United States Senate
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
WASHINGTON, DC 20510–6125
WEBSITE: https://commerce.senate.gov

December 5, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528

Dear Ms. Easterly:

I am writing regarding the role of the Cybersecurity and Infrastructure Security Agency (CISA) in funding and supporting programs to censor Americans' constitutionally protected speech.

As you may know, in February I launched an investigation into Big Tech's content moderation and censorship practices.[1] Documents obtained in my investigation, as well as information made public via the Twitter Files and legal discovery, have exposed the extent to which speech suppression on social media was materially driven by government agencies. In addition to directly flagging content to social media companies, government agencies funneled money to private sector third parties, including nonprofits and academic institutions, that then pressured social media companies to remove content and accounts.[2] By laundering taxpayer dollars through third parties, government agencies tried to absolve themselves of liability for infringement of Americans' First Amendment rights.

In some cases, this scheme was blatant. For example, the University of Washington and Stanford University received federal funds to create the so-called "Election Integrity Partnership" (EIP).[3] The stated purpose of the project was to focus on "attempts to suppress voting, reduce participation, confuse voters, or delegitimize election results without evidence."[4] The Twitter

[1] Press Release, Committee on Commerce, Science, and Transportation, Sen. Cruz Launches Sweeping Big Tech Oversight Investigation (Feb. 13, 2023), https://www.commerce.senate.gov/index.php/2023/2/sen-cruz-launches-sweeping-big-tech-oversight-investigation.
[2] *See Weaponization of the Federal Government on the Twitter Files: Hearing Before the Select Subcomm. on Weaponization of the Fed. Gov't of the H. Comm on the Judiciary* (Mar. 9, 2023) (statement of Michael Shellenberger), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/shellenberger-testimony.pdf.
[3] Press Release, University of Washington, $2.25 million in National Science Foundation Funding Will Support Center for an Informed Public's Rapid-response Research of Mis- and Disinformation (Aug. 15, 2021), https://www.cip.uw.edu/2021/08/15/national-science-foundation-uw-cip-misinformation-rapid-response-research/.
[4] ELECTION INTEGRITY PARTNERSHIP, https://www.eipartnership.net/ (last visited Oct. 23, 2023).

Files later revealed that the EIP had successfully coerced social media companies to review millions of tweets with the help of CISA.[5] In a 2021 interview, the EIP's lead researcher did not attempt to hide the fact that taxpayer money had flowed through a third party to evade First Amendment liability. He described the project's purpose as "to fill the gap of things that the government could not do themselves" because the government "lacked both . . . the funding and the *legal authorizations*."[6]

Additionally, CISA disbursed over $87 million to build the Center for Internet Security (CIS), which was created to "collaborate with State and local governments on cybersecurity risks and incidents" but was actually used to monitor lawful speech.[7] The CIS runs the Election Infrastructure Information Sharing and Analysis Center , which in past elections used a ticketing system operated by Stanford University-employed CISA interns and other members of CISA's mis-, dis-, and mal-information (MDM) team to report posts to social media companies and pressure them into removing content that academics and CISA deemed dangerous.[8] In fact, the EIP boasted about using the center to "effectively counter viral falsehoods"[9] posted by Americans online.

Just because the government hires a hitman to kill speech does not absolve the government of guilt. Regrettably, the Election Integrity Partnership and the CIS appear to be just two of numerous instances of third parties receiving government support to suppress speech. It has also become apparent that our nation's higher education institutions were often used as conduits through which the government could police speech online.

The Standing Rules of the Senate provide the Committee on Commerce, Science, and Transportation jurisdiction over technology and interstate commerce including to "review and study" those topics "on a continuing basis."[10] So that I may better understand the scope and nature of your agency's activities in this area, please provide the documents requested below and written responses to the questions below no later than December 19, 2023, in accordance with the attached instructions.

---

[5] Mike Benz, *DHS Censorship Agency Had Strange First Mission: Banning Speech That Casts Doubt on 'Red Mirage, Blue Shift' Election Events*, FOUNDATION FOR FREEDOM ONLINE (Nov. 9, 2022), https://foundationforfreedomonline.com/dhs-censorship-agency-had-strange-first-mission-banning-speech-that-casts-doubt-on-red-mirage-blue-shift-election-events/.

