City of New York
THE SPECIAL COMMISSIONER OF INVESTIGATION
FOR THE NEW YORK CITY SCHOOL DISTRICT
80 Maiden Lane, 20th Floor
New York, New York 10038

Anastasia Coleman
Special Commissioner

Telephone: (212) 510-1400
Fax: (212) 510-1550
www.nycsci.org

VIA ELECTRONIC MAIL

September 21, 2021

Hon. Meisha Porter
Chancellor
New York City Public Schools
Department of Education
52 Chambers Street, Room 314
New York, NY 10007

Re: G-Suite Data Breaches
SCI Cases #: 2020-3399 and 2021-0839

Dear Chancellor Porter:

An investigation conducted by this office has substantiated that two separate but related New York City Department of Education ("DOE") data leaks were caused by a combination of factors, including the DOE's failure to properly safeguard information and inherent security flaws within the Google Suite ("G-Suite") software used by DOE employees.[1] As both incidents involved the same software, our findings are presented jointly in this letter.

I. Investigation & Findings:

A. 2020 Incident

a. Initial Complaint

The investigation began when the office of the Special Commissioner of Investigation for the New York City School District ("SCI") received a complaint from [redacted]. [redacted] alleged that an unidentified New York State Education Department ("NYSED") attorney informed her that an unidentified DOE student (who SCI later learned was a 15-year-old male student, "Student A") filed a complaint to NYSED in which he alleged that the DOE had a security breach and flaw in its G-Suite

[1] G-Suite is now known as Google Workspace. Per Google, "Similar to G Suite, all Google Workspace plans provide a custom email for your business and includes collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more." *See* https://workspace.google.com/.

configuration, one that allowed anyone with access to the DOE G-Suite application to view files that contained Personal Identifying Information ("PII") of DOE students. Student A alleged that within G-Suite, students such as he had access to any shared G-Suite file, and that, by entering "Source: domain" or "type: spreadsheet" into the search bar, he was able to find lists of failing students, attendance sheets, and other internal school documents.

b. DOE Personnel

SCI investigators conducted a phone interview with [redacted], who confirmed the DOE General Counsel's Office had received a complaint from NYSED's Chief Privacy Officer, and that DOE Division of Instructional and Information Technology ("DIIT") was trying to "track down" where the vulnerability lied within G-Suite. [redacted] also said that the person who accessed the documents engaged in a data breach as well as violations of state and federal regulations by accessing approximately 200 students' PII.

[redacted] confirmed that his team was investigating the issue, and pointed out that Student A was not able to access the actual files, but rather, only the file *names* were viewable. Over Zoom, SCI investigators met with members of DIIT's Cybersecurity Incident Response Team, including [redacted], and [redacted]. [redacted] who confirmed [redacted] had received a complaint about a potential leak of DOE PII, said DIIT's investigation revealed that Student A had looked into the DOE Google Drive and accessed certain files with DOE PII (including students' OSIS numbers and first and last names). [redacted] said that the DIIT team replicated what the student did and were able to find the files with the PII, and that the files that Student A accessed were then privatized. Further, per [redacted] DIIT was in the process of making all DOE files private.

In addition, DIIT prepared an investigative report dated September 28, 2020 (the "September 2020 letter") that was sent to NYSED's Chief Privacy Officer.[2] The September 2020 letter provided a summary of DIIT's investigation, technical findings, and mitigation efforts. Specifically, in Section IV – Corrective Action and Next Steps, DIIT outlined nine actions it would take to resolve the issue, specifically:

> "1. DIIT has changed the permissions to "Private" on the files accessed by the student account that contain PII.
> 2. DIIT is in the process of identifying files that have student information and re-setting permission on the files to "Private." Consequently, the full number of individuals whose information was breached is still being determined.
> 3. DIIT will evaluate and consider purchasing a Cloud Access Security Broker to provide enhanced DLP functionality of collaboration tools. This would assist with the identification and remediation of documents containing student information.
> 4. DIIT will implement new functionality to disallow sharing to the entire NYCDOE once available from Google.

[2] The report also indicated that Student A attended Bard High School Early College in Manhattan ("Bard").

