NSA, NIST, and post-quantum cryptography

Exhibit 1

14 Communications 4 Files

Share

Daniel J. Bernstein filed this request with the National Institute of Standards and Technology of the United States of America.

Tracking #	DOC-NIST-2022-001064
Submitted	March 15, 2022
Est. Completion	None

STATUS

Awaiting Response

Filter communications

Collapse All

From: Daniel J. Bernstein 03/16/2022

Subject: Freedom of Information Act Request: NSA, NIST, and post-quantum cryptography Email

1. Summary

This is a FOIA request for the records described below.

2. Preamble

NSA's policy decision to sabotage public cryptographic standards is described in an internal NSA history book released in 2013:

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB441/
https://archive.org/details/cold_war_iii-nsa/cold_war_iii-ISCAP/page/n239/mode/2up

The critical quote from NSA's history book is as follows: "Narrowing the encryption problem to a single, influential algorithm might drive out competitors, and that would reduce the field that NSA had to be concerned about. Could a public encryption standard be made secure enough to protect against everything but a massive brute force attack, but weak enough to still permit an attack of some nature using very sophisticated (and expensive) techniques?"

The first cryptographic mechanism standardized by NBS/NIST was DES in the 1970s. DES had a key size that was too small for security. The same history book reports that NSA had managed to "convince" the DES designers to reduce the key size.

In the 1990s, NIST proposed DSA, another cryptographic mechanism with a key size that was too small for security. A lawsuit by CPSR revealed that DSA had been secretly designed by NSA:

https://web.archive.org/web/20200229145033/https://catless.ncl.ac.uk/Risks/14/59

In 2005, 2006, and 2007, ISO, NIST and ANSI respectively issued standards for Dual EC, a cryptographic mechanism with an NSA back door:

https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

The same 2013 report describes NSA's budget to "covertly influence and/or overtly leverage" cryptography to make it "exploitable", in NSA's words. The budget had grown to a quarter of a billion dollars per year. Presumably NSA's budget for cryptographic sabotage is even larger today.

NIST's Dual EC post-mortem concluded that "It is of paramount importance that NIST's process for developing cryptographic standards is open and transparent and has the trust and support of the cryptographic community":

https://web.archive.org/web/20220219211917/https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

The same post-mortem shows NIST's invited reviewers recommending clear transparency rules, such as "full documentation of all decisions, and clear processes for the disposition of each and every comment received", along with being open about "what authorities were consulted".

In 2016, NIST's call for proposals for its Post-Quantum Cryptography Standardization Project stated that "NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public":

https://web.archive.org/web/20220119113311/https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

81 FR 92787 says that this call for proposals establishes the criteria "that will be used to appraise the candidate algorithms":

https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms

Regarding the Post-Quantum Cryptography Standardization Project, NIST stated in October 2021 that "We operate transparently. We've shown all our work":

https://web.archive.org/web/20211115191840/https://www.nist.gov/blogs/taking-measure/post-quantum-encryption-qa-nists-matt-scholl

However, my current understanding is that, for five years, NIST was intentionally concealing NSA's involvement in this project. On 22 July 2020, NSA and NIST issued coordinated announcements that made reasonably clear NSA was involved but that did not reveal the details. On 2 August 2020, I asked "What exactly has NSA told NIST regarding NISTPQC, regarding security levels or otherwise?" NIST did not answer. NIST later tried to suggest that NSA has had only a minor influence, but NIST has provided no records showing what NSA's input actually was.