[6] 360/Open Summit, *Lighting talk | Election Integrity Partnership*, Atlantic Council, https://www.atlanticcouncil.tv/videos/360-open-summit-the-world-in-motion-012-lightning-talk-election-integrity-partnership (last visited Dec. 4, 2023) (emphasis added).

[7] *See* Cooperative Agreement, DHS and Center for Internet Security, Inc., USASPENDING.GOV (last visited Dec. 4, 2023), https://www.usaspending.gov/award/ASST_NON_19PDMSI00002_7061.

[8] *See* Matt Taibbi, *Twitter File #19*, TWITTER (Mar. 17, 2023, 10:00 AM), https://twitter.com/mtaibbi/status/1636729166631432195.

[9] Election Integrity Partnership, *The Long Fuse: Misinformation and the 2020 Election* (Jun. 15, 2021), https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf.

[10] S. Rules XXV(1)(f), XXVI(8)(a)(2).

1. How does CISA uphold the First Amendment in its grant making and non-governmental partnerships processes to ensure that all projects and partnerships align with constitutional principles?

2. Provide a list of all institutions of higher education (IHEs) that received funding (including grants, loans, or other financing) or other forms of support (including partnerships) through your agency from January 1, 2018, to present, for any project or partnership containing one or more of the keywords listed below. In your response, include the name of the IHE, the amount of funding allocated (if applicable), a detailed description of the project or partnership's stated purpose, and the duration of the project or partnership.

    a. censorship
    b. digital dashboard
    c. digital literacy
    d. disinformation
    e. emotional impacts of social media
    f. engagement on social media
    g. fact-checking
    h. fake news
    i. information manipulation
    j. mal-information
    k. misinformation
    l. narratives
    m. online abuse
    n. online journalists
    o. online harassment
    p. rumors
    q. social media
    r. social media content
    s. social media providers
    t. truthfulness of content
    u. trending networks
    v. user-centric
    w. user-centric intervention

3. Produce all documents referring or relating to the funding arrangements or other forms of support (including partnerships) described in your response to item 2.

4. Provide a list of all CISA-affiliated individuals—including employees, interns, and contractors—who built or used the CIS Elections Infrastructure Information Sharing and

Analysis Center or the project's extension, the Multi-State Information Sharing and Analysis Center, both housed at CIS.[11]

5. Does CISA actively incorporate First Amendment considerations into its decision-making process when awarding funding to or partnering with organizations involved in the research, identification, or monitoring of MDM?

    a. If so, produce all documents and communications referring or relating to the CISA's First Amendment considerations for each project or partnership mentioned in response to item 2.

6. When evaluating whether the grants or other forms of support (including partnerships) mentioned in response to item 2 should be awarded, did CISA consult, including informally, with employees of any other U.S. government agencies? If so, provide the names of those agencies for each relevant project or partnership.

7. Produce all communications between employees and contractors of CISA and any of the individuals or entities listed below, as well as any documents or communications referring or relating to any individual or entity listed below, for the period of January 1, 2018, to present.

    a. Alex Stamos (Stanford University)
    b. American University
    c. Brown University
    d. Brown University Information Futures Lab
    e. Carnegie Mellon University
    f. Claire Wardle (Brown University)
    g. Clemson University
    h. Clemson University Media Forensics Lab
    i. Darren Linvill (Clemson University)
    j. Georgetown University
    k. Hany Farid (University of California, Berkeley)
    l. Harvard University
    m. Harvard University Shorenstein Center on Media, Politics and Public Policy
    n. Harvard University Berkman Klein Center for Internet and Society
    o. Joan Donovan (Harvard University)
    p. Kate Starbird (University of Washington)
    q. Michigan State University
    r. New York University
    s. New York University Center for Social Media & Politics

[11] CENTER FOR INTERNET SECURITY, *About Us*, https://www.cisecurity.org/about-us (last visited Dec. 4, 2023).

t. New York University Tandon School of Engineering
u. Patrick Warren (Clemson University)
v. Princeton University
w. Renee DiResta (Stanford University)
x. Stanford University
y. Stanford Cyber Policy Center
z. Stanford Internet Observatory
aa. The Election Integrity Partnership
bb. The Virality Project
cc. University of California, Berkeley
dd. University of Michigan
ee. University of Washington
ff. University of Washington Center for an Informed Public
gg. Any additional IHEs listed in your response to item 2

8. Yes or no: Is CISA aware that recipients of CISA grants and partnerships, using those funds, advised social media companies to remove protected speech flagged by CISA?