5. DIIT will determine whether other similar, commonly-utilized tools share similar vulnerabilities, and will correct or mitigate such vulnerabilities where possible.
6. The NYCDOE will individually advise staff members who have utilized the NYCDOE-access function to cease using it.
7. The NYCDOE will inform employees system-wide of the issue and provide additional instructions in how to appropriately set access controls.
8. The NYCDOE has reported this incident to the Special Commissioner of Investigation for the New York City School District to investigate whether any misconduct or other wrongdoing has occurred.
9. The NYCDOE will notify the parents of the students whose information was viewed or downloaded by the student in question. However, pursuant to 8 N.Y.C.R.R. 121.10(e), notification of the parents of the students whose PII has been breached will be held in abeyance during the period of time that SCI's investigation is ongoing, and until all vulnerabilities in this report have been addressed."[3]

c. Student A

SCI investigators conducted a phone interview with Student A, along with his parents ("Father A" and "Mother A"). Father A said that his son was not "trying to do anything improper" when he discovered the flaw in the DOE's G-Suite, but that he was attempting to find a file that his teacher had sent to everyone in his Spanish class. When he could not find the file, he performed a Google search and discovered that when he entered "source:colon" into the search bar in G-Suite, he was able to see emails with parents' contact information and a "financial document." Student A said that these documents belonged to his school and he reported the issue to Bard's administration. When Bard sent students email accounts – accounts that ended in "nycstudents.gov" – to operate Zoom for remote learning, Student A used his Zoom email account to investigate whether he could still access the same G-Suite documents he was able to previously; he confirmed he was able to access numerous documents, again with parents' contact information. At this point, he filed an anonymous complaint.

B. 2021 Incident

a. Initial Complaint

As noted above, SCI was made aware of a second incident involving the DOE and its use of G-Suite software. On March 11, 2021, [redacted], emailed SCI regarding a security breach of its student data. [redacted] reported that she received an email from someone with an email address ending with "@nycstudents.net," and the email included a link to a Google Drive document that contained a list of students' names eligible for accommodations commonly known as "504s."[4] [redacted] and [redacted] access the document, and confirmed it was available in Google Drive and shared with schools.nyc.gov accounts. [redacted] and [redacted] disabled the document and removed it from Google

[3] Notably, [redacted] advised SCI that parental notifications were made by letters dated August 3, 2021.
[4] *See* https://www.schools.nyc.gov/school-life/health-and-wellness/504-accommodations.

Drive. [redacted] then received a second email containing information about a 10-year-old male student ("Student B"); with the subject "Security [Student B] DOB," from the Student B's parents ("Mother B" and "Father B"). The email sent to Mother B and Father B also came from the same email address, ending in "@nycstudents.net," and contained Student B's date of birth [redacted]. In the email, Student B's parents asked [redacted] "Why can this be seen? [redacted]

Subsequently, SCI investigators spoke with [redacted] via telephone. She confirmed that, after receiving the email, she spoke to [redacted] to ask about the visibility of 504 plans on Google Drive. Per [redacted] said that she shared a document encompassing the plans via email to relevant P.S. 187 staff, but did not realize that the document would also be shared with anyone with an "nycstudents.net" email address. [redacted] and [redacted] "restricted the document immediately" to ensure no one else had access to it any longer.

b. DOE Personnel

SCI investigators conducted a telephone interview with [redacted] to discuss the instant issue. [redacted] who said that he drafted the letter referenced in section I.A.b. above, said that the student who exposed the 504 vulnerability was able to see "hundreds of documents" including DOE documents from multiple schools. [redacted] said that the files had "incorrect" settings that allowed shared access by all DOE students and staff. Further, the student also changed approximately 16 students' Open Student Information System ("OSIS") passwords. Per [redacted] and his DIIT team did "write scripts" to hide the files exposed in the earlier 2020 incident. [redacted] later advised SCI that the data breach was worse than first anticipated; he sent an email that stated, "The staff member who has been reviewing files that the student accessed in some fashion to determine what personal information is in them, and whose information is involved, informed us that the student suspect appears to have downloaded documents for approximately 55 DOE employees that included either the last four digits of their social security numbers, or in a few cases contained their full social security number. The student also accessed a copy of a parents driver's license. We will also need to let NYPD know about this, as these categories of information are specifically covered in the Ad Code [Administrative Code] provision that requires NYPD notification."

Following the initial conversation with [redacted] SCI investigators conducted a Zoom meeting with [redacted].[5] The conversation focused on the letter sent after the last incident, and corrective measures the DOE had taken since that initial breach. [redacted] stated that neither she nor [redacted] followed up with [redacted] or SIRT to determine if the corrective measures outlined in the above-referenced letter were implemented. [redacted] stated that, "DIIT has changed the permissions to 'Private' on the files accessed by the student account that contained Personally Identifiable Information (PII)," but only on those (fewer than 10) files. [redacted] also said that, a week prior to the Zoom call, the

[5] Also present during the call was [redacted], who represented the DOE's legal interest and not any party on the call.