More broadly, most of the information that I've found on NIST's web site for this project is simply copies of submissions. NIST has posted some extra information, but the total volume of information in NIST's reports, web pages, and mailing-list messages obviously falls far short of "all our work". Anyone trying to obtain more than a superficial understanding of what has happened in this project rapidly discovers that critical information is missing. See Section 5 of the following paper for various examples of mysteries regarding the NIST process:

https://cr.yp.to/papers/categories-20200918.pdf

I've filed six FOIA requests with NIST since mid-2020. NIST has released a few dribbles of information, but in general NIST's responses have been very slow and obviously not complete. For example, my FOIA request #20210610-NIST eight months ago, which asked for "copies of all NIST records of communication between NSA and NIST regarding the NIST Post-Quantum Cryptography Standardization Project", has, so far, produced zero records, even though NIST had already admitted in the following document that it made changes to a report based on "feedback received (from the NSA)":

https://web.archive.org/web/20210508052729/https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf

Analyzing NSA's impact on this project will require not just seeing NSA's communication with NIST, but also tracing how NIST's decisions were made and analyzing the influence of the information that NIST received from NSA. If each step of this analysis requires dealing with another round of stonewalling from NIST then the analysis will obviously not be done in time to help the public make safe decisions regarding post-quantum cryptography.

NSA's documented history of sabotage, along with its evident sway over NIST, makes NSA's influence on NIST a high priority to review, but it also seems likely that other entities have also been trying to sabotage NIST's process. As far as I can tell, NIST has no procedures in place to prevent attackers from influencing the project through pseudonyms, proxies, etc. Anything short of a full review of project records could easily miss evidence of attacks.

Even without sabotage, getting cryptography right is challenging. Public review has identified security flaws in dozens of submissions and has identified many errors in the limited additional information released by NIST. Having NIST keep most of its analysis secret is a recipe for disaster. Given that NIST promised to be "open and transparent", and recently claimed to have "shown all our work", it's hard to understand why the full project records aren't already available to the public.

3. Request for records

Please send me, in electronic form, a copy of NIST's records regarding the NIST Post-Quantum Cryptography Standardization Project. Specifically, I am requesting 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 (20 December 2016);

(2) records of the submission phase, meaning the period starting from the issuance of 81 FR 92787 and continuing through the submission deadline (30 November 2017);

(3) records of the first round, meaning the period starting from the submission deadline and continuing through the issuance of NIST IR 8240 (31 January 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 (22 July 2020); and

(5) more recent records, up to the day that this request is processed.

This request includes the full records of the project, and also includes any further records referencing the project.

This request includes, but is not limited to, documents from NIST, documents from NSA, documents from other U.S. government agencies, and documents from foreign government agencies. This request also includes all records of NIST/NSA meetings mentioning the word "quantum", whether or not NIST views those meetings as part of this project. This request also includes all records of NSA's writeup of post-quantum cryptography mentioned at the 27 August 2013 NIST/NSA meeting.

If there are any responsive records that are publicly available on NIST's web site as of the date that this request is processed, I request that NIST provide the specific URL for each record. Please clearly indicate any such parts of your response as "Records already available".

For all other responsive records, I request that NIST deliver the records in their original electronic format, such as PDF format, or as PDF scans for documents that were originally created on paper.

For email messages sent publicly to NIST's pqc-forum mailing list, I am willing to narrow the scope of this request to records showing the metadata of each message, at least the date and time. (It should be easy for NIST to produce a list of metadata. Please note that pqc-forum email dated 21 Nov 2021 16:20:14 +0100 and 21 Nov 2021 21:44:58 +0100 pointed out a pqc-forum message missing from Google's archive; I presume there are more messages missing.)

Regarding the search of the records, it has come to my attention that some NIST employees have been using their private gmail.com addresses such as dbmoody25@gmail.com and dapon.crypto@gmail.com for some of their work on this project, as the following documents illustrate:

https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/fvnhyQ25jUg/m/NCduE66ZBAAJ
https://web.archive.org/web/20220223131246/https://www.cs.umd.edu/~gasarch/COURSES/456/F21/L.pdf

I request not just project records stored on government servers, but also project records that NIST employees have stored on private servers such as gmail.com.