9. Considering the Fifth Circuit's recent decision in *Missouri v. Biden*,[12] has CISA planned or implemented new guardrails to protect Americans' First Amendment rights?

Thank you for your attention to this matter.

Sincerely,

Ted Cruz
Ranking Member

[12] No. 23-30445 (Sept. 8, 2023) (per curiam).

Instructions for Responding to a Committee Request

Committee on Commerce, Science, & Transportation
United States Senate
118th Congress

A. Responding to a Request for Documents

1. In complying with the Committee's request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. This request extends to any personal devices utilized for official business. Requested records, documents, data, or information should not be destroyed, modified, removed, transferred, or otherwise made inaccessible to the Committee.

2. To ensure the integrity of the Committee's investigation, preserve all documents, communications, and other data whether physical documents or electronically stored information ("ESI") that can reasonably be anticipated to be subject to a request for production by the Committee in this investigation, regardless of production pursuant to paragraph (1). "Documents, communications, and other data" should be construed broadly. For the purposes of this request, "preserve" means taking reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, shredding, incineration, wiping, relocation, migration, theft, or mutation of ESI, as well as negligent or intentional handling that would make such records, communications, or data incomplete or inaccessible. Further, we request that you:

    a. Exercise reasonable efforts to identify and notify former employees and contractors, subcontractors, and consultants who may have access to such documents, communications, and other data that it is to be preserved;

    b. Exercise reasonable efforts to identify, recover, and preserve any documents, communications, and other data which has been deleted, partially destroyed, or marked for deletion or destruction but is still recoverable; and

    c. If it is the routine practice of any employee or contractor to destroy or otherwise alter such documents, communications, and other data, either halt such practices or arrange for the preservation of complete and accurate duplicates or copies of such documents, communications, and other data, suitable for production, if requested.

3. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should be read also to include the alternative identification.

4. Documents should be produced in electronic form, *i.e.*, email, cloud-based production (such as the Committee's Large File Transfer Service or other Senate-approved mechanism) memory stick, or thumb drive, in lieu of paper productions.

5. Documents produced in electronic form should be organized, identified, and indexed electronically.

6. Electronic document productions should be prepared according to the following standards:

    a. The production should consist of single page Tagged Image Files (".tif"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.

    b. Document numbers in the load file should match document Bates numbers and .tif file names.

    c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

    d. All electronic documents produced should include the following fields of metadata specific to each document: BEGDOC, ENDDOC, TEXT PATH, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION.

    e. Alternatively, if the production cannot be made in .tif format, all documents derived from word processing programs, email applications, instant message logs, spreadsheets, and wherever else practicable should be produced as in their native format. In such circumstances, consult with Committee staff prior to production of the requested documents.

    f. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), consult with the Committee staff to determine the appropriate format in which to produce the information.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one tranche of files is produced, each tranche should contain an index describing its contents.

8. Documents produced in response to the request should be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.

9. When producing documents, identify the paragraph in the Committee's schedule to which the documents respond.

Instructions for Responding to a Committee Request

10. Do not refuse to produce documents on the basis that any other person or entity also possesses non-identical or identical copies of the same documents or on the basis that although the documents are in your custody or control they did not originate with you or are not owned by you.

11. This request is continuing in nature and applies to any newly discovered information. Any record, document, compilation of data or information not produced because it has not been located or discovered by the return date, should be produced immediately upon subsequent location or discovery.

12. All documents should be Bates-stamped sequentially and produced sequentially. Each page should bear a unique Bates number.

13. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as soon as possible if full compliance cannot be made by the date specified in the request, and provide an explanation for why full compliance is not possible by that date.

14. In the event that any document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, and addressee; and (e) the relationship of the author and addressee to each other.

15. In the event that a portion of a document is redacted on the basis of privilege, provide a privilege log containing the following information concerning any such redaction: (a) the privilege asserted; (b) the location of the redaction in the document; (c) the general subject matter of the redacted material; (d) the date, author, and addressee of the document, if not readily apparent; and (e) the relationship of the author and addressee to each other.

