IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DANIEL J. BERNSTEIN,)
)
Plaintiff,)
)
v.)
)
NATIONAL INSTITUTE OF STANDARDS)
AND TECHNOLOGY,)
100 Bureau Drive)
Gaithersburg, MD 20899)
)
U.S. DEPARTMENT OF COMMERCE,)
1401 Constitution Ave NW)
Washington, D.C. 20230)
)
Defendants.)

COMPLAINT

1. Plaintiff, DANIEL J. BERNSTEIN, brings this Freedom of Information Act suit to force Defendants NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) and U.S. DEPARTMENT OF COMMERCE to comply with Plaintiff's FOIA request for records pertaining to the NIST Post-Quantum Cryptography Standardization Project. In violation of the Freedom of Information Act, Defendants have failed to issue a determination, have failed to produce records promptly, and have failed to provide an estimated date of completion for the request.

PARTIES

2. Plaintiff DANIEL J. BERNSTEIN is a mathematician, cryptologist, and computer scientist. He is a professor of Computer Science at the University of Illinois at Chicago. He also

has a professorship at Ruhr University Bochum in Germany. BERNSTEIN made the FOIA request at issue in this case.

3. Defendant NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) is a federal agency subject to the Freedom of Information Act, 5 U.S.C. § 552.

4. Defendant U.S. DEPARTMENT OF COMMERCE (DOC) is a parent agency of NIST and a federal agency subject to the Freedom of Information Act, 5 U.S.C. § 552.

JURISDICTION AND VENUE

5. This case is brought under 5 U.S.C. § 552(a)(4)(B) and presents a federal question conferring jurisdiction on this Court. *See* 28 U.S.C. § 1331.

6. Venue is proper under 5 U.S.C. § 552(a)(4)(B).

BACKGROUND

7. Cryptography is used by billions of people around the world to protect communication against espionage and sabotage. For example, a cryptographic mechanism called "Curve25519" introduced by BERNSTEIN is now used automatically by Apple iPhones, Facebook's WhatsApp, and Google Chrome.

8. NIST and its predecessor, the National Bureau of Standards, have issued a variety of standards for cryptography, starting in the 1970s.

9. U.S. government purchasing often requires compliance with NIST's cryptographic standards.

10. Further NIST activities have resulted in much broader domestic and international usage of some of NIST's cryptographic standards. *See, e.g.,* "The Economic Impacts of NIST's Data Encryption Standard (DES) Program", 2001, https://csrc.nist.gov/publications/detail/white-paper/2001/10/01/the-economic-impacts-of-nist-des-program/final, at 21.

11. In 2016, NIST announced a Post-Quantum Cryptography Standardization Project.

12. Quantum computers are under active development and threaten the security of many existing cryptographic mechanisms, including Curve25519 and various NIST standards. The objective of post-quantum cryptography is to protect against this threat.

13. On or around December 15, 2016, NIST issued a call for submissions to the NIST Post-Quantum Cryptography Standardization Project, setting a submission deadline of November 30, 2017. 81 Fed. Reg. 92787 (December 20, 2016).

14. On January 31, 2019, NIST issued a report regarding the first round of the project. *See* https://csrc.nist.gov/publications/detail/nistir/8240/final.

15. On July 22, 2020, NIST issued a report regarding the second round of the project. *See* https://csrc.nist.gov/publications/detail/nistir/8309/final.

16. On July 5, 2022, NIST issued a report regarding the third round of the project. *See* https://csrc.nist.gov/publications/detail/nistir/8413/final.

17. The NIST Post-Quantum Cryptography Standardization Project is ongoing.

18. Upon information and belief, the U.S. National Security Agency (NSA) was already involved with the NIST Post-Quantum Cryptography Standardization Project before the 2016 project announcement.

19. In July 2020, NIST and NSA revealed that NSA had already been involved with the NIST Post-Quantum Cryptography Standardization Project.

20. The details of NSA's influence upon the NIST Post-Quantum Cryptography Standardization Project, before and after July 2020, are still not public.

THE FOIA REQUEST "NSA, NIST, AND POST-QUANTUM CRYPTOGRAPHY"

21. On March 16, 2022, BERNSTEIN submitted a FOIA request, "NSA, NIST, and post-quantum cryptography," to NIST. This FOIA request asked for the records of the NIST Post-Quantum Cryptography Standardization Project, including the following records:

> [1] Records of the project phase leading up to the call for submissions, meaning the period before the issuance of 81 FR 92787 (December 20, 2016);
> [2] Records of the submission phase, meaning the period starting from the issuance of 81 FR 92787 and continuing through the submission deadline (November 30, 2017);
> [3] Records of the first round, meaning the period starting from the submission deadline and continuing through the issuance of NIST IR 8240 (January 31, 2019);
> [4] Records of the second round, meaning the period starting from the issuance of NIST IR 8240 and continuing through the issuance of NIST IR 8309 (July 22, 2020);
> [5] More recent records, up to the day that this request is processed.

