliged to *preserve* potentially relevant evidence from *both* these sources of ESI.

This notice and request that you preserve both accessible and inaccessible ESI is reasonable and necessary. Under Federal Rules of Civil Procedure approved by the United States Supreme Court, you must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible.

For good cause shown, the court may then order ESI's production, even if it finds that it isn't reasonably accessible. Thus, even ESI you deem reasonably inaccessible *must be preserved in*

the interim so as not to deprive our clients of their right to secure the evidence or a court of its right to decide the issue.

Preservation requires immediate intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the *earlier* of a Created or Last Modified date on or after January 20, 2025 through the date of this demand and concerning:

1. The events and causes leading to the actions taken against my clients and all those similarly situated, including, but not limited to, placement on administrative leave;

2. Records, including ESI, you may use to support claims or defenses in any litigation related to my clients;

3. All communications or personal notes regarding my clients or similarly affected individuals—with anyone, including, but not limited to, communications to and from executive-branch officials, government actors, police, attorneys, and third parties.

4. Any communications or correspondence showing anyone targeting, seeking to target, or discussing targetting employees who have in any way participated in diversity, equity, inclusion, and accessibility programs, including serving on committees, attending seminars, or volunteering for requests to serve as change agents.

Adequate preservation of ESI requires more than just refraining from efforts to destroy or dispose of such evidence.

You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. *Be advised that sources of ESI are altered and erased by continued use of your computers, phones, other devices, and accounts.* Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. So alteration and erasure may result from failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish the concurrent obligation to preserve document, tangible things, and other potentially relevant evidence.

Suspension of routine, and automated destruction

Please immediately initiate a litigation hold for potentially relevant ESI, documents, and tangible things, and act diligently and in good faith to secure and audit compliance with that

litigation hold. Please identify and modify or suspend features of your information systems and devices that, in routine operation, cause the loss of potentially relevant ESI.

Examples of such features and operations include:

- Purging the contents of email repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure, or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back-up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online-storage repositories;
- Using metadata-stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file-defragmentation or compression programs.

Guard against all deletion—even "inadvertent" deletion

You should anticipate that your agents, employees, officers, or others may seek to hide, destroy, or alter ESI and act to prevent or guard against such actions. Especially where entity machines have been used for internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential, or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your agents. It's simply an event that occurs so regularly in electronic-discovery efforts that any ESI custodians and their counsel are obliged to anticipate and guard against its occurrence.

Preservation by imaging

Please take affirmative steps to prevent anyone with access to your data, systems, and archives from seeking to modify, destroy, or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data-shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). As for local hard drives, one way to protect existing data on local hard drives is by creating and authenticating a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is *not* a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space, and the swap file.

Demand is made that you immediately obtain, authenticate, and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by relevant personnel during the period from **January 20, 2025 to the present,** as well as recording and preserving the system time and date of each such computer.

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system, and medium from which it was obtained. Each such image should be preserved without alteration.

You should anticipate that certain ESI, including, but not limited to, spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should also refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location, and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but that may not be apparent to a user, including deleted content, draft language, commentary, collaboration, and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header-routing data and Base 64-encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Servers

Regarding servers like those used to manage email (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and email account should be preserved. There are several ways to preserve the contents of a server depending on, e.g., its RAID configuration and whether it can be downed or must be online 24/7.

If you question whether the preservation method you pursue is one that we will accept as sufficient, please call us to discuss it.

Home systems, laptops, online accounts, app accounts, social-media accounts, and other ESI venues

Though we expect that you will act swiftly to preserve data on workstations and servers, you should also determine whether any home or portable systems, or personal communication

channels, may contain potentially relevant data. If agents, officers, deputies, or employees have sent or received potentially relevant emails, instant messages using private apps, or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices, accounts, and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable flash drives, CD-R disks, and the user's personal-digital assistant (PDA), smartphone, voice mailbox, social-media and instant-messaging accounts, or other forms of ESI storage.). Similarly, if agents, employees, officers, or board members used online or browser-based email accounts or services (like AOL, Gmail, Yahoo Mail or the like) or instant-message accounts (like Telegram, Signal, SnapChat Messenger, Slack, etc.) to send or receive potentially relevant messages and attachments, you must preserve the contents of these account mailboxes (including Sent, Deleted, and Archived Message folders).

You must warn users not to use autodelete.

Ancillary preservation

You must preserve documents and other tangible items that may be required to access, interpret, or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID, and password rosters, or the like.

You must preserve any passwords, keys, or other authenticators required to access encrypted files and accounts, or run applications, along with the installation disks, user manuals, and license keys for applications required to access the ESI.

You must preserve any cabling, drivers, and hardware, other than a CD, flash drive, or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar-code readers, Zip drives, and other legacy or proprietary devices.

Paper preservation of ESI is inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, attorneys, and third parties

Your preservation obligation extends beyond ESI in your care, possession, or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian, or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System sequestration or forensically sound imaging

We suggest that removing your ESI systems, media, and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step.

If you deem it impractical to sequester systems, media, and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Again, merely "backing up" computers, phones, tablets, flash drives, CDs, or other devices by copying data to a USB drive, CD, or DVD is insufficient to adequately meet the requirements for preserving ESI because doing so can omit potentially relevant data and metadata like dates of access and modification, deleted files, configuration files, file-allocation tables, logs, and other artifacts.

To avoid these issues, again, you should image hard drives in bitstream copies, where all areas, used and unused, of a hard drive are copied. If a file is deleted before a backup is made, the deleted file will be copied only if it is a bitstream copy. All deleted files that are reasonably recoverable should be immediately undeleted. No procedures should be implemented to alter any active, deleted, or fragmented data. And no electronic data should be disposed of or destroyed.

We are prepared to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Otherwise, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them.

A successful and compliant ESI-preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics.

Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides.

Do not delay preservation

We're available to discuss reasonable preservation steps. But ***you must not defer preservation steps pending such discussions if ESI may be lost or corrupted because of delay.*** If your failure to preserve potentially relevant evidence results in the corruption, loss, or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Confirmation of compliance

Again, please **confirm by February 15**, that you have taken the steps outlined in this letter to preserve ESI and tangible documents. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence. We also trust that you will preserve such electronic data and paper files and that you will promptly notify us if any such records have been destroyed.

We thank you for your prompt attention to this matter.

Best regards,

Subodh Chandra