4. Request for fee categorization

Please confirm that you're categorizing this FOIA request, like my previous FOIA requests, under the "educational" requester category. You can find my University of Illinois at Chicago profile here:

https://cs.uic.edu/profiles/daniel-j-bernstein/

Here is an example of a paper that I coauthored analyzing previous NSA sabotage of cryptographic standards:

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

This paper was published as pages 256 through 281 in "The new codebreakers", edited by Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, Lecture Notes in Computer Science 9100, Springer, 2015, ISBN 978-3-662-49300-7. The paper already has more than 100 citations, according to Google Scholar.

5. Request for fee waiver

I request a waiver of all fees. I am filing this request via MuckRock to ensure that the results will be made easily available to journalists and to the general public. This disclosure will contribute significantly to public understanding of NIST activities, and I have no commercial interest that would be furthered by the requested disclosure.

Regarding the six fee-waiver factors:

(1) Whether the subject of the requested records concerns "the operations or activities of the government": 81 FR 92787 is a Federal Register notice calling for submissions to a government project and saying how the submissions would be evaluated. This is a request for the records of what has happened in that project.

(2) Whether the disclosure is "likely to contribute" to an understanding of government operations or activities: Given records from the 1970s through the 2010s demonstrating NSA motivations, budgets, and activities to sabotage cryptographic standards (see links above), presumably NSA has also been trying to sabotage the NIST Post-Quantum Cryptography Standardization Project. Documents released in the past have played a major role in public analyses of NSA sabotage and other problems with NIST's cryptographic standards; see, e.g., the role of these releases in https://cr.yp.to/talks.html#2013.12.28.

(3) Whether disclosure of the requested information will contribute to "public understanding" as opposed to just "individual understanding": I have already posted a variety of in-depth analyses of the limited information that NIST has released so far regarding the Post-Quantum Cryptography Standardization Project (see, e.g., https://cr.yp.to/papers/categories-20200918.pdf), and will similarly post analyses of the further information released under this FOIA request. Cryptography is a technical subject, but there are more than 1000 members of the International Association of Cryptologic Research. There are also established mechanisms of bringing cryptographic news to broader audiences and to the general public, reflecting the public interest in the safety of Internet communication. I have been fighting NSA's cryptographic sabotage for 30 years (see, e.g., _Bernstein v. United States_, 176 F.3d 1132); together with colleagues, I have found many problems with NIST's previous NSA-influenced work on cryptography (see, e.g., https://cr.yp.to/newelliptic/nistecc-20160106.pdf), and have given talks to audiences of thousands based on NSA/NIST documents (see, e.g., https://cr.yp.to/talks.html#2013.12.28).

(4) Whether the disclosure is likely to contribute "significantly" to public understanding of government operations or activities: The limited information that NIST has released regarding the Post-Quantum Cryptography Standardization Project provides only superficial explanations of what happened in the project. It is impossible today for the public to track what inputs were provided to NIST and to analyze how the inputs influenced NIST's decisions, whereas transparency will give the public an answer to these critical questions. Transparency was also highlighted in NIST's Dual EC post-mortem (see link above), recognizing the effectiveness and importance of public disclosures of this type of information regarding cryptographic standards.

(5) Whether the requester has a commercial interest that would be furthered by the requested disclosure: No. I'm a professor. I make my work available for free with no royalties. My interest is in ensuring the safety of cryptographic mechanisms used by the general public.

(6) Whether any such commercial interest outweighs the public interest in disclosure: Not applicable. See #5.

Please let me know if you need any further information.

---Daniel J. Bernstein

From: National Institute of Standards and Technology 03/21/2022

Subject: FOIA: DOC-NIST-2022-001064: Acknowledgement Letter Email

Good afternoon,

Attached you will find the following correspondence in regards to FOIA: DOC-NIST-2022-001064. Thank you.