DOE purchased a software tool known as a Cloud Access Security Broker ("CASB"), and that he was confident CASB would be able to detect documents containing students' first and last names and OSIS IDs, as well as be able to privatize and lock documents available on G-Suite and Google. Per [redacted] DIIT was planning to expand the software to detect other information in documents to cover a broad range of them to be privatized and locked, including those with DOE staff members' Social Security numbers. Between the occurrence of the prior data breach in August 2020 and the instant one, [redacted] said that DIIT evaluated CASB providers, and that DIIT would work to "centralize" it to provide protection for DOE documents. However, [redacted] noted that some schools operated independently in the G-Suite application, and so DIIT would not be able to implement CASB on their G-Suite software, meaning they would need to migrate to DIIT or operate without DIIT protection on their documents. [redacted] said that DIIT migrated 652 schools onto the central network beginning in April 2020, and that it anticipated having more schools migrate on to the network in 2021. Though "schools have a choice" whether to operate under DIIT's protected G-Suite system or independently, "it is not a mandate." [redacted] stated that DIIT would recommend informing schools to migrate to DIIT's network to have CASB protection.

Regarding how someone was able to access a sensitive document in Google Drive, [redacted] explained that there was a feature in the settings that allowed the document to be "searchable" by anyone and someone may have selected in error or – simply put – that the error was not with the technology, but how it was used. [redacted] said, to mitigate "searchability" of documents, DIIT "ran a script" that hid 840,000 files that contained personal information. However, if a document is shared to groups (intentionally and/or in error), those groups will be able to view the document. [redacted] advised that DIIT was making all files "private" through CASB, and implementing automation so that if anyone were to click on the setting to "share" a document containing student information, the document would be privatized and the user would be sent a notification regarding "the best way" to share the document. After remote learning due to the Covid-19 pandemic, DOE staff and students were set to begin using the same tenant, and certain DOE personnel did not realize that when they shared documents, students were also able to view those documents through their DOE student accounts.[6] To bifurcate student accounts (*i.e.* those that end in @nycstudents.net) and DOE personnel accounts (*i.e.* those that end in @schools.nyc.gov), DIIT was scheduled to implement a feature called "target audiences" so that people in individual schools could only share documents within the school unless the person specified that the intention was to share the document outside of the school by entering an email address; the feature to share a document to all of DOE was no longer available. [redacted] stated that if anyone, including a DOE student, tried to access a DOE file/document in Google Drive without having the proper rights, DIIT would not be notified, but the user would receive a message stating that the person needs "to have permission to view this file."

When asked about the corrective measures referenced in the 2020 letter, specifically that "the NYC DOE will individually advise staff members who have utilized the DOE access function to cease

[6] "In multi-tenant software architecture—also called software multitenancy—a single instance of a software application (and its underlying database and hardware) serves multiple tenants (or user accounts). A tenant can be an individual user, but more frequently, it's a group of users—such as a customer organization—that shares common access to and privileges within the application instance. Each tenant's data is isolated from, and invisible to, the other tenants sharing the application instance, ensuring data security and privacy for all tenants." *See* https://www.ibm.com/cloud/learn/multi-tenant.

using it," [redacted] stated that a "DOE-wide e-mail was sent out" on April 13, 2021, regarding the correct way to share DOE documents and that some individual emails were sent informing DOE staff members after the breach the 2020 case – though he did not know the exact number. Subsequently, [redacted] provided SCI an email dated April 13, 2021, sent by [redacted] to all DOE personnel that detailed the correct procedure to share documents on the Google Drive.

[redacted] spoke again with SCI investigators via telephone to offer an update on the incident. He said that DIIT determined that the student who viewed the document was able to access the last four digits or the complete nine digits of the Social Security numbers of at least 55 DOE employees. [redacted] said that DOE Division of Operations Staff Member [redacted] was responsible for conducting an analysis of the documents viewed and/or accessed by the student. Regarding CASB, [redacted] indicated that the use of it should assist in preventing future data breaches of DATA files on the Google tenant. [redacted] spoke with SCI investigators, and confirmed that he analyzed the files that the student appeared to have accessed. Most of the documents he reviewed contained DOE staff members' Social Security numbers and one had a staff member's driver's license. [redacted] said that 260 "unique files," *i.e.* homework assignments, 504-plans, and others, were accessed. While [redacted] said that all files appeared to have been viewed by the subject and not downloaded, he agreed that someone could have viewed the documents and taken a photo of them with a camera phone or via screen shot for future use.