Ex. 1.

22. This FOIA request also asked for [6] all records of NIST/NSA meetings mentioning the word "quantum", whether or not NIST views those meetings as part of the project; and for [7] all records of NSA's writeup of post-quantum cryptography mentioned at the August 27, 2013, NIST/NSA meeting. *Id.*

23. BERNSTEIN provided links that he described as illustrating that some NIST employees had been using their private gmail.com addresses for some of their work on this project. BERNSTEIN requested that NIST include these project records in its search. *Id.*

24. On March 21, 2022, NIST acknowledged receipt of the request and assigned reference number DOC-NIST-2022-001064 to the request. Ex. 2.

25. On March 28, 2022, NIST wrote to BERNSTEIN, claiming that the FOIA request included "any correspondence involving the word 'quantum'," that the request was "overly broad," and that NIST was unable to process the request. Ex. 3.

26. On April 12, 2022, BERNSTEIN wrote to NIST, emphasizing that he had asked merely for "records of NIST/NSA meetings mentioning the word 'quantum'," not for all correspondence mentioning the word. Ex. 1 at 5-6.

27. On May 2, 2022, NIST wrote to BERNSTEIN, claiming that the FOIA request had "no defined start date," that the request was "overly broad," and that NIST was unable to process the request. Ex. 4.

28. On May 4, 2022, BERNSTEIN referred to the original request, which did identify start dates or time frames where available. BERNSTEIN also provided additional time frames to help guide the search. Ex. 1 at 7-9.

29. BERNSTEIN also emphasized that the NIST Post-Quantum Cryptography Standardization Project "is a project that was initiated and named by NIST" and stated his understanding that NIST has a specific list of personnel working on the project. *Id.*

30. On June 3, 2022, BERNSTEIN sought an estimated date of completion for the request. Ex. 1 at 9.

31. On June 3, 2022, NIST stated that it is "in the process of estimating a fee estimate" for the request. NIST did not provide an estimated date of completion. Ex. 1 at 9.

32. As of the date of this filing, Defendants have failed to issue a determination letter and have failed to produce records responsive to the request.

33. The Defendants have also not complied with the statutory requirement under 5 U.S.C. §(a)(7)(B)(ii) to furnish an estimated date of completion when requested.

COUNT I – DEFENDANTS' FOIA VIOLATION:
FAILURE TO ISSUE A DETERMINATION

34. The above paragraphs are incorporated herein.

35. The request seeks the disclosure of agency records and was properly made.

36. NIST is a component of DOC and is subject to FOIA.

37. Included within the scope of the request are one or more records or portions of records that are not exempt under FOIA.

38. Defendants have failed to issue a determination within the statutory deadline.

COUNT II – DEFENDANTS' FOIA VIOLATION:
FAILURE TO CONDUCT A REASONABLE SEARCH

39. The above paragraphs are incorporated herein.

40. The request seeks the disclosure of agency records and was properly made.

41. NIST is a component of DOC and is subject to FOIA.

42. Defendants have failed to conduct a reasonable search for records responsive to the request.

COUNT III – DEFENDANTS' FOIA VIOLATION:
FAILURE TO PRODUCE RECORDS

43. The above paragraphs are incorporated herein.

44. The request seeks the disclosure of agency records and was properly made.

45. NIST is a component of DOC and is subject to FOIA.

46. Included within the scope of the request are one or more records or portions of records that are not exempt under FOIA.

47. Defendants have failed to produce records responsive to the request.

WHEREFORE, BERNSTEIN asks the Court to:

i. declare that Defendants have violated FOIA;

ii. order Defendants to issue a determination where appropriate;

iii. order Defendants to conduct a reasonable search for records;

iv. order Defendants to produce all non-exempt records responsive to the request or portions of records promptly;

v. enjoin Defendants from withholding non-exempt public records under FOIA;

vi. award BERNSTEIN attorneys' fees and costs; and

vii. award any other relief the Court considers appropriate.

Dated: August 5, 2022

RESPECTFULLY SUBMITTED,

/s/ *Matthew V. Topic*

Attorney for Plaintiff,
DANIEL J. BERNSTEIN

Matthew Topic, D.C. Bar No. IL 0037
Josh Loevy, D.C. Bar No. IL0105
Merrick Wayne, D.C. Bar No. IL 0058
Shelley Geiszler D.C. Bar No. IL 0087
LOEVY & LOEVY
311 North Aberdeen, 3rd Floor
Chicago, IL 60607
312-243-5900
foia@loevy.com