Matthew Gonzales, PMP
Management Analyst
United States Department of Commerce
National Institute of Standards and Technology
Office of the Director, Management & Organization Office

100 Bureau Drive, Mail Stop: 1710
Gaithersburg, MD 20899
Office: 301-975-4092
Email: matthew.gonzales@nist.gov<mailto:matthew.gonzales@nist.gov>

2022-001064_Acknowledgement_Lettercsf

View Embed Download

From: National Institute of Standards and Technology 03/28/2022

Subject: FOIA: DOC-NIST-2022-001064: Clarification Letter Email

Good afternoon,

Attached you will find the following correspondence regarding FOIA: DOC-NIST-2022-001064. Thank you.

Matthew Gonzales, PMP
Management Analyst
United States Department of Commerce
National Institute of Standards and Technology
Office of the Director, Management & Organization Office

100 Bureau Drive, Mail Stop: 1710
Gaithersburg, MD 20899
Office: 301-975-4092
Email: matthew.gonzales@nist.gov<mailto:matthew.gonzales@nist.gov>

2022-001064_Clarification_Letter_csf

View Embed Download

From: Daniel J. Bernstein 04/12/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

1. NIST's 21 March 2022 letter acknowledges receipt of my FOIA request. I appreciate this acknowledgment. Unfortunately, this letter also misquotes the FOIA request.

For example, immediately after initial quotation marks, NIST writes "the electronic form of NIST's records", which could easily be understood as asking merely for the records that happen to be in electronic form. The FOIA request actually asked NIST to "send me, in electronic form, a copy of NIST's records" and included asking for "PDF scans for documents that were originally created on paper". I wish to receive the records in electronic format; this does not mean that my request excludes paper records.

As another example, NIST's quotation says "more recent records leading up to the day of this request", whereas the FOIA request actually asked for "more recent records, up to the day that this request is processed". This is an important difference, given NIST's overall pattern of serious delays in handling my FOIA requests. Please make sure

that NIST's search includes records up to the date the request is processed, rather than discarding records merely because they are after the date of the request (15 March 2022).

There are more examples. To avoid ongoing confusion, I request that NIST withdraw its 21 March 2022 characterization of my FOIA request. I would also appreciate confirmation that NIST's FOIA personnel have read fully through my FOIA request and were not intending to use NIST's 21 March 2022 text as a replacement for the text of the FOIA request.

2. NIST's 28 March 2022 letter claims that the FOIA request "included any correspondence involving the word 'quantum' which will be voluminous and include a significant number of documents that are outside the scope of the Post Quantum Cryptography Standardization Project".

In fact, this portion of the FOIA request asks merely for "records of NIST/NSA meetings mentioning the word 'quantum', whether or not NIST views those meetings as part of this project". The "NIST/NSA meetings" phrase is important, and is much narrower than NIST's "any correspondence" paraphrase.

Regarding the FOIA request as a whole, I would expect almost all of the responsive records to be the records of NIST's Post-Quantum Cryptography Standardization project, with very little volume added by the records of NIST/NSA meetings.

Going forward, I would appreciate confirmation that NIST will take due care in handling my FOIA request, and in particular in double-checking the text of my FOIA request.

3. NIST's 28 March 2022 letter (a) claims that "the document descriptions are overly broad", (b) claims that as a result NIST is unable to process my request, and (c) asks me to narrow the request.

As a preliminary matter, my understanding is that breadth per se is not an exception to FOIA:

https://www.justice.gov/oip/blog/foia-update-foia-counselor-questions-answers-21

More to the point, I see no factual basis for any of (a), (b), (c). Again, it's simply not true that I asked NIST for all correspondence involving the word "quantum".

4. NIST's 28 March 2022 letter asks for "clarification" of my FOIA request.

If NIST quotes the FOIA request and explains why it doesn't find the quoted text clear, then I'll consider the explanation, and, if there's actually an issue, clarify the text. However, I see nothing from NIST pointing to anything unclear in the FOIA request.

I've also double-checked the FOIA request and see nothing ambiguous. The request clearly identifies the records that I would like to see.

5. To summarize, I see no basis for NIST not processing my FOIA request as is. Please confirm that NIST will process the request. Please let me know if you have any further questions.