16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.

17. If a date, name, title, or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date, name, title, or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents which would be responsive as if the date, name, title, or other descriptive detail was correct.

18. In the event a complete response requires the production of classified information, provide all as much information in unclassified form as possible in your response and send all classified information under separate cover via the Office of Senate Security.

19. Unless otherwise specified, the period covered by this request is from January 1, 2013 to the present.

20. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

B. Responding to Interrogatories or a Request for Information

1. In complying with the Committee's request, answer truthfully and completely. Persons that knowingly provide false testimony could be subject to criminal prosecution for perjury (when under oath) or for making false statements. Persons that knowingly withhold subpoenaed information could be subject to proceedings for contempt of Congress. If you are unable to answer an interrogatory or information request fully, provide as much information as possible and explain why your answer is incomplete.

2. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should also be read to include the alternative identification.

3. Your response to the Committee's interrogatories or information requests should be made in writing and should be signed by you, your counsel, or a duly authorized designee.

4. When responding to interrogatories or information requests, respond to each paragraph in the Committee's schedule separately. Clearly identify the paragraph in the Committee's schedule to which the information responds.

5. Where knowledge, information, or facts are requested, the request encompasses knowledge, information or facts in your possession, custody, or control, or in the possession, custody, or control of your staff, agents, employees, representatives, and any other person who has possession, custody, or control of your proprietary knowledge, information, or facts.

6. Do not refuse to provide knowledge, information, or facts on the basis that any other person or entity also possesses the same knowledge, information, or facts or on the basis that although the documents are in your custody or control they did not originate with you or are not owned by you.

7. The request is continuing in nature and applies to any newly discovered knowledge, information, or facts. Any knowledge, information, or facts not provided because it was not known by the return date, should be provided immediately upon subsequent discovery.

8. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as soon as possible if full compliance cannot be made by the date

specified in the request, and provide an explanation for why full compliance is not possible by that date.

9. In the event that knowledge, information, or facts are withheld on the basis of privilege, provide a privilege log containing the following information: (a) the privilege asserted; (b) the general subject matter of the knowledge, information, or facts withheld; (c) the source of the knowledge, information, or facts withheld; (d) the paragraph in the Committee's request to which the knowledge, information, or facts are responsive; and (e) each individual to whom the knowledge, information, or facts have been disclosed.

10. If a date, name, title, or other descriptive detail set forth in this request is inaccurate, but the actual date, name, title, or other descriptive detail is known to you or is otherwise apparent from the context of the request, provide the information that would be responsive as if the date, name, title, or other descriptive detail was correct.

11. In the event a complete response requires the transmission of classified information, provide as much information in unclassified form as possible in your response directly to the Committee offices and send only the classified information under separate cover via the Office of Senate Security.

12. Unless otherwise specified, the period covered by this request is from January 1, 2013 to the present.

C. Definitions

1. The term "document" in the request or the instructions means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra- office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

Instructions for Responding to a Committee Request

2. The term "communication" in the request or the instructions means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether face to face, in meetings, by telephone, mail, telex, facsimile, email (desktop or mobile device), computer, text message, instant message, iMessage, MMS, RCS, or SMS message, WhatsApp, Signal, any other encrypted message, regular mail, discussions, releases, delivery, or otherwise. This includes communications on encrypted phones and personal devices and personal accounts utilized for official business.

3. The terms "and" and "or" in the request or the instructions should be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" in the request or the instructions mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, businesses or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify" in the request or the instructions, when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address, email address, and phone number.

6. The terms "referring" or "relating" in the request or the instructions, when used separately or collectively, with respect to any given subject, mean anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.

7. The term "employee" in the request or the instructions means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint venturer, loaned employee, part-time employee, permanent employee, provisional employee, or subcontractor.

8. The terms "you" and "your" in the request or the instructions refer to yourself; your firm, corporation, partnership, association, department, or other legal or government entity, including all subsidiaries, divisions, branches, or other units thereof; and all members, officers, employees, agents, contractors, and all other individuals acting or purporting to act on your behalf, including all present and former members, officers, employees, agents, contractors, and all other individuals exercising or purporting to exercise discretion, make policy, and/or decisions.

# # #