[redacted] sent an email to SCI investigators in which he stated that the exposure of Social Security numbers was being "addressed with CASB as well as other mitigating controls." He broke down the email into two parts: how the incident happened and what mitigating controls DIIT was taking to prevent future issues. Per [redacted]

"How the incident happened:

> The owner(s) of the files change [sic] the link to share link with the NYC Department of Education and also changed the link settings / permissions to "people in NYC Department of Education can search for this file". This makes the file searchable by anyone with a DOE account. The suspect search [sic] for files and found files containing PII.
>
> The link setting to make the file searchable cannot be removed from Google and it is not the default setting. The file owner must select both options in order for the files to be discoverable.

Mitigating Controls:

- All files that were made searchable by the file owners has [sic] been hidden.
- A script runs every minute to hide any files that has [sic] been searchable if a user decides to click on the option to make file searchable
- CASB has been implemented
- CASB identified all files containing SSNs and Student information (Student First Name, Last Name & SSN)
- CASB change files permission to private on all files that are shared to everyone in the NYC DOE."

Essentially, [redacted] in his first point, repeated that the issue was human/user error, in that the owner of the file incorrectly changed sharing permissions. With regard to mitigation, [redacted] indicated that CASB was able to privatize files that included SSNs.

II. Conclusion and Recommendations:

There is no doubt that two separate yet related data breaches occurred, both of which resulted in private information being accessed by someone who did not have proper authority. While the first incident appears to have been caused by a student who was trying to demonstrate security flaws, the second incident appears more malicious in nature. SCI was able to substantiate that the DOE failed to take appropriate safety precautions, especially after the first incident made everyone aware that such breaches could occur. After the 2020 incident, DIIT confirmed it set to private the files accessed by Student A, and sent a DOE-wide email about proper security protocols for G-Suite files. Yet months later, another student was able to access 55 Social Security numbers. [redacted] indicated to SCI that the CASB system would automatically privatize documents that contained PII such as Social Security numbers, yet Syed said that the CASB would only be implemented for the schools who opt-in for DIIT protection. Both incidents also appear to be the result of human error, yet outside of CASB and one DOE-wide email, no steps seem to have been taken to prevent such human error moving forward. Therefore, SCI offers the following Policy and Procedure Recommendations ("PPRs") to obviate future data breaches:

1) Require that all schools that receive DOE funding or staff DOE pedagogues, and have documents that contain PII, utilize DIIT servers and protection. It is inexplicable how individual schools could run into the same issues as noted above and not be required to take the simple, corrective action of having the CASB protection about which Waters spoke so highly.
    a. Within one month, a list of all schools that are *not* currently operating with DIIT protection should be created, to determine next steps in migration.
    b. By the end of the 2021-2022 school year, all DOE schools should be migrated to the DIIT system.
2) The DOE should also require that any document that contains PII – particularly someone's driver's license, Social Security number, 504 form, or the like – be set in default mode to "private," *i.e.* non-shareable. If someone were to change the setting, a member of DIIT should be immediately notified.
3) Within the next six months, an audit should be conducted by DIIT to determine how many documents CASB has privatized. In addition, a random audit should be conducted of documents that are not marked private, to determine if the CASB system has sufficiently worked as intended.
4) Emails or other reminders regarding the importance of safeguarding PII should be sent no fewer than once every three months to all DOE staff.

5) DIIT should provide all DOE employees with security awareness training on an annual basis, with an emphasis on privacy issues, phishing and other scams, the difference between public and private systems, and best practices.
    a. Notably, SCI recognizes that different trainings should be customized to the audience, *i.e.* a training for classroom-based pedagogues may differ from managers, executives, and the staffs of units within DOE such as ORS and OSYD.
6) The DOE should establish a delineated Code of Conduct regarding DOE protected information, including private and identifying information of students and DOE employees.
7) The DOE should prohibit the usage of free products and services, which would run on the DOE's network, to be used in storing PII, until such product or service is vetted by DIIT and/or computer and technology teachers trained in such matters by the DOE.

Please respond in writing within 30 days of receipt of this letter as to any action taken or contemplated regarding the above-listed PPRs. We are sending a copy of this letter to the DOE Office of Legal Services, for whatever action they deem necessary.

Should you have any inquiries regarding the above, please contact Jonathan Jacobs, the assigned attorney for this matter, at (212) 510-1423 or jjacobs@nycsci.org.

Sincerely,

ANASTASIA COLEMAN
Special Commissioner of Investigation
for the New York City School District

By: */s/ Daniel I. Schlachet*
Daniel I. Schlachet
First Deputy Commissioner

AC:DS:JJ:lr
cc: Judy Nathan, Esq.
Karen Antoine, Esq.
Katherine Rodi, Esq.