---Daniel J. Bernstein

From: National Institute of Standards and Technology 05/02/2022

Subject: FOIA: DOC-NIST-2022-001064: Clarification Letter Email

Good afternoon,

Attached you will find the following correspondence regarding FOIA: DOC-NIST-2022-001064. Thank you.

Matthew Gonzales, PMP
Management Analyst
United States Department of Commerce
National Institute of Standards and Technology
Office of the Director, Management & Organization Office

100 Bureau Drive, Mail Stop: 1710
Gaithersburg, MD 20899
Office: 301-975-4092
Email: matthew.gonzales@nist.gov<mailto:matthew.gonzales@nist.gov>

2022-001064_Clarification_Letter_2_5.2.22csf

View Embed Download

From: Daniel J. Bernstein 05/04/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

1. NIST's 2 May 2022 letter states that NIST is "unable to process your FOIA request as submitted because the document descriptions are overly broad".

As I wrote before, my understanding is that breadth per se is not an exception to FOIA:

https://www.justice.gov/oip/blog/foia-update-foia-counselor-questions-answers-21

Even if a FOIA request is for an "enormous volume of records" (never mind the question of whether a single NIST project could qualify as "enormous"), the Department of Justice writes that this "does not entitle an agency to deny that request on the ground that it does not 'reasonably describe' records within the meaning of 5 U.S.C. § 552(a)(3)(A)".

Please confirm that NIST will go ahead with processing my FOIA request. Going forward, if NIST believes that it has authority under FOIA for not processing part or all of my request, please cite the specific authority.

2. NIST states that an example of my request being "overly broad" is that "there is no defined start date for this request that is identified".

I requested "NIST's records regarding the NIST Post-Quantum Cryptography Standardization Project". The NIST Post-Quantum Cryptography Standardization Project is a project that was initiated and named by NIST. It should be easy for NIST to locate the complete project records.

Part (1) of the request is for "records of the project phase leading up to the call for submissions, meaning the period before the issuance of 81 FR 92787 (20 December 2016)". The reason this does not identify a start date is that I do not know NIST's project start date. NIST's project web page

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

says that "NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms" and points to a 2016 press release, but does not make clear how much earlier NIST began the process internally. If NIST is unable to determine from its own records when the NIST Post-Quantum Cryptography Standardization Project began, then I will accept 1 January 2013 as a start date for NIST's search. I will also accept 1 January 2013 as a start date for the search of records that are outside the project but reference the project.

Parts (2), (3), (4), and (5) of the request already have explicit start dates. Regarding the further request for "all records of NIST/NSA meetings mentioning the word 'quantum', whether or not NIST views those meetings as part of this project", please see below regarding dates.

3. NIST states that it has "been working on the field of quantum and encryption for many years and a search start date would help scope the material".

I understand that the NIST Post-Quantum Cryptography Standardization Project has been running for years. I would like copies of the project records. If there is some reason that locating the complete project records is difficult, please tell me what the difficulty is. I did not ask for a general search of all NIST records that might be in "the field of quantum and encryption".

4. NIST states that it "has also had staff changes and technology updates throughout the years (in both mail and file storage) and this would help us focus the search".

My understanding is that NIST has a specific list of personnel working on the NIST Post-Quantum Cryptography Standardization Project. I understand that there are sometimes changes of personnel; I expect agencies to maintain records centrally so that changes of personnel do not interfere with FOIA and other records-management requirements. If NIST is facing a specific problem with its records-management technology, please tell me what that problem is.

5. NIST states that "FOIA requests do not include the scope of publicly available materials" and gives various links to related NIST web pages.

As already noted in my FOIA request, the total volume of information in NIST's reports, web pages, and mailing-list messages obviously falls far short of NIST's complete work on the project. My FOIA request gives various examples of missing information, and explains how NIST's stonewalling regarding my previous FOIA requests has led to my current request for the complete project records.

The reason I am not excluding publicly available materials from the scope of my FOIA request is that, with all due respect to the people involved, I believe NIST will abuse such an exclusion to conceal records that NIST internally claims are publicly available but that the public cannot actually find. So I requested "the specific URL for each record"; for example, for a PDF that was submitted to NIST and that NIST posted on its web page, the request is for a URL of that PDF, rather than a copy of the PDF. Please note that each URL for a NIST web page is a NIST record subject to FOIA.

6. NIST states that "Email meta data is unclear".

This appears to be in response to the following portion of my FOIA request: "For email messages sent publicly to NIST's pqc-forum mailing list, I am willing to narrow the scope of this request to records showing the metadata of each message, at least the date and time".

In the context of email messages, "metadata" is a standard way to refer to date, time, sender, recipient list, etc. Surely NIST's pqc-forum operator has a central archive of the list messages, including a complete index of those messages. Whatever metadata appears in the index is fine with me as long as it includes a separate line for each message, showing at least the date and the time of that message.

7. NIST objects to the pqc-forum portion of my request by saying that this information would be publicly available and that I have been on the mailing list "from the start of that service".

However, my FOIA request specifically states "Please note that pqc-forum email dated 21 Nov 2021 16:20:14 +0100 and 21 Nov 2021 21:44:58 +0100 pointed out a pqc-forum message missing from Google's archive; I presume there are more messages missing."

Given the documented discrepancies in NIST's delivery of pqc-forum messages to different recipients, I would like to be able to check for further pqc-forum messages that NIST has delivered neither to Google nor to me. A list of metadata will suffice for this. (Once I have received the list, I will follow up with specific requests for copies of any messages that turn out to be missing.)

8. NIST also states that "meetings between NIST and NSA that mentions the word 'quantum' is well beyond the scope of Post-Quantum Cryptography" and continues by giving miscellaneous examples of NIST's "long history in quantum information, standards and technology".

But this part of my request is not for NIST's long history in the topic in general. It is specifically regarding meetings that NIST had with NSA. I understand that NIST may view these meetings as being outside the

scope of the Post-Quantum Cryptography Standardization Project, which is exactly why I made a special request for these records: "This request also includes all records of NIST/NSA meetings mentioning the word 'quantum', whether or not NIST views those meetings as part of this project."

Regarding dates, the first publication of a quantum algorithm threatening cryptography was in 1994, so it would be reasonable for NIST's search for the records of NIST/NSA meetings mentioning the word "quantum" to go back through 1 January 1994. How often do NIST and NSA meet? Once a month, so in total just a few hundred sets of minutes from 1994 through 2022?

Even if the meetings are more frequent, searching the meeting records for the word "quantum" should not be difficult. As I wrote previously: "Regarding the FOIA request as a whole, I would expect almost all of the responsive records to be the records of NIST's Post-Quantum Cryptography Standardization project, with very little volume added by the records of NIST/NSA meetings."

9. NIST also states that "Clarification of the scope of your request will help ensure the response is not overwhelming to yourself and will focus the response to the specific materials you are interested in".

My FOIA request is already asking specifically for the materials that I am interested in. I see nothing unclear. I appreciate NIST's concern for my reading time.

10. NIST states that it "is only required to search records in our custody and control" and continues by saying that FOIA does not provide access to records held "by private businesses or individuals".

It is not clear to me whether this is meant to respond to the portion of my FOIA request giving evidence that "some NIST employees have been using their private gmail.com addresses such as dbmoody25@gmail.com and dapon.crypto@gmail.com for some of their work on this project". Please confirm that NIST will search not just project records stored on government servers, but also project records that any of the relevant NIST employees have stored on private servers.

11. NIST states "If you wish to pursue your request, please describe as best as possible the records you are requesting".

I wish to pursue the request. My original FOIA request already clearly identifies the records that I would like to see. Nothing I have seen from NIST identifies any ambiguities in the FOIA request. Please confirm that NIST will process the request as filed. Please let me know if you have any further questions.

---Daniel J. Bernstein

From: Daniel J. Bernstein 06/03/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

Pursuant to 5 U.S.C. § 552(a)(7)(B)(ii), I request an estimated date of completion for DOC-NIST-2022-001064.

---Daniel J. Bernstein

From: National Institute of Standards and Technology 06/03/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

Good morning,

The responsive office is in the process of estimating a fee estimate for this and as soon as an estimate is done you will receive an estimate for the searching and duplication of the potential responsive documents and then the responsive office will be tasked in gathering the potential responsive documents. Any documents that are responsive to this request will be sent to you on a rolling basis. Thank you.

From: Daniel J. Bernstein 06/03/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

5 U.S.C. § 552(a)(7)(B)(ii) is part of the FOIA statute. It requires an agency that received a FOIA request to provide, when asked, "an estimated date on which the agency will complete action on the request."

On this basis, I asked for "an estimated date of completion for DOC-NIST-2022-001064." NIST's statement that "Any documents that are responsive to this request will be sent to you on a rolling basis" is not an answer.

To repeat: Pursuant to 5 U.S.C. § 552(a)(7)(B)(ii), please tell me an estimated date on which NIST will complete action on DOC-NIST-2022-001064. Thank you in advance for your cooperation.

---Daniel J. Bernstein

From: National Institute of Standards and Technology 06/14/2022

Subject: FOIA: DOC-NIST-2022-001064: Fee Estimate Letter Email

Good afternoon,

Please see the attached correspondence regarding FOIA: DOC-NIST-2022-001064. Thank you.

Matthew Gonzales, PMP
Management Analyst
United States Department of Commerce
National Institute of Standards and Technology
Office of the Director, Management & Organization Office

100 Bureau Drive, Mail Stop: 1710
Gaithersburg, MD 20899
Office: 301-975-4092
Email: matthew.gonzales@nist.gov<mailto:matthew.gonzales@nist.gov>

2022-001064_Fee_Estimate_Letter_and_Fee_Waiver_Denialcsf

View Embed Download

From: Daniel J. Bernstein 06/29/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

NIST's 14 June 2022 message indicates that NIST's initial estimate is that there are under 100 pages of records responsive to my FOIA request. The centerpiece of the request is asking for "a copy of NIST's records regarding the NIST Post-Quantum Cryptography Standardization Project".

The under-100-page estimate is surprising and concerning.

NIST issued a 27-page report (NIST IR 8240) on this project in 2019, listing 12 authors, and a 39-page report (NIST IR 8309) on this project in 2020, listing 13 authors. My understanding is that several of these authors have been working on this project full-time for several years and have generated many pages of project records that are not currently available to the public, including extensive email exchanges with NSA and other entities outside NIST, such as defense contractors.

In your search for responsive records, please make sure to include any project record generated by, received by, or under custody of any of the authors of the project reports. In particular, each of the following individuals is listed as an author of NIST IR 8240 or NIST IR 8309 or both: Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone. Given federal recordkeeping requirements, I expect that your search can access all project records even when the individuals involved are no longer employed by NIST. Please also keep in mind the evidence provided in my FOIA request that some of these individuals used gmail.com for some of their work on this project.

Please let me know by the end of next week if you have any updates to your estimate of the number of responsive pages.

---Daniel J. Bernstein

From: National Institute of Standards and Technology 06/30/2022

Subject: RE: Freedom of Information Act Request #DOC-NIST-2022-001064 Email

Good morning,

The charges are for the first 100 pages of duplication, if the responsive documents are electronic there are no duplication fees, therefore there could be over 100 pages of electronic documents, but just under 100 pages of hard copy responsive documents that need to be duplicated if that makes sense so there could be over 100 pages of responsive documents for this FOIA, if the bulk or all of them are electronic there are no duplication fees though. Thank you.

Exhibit 2

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

Mr. Daniel J. Bernstein
MuckRock News
DEPT MR 126349
411A Highland Ave.
Somerville, MA 02144-2516
126349-45451275@requests.muckrock.com

Dear Mr. Bernstein:

This acknowledges receipt of your March 17, 2022, Freedom of Information Act (FOIA) request to the National Institute of Standards and Technology (NIST) in which you requested: **"The electronic form of NIST's records regarding the NIST Post-Quantum Cryptography Standardization Project. Specifically, I am requesting records of the project phase leading up to the call for submissions, records of the submission phase, records of the first round, records of the second round and more recent records leading up to the day of this request. Documents from NIST, documents from NSA, documents from other U.S. government agencies and documents from foreign government agencies. This request also includes all records from NIST/NSA meetings mentioning the word "quantum", whether or not NIST views those meetings as part of this project. This request also includes all records of NSA's writeup of post-quantum cryptography mentioned at the 27th August 2013 NIST/NSA meeting.**

Your request was received at the FOIA Control Desk on March 17, 2022 and was assigned FOIA Log # DOC-NIST-2022-001064.

FOIA allows agencies twenty working days to make a determination on the request. However, it may not always be possible to provide the documents within this time period. In some cases, we may take an extension and will advise you. Please be advised that your request may be subject to fees for search, review, and reproduction costs. Should this be the case, you will be given an estimate of the costs. Fee estimates are developed in good faith and are based on our reasonable judgment. However, due to the unique nature of each request and complexity of documents involved, actual costs to search and review the material may vary from the original estimate.

Matt Gonzales, a Management Analyst in my office, is the contact point for processing your request. If you have any questions regarding your pending FOIA request, he may be reached by email at foia@nist.gov.

Sincerely,

Catherine S. Fletcher
Freedom of Information Act Officer

Exhibit 3

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

Mr. Daniel J. Bernstein
MuckRock News
DEPT MR 126349
411A Highland Ave.
Somerville, MA 02144-2516
126349-45451275@requests.muckrock.com

Dear Mr. Bernstein,

This letter is in response to your March 17, 2022, e-mail to the National Institute of Standards and Technology (NIST), Freedom of Information Act (FOIA) office for information. Your request was received at the FOIA Control Desk on March 17, 2022 and assigned FOIA Log Number DOC-NIST-2022-001064.

We are unable to process your FOIA request as submitted because the document descriptions are overly broad. For example, your request included any correspondence involving the word "quantum" which will be voluminous and include a significant number of documents that are outside the scope of the Post Quantum Cryptography Standardization Project. Please provide more specific descriptions or clarification of the particular documents you are requesting for each item in your request.

The FOIA, which can be found in Title 5 of the United States Code, section 552, provides that a person may obtain access to federal agency records, except to the extent that such records are protected from public disclosure. The FOIA does not, however, provide access to records held by Congress or the federal courts, by state or local government agencies, or by private businesses or individuals.

A FOIA request can be made for any agency record that is not publicly available. If you wish to pursue your request, please describe as best as possible the records you are requesting. In your description include information such as the date and place the records were created, the file descriptions, subject matter, persons involved, and other pertinent details that will help identify the records. For your convenience, FOIA information can be viewed from http://www.nist.gov/director/foia/ . Other helpful FOIA information can be found at: http://www.usdoj.gov/oip/index.html.

NIST

If we do not receive clarification or a revised request by COB, April 28, 2022, we will assume that you are no longer interested in receiving the documents requested and your FOIA request will be closed.

Sincerely,

Catherine S. Fletcher
Freedom of Information Act Officer

Exhibit 4

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

Mr. Daniel J. Bernstein
MuckRock News
DEPT MR 126349
411A Highland Ave.
Somerville, MA 02144-2516
126349-45451275@requests.muckrock.com

Dear Mr. Bernstein,

This letter is in response to your March 17, 2022, e-mail to the National Institute of Standards and Technology (NIST), Freedom of Information Act (FOIA) office for information. Your request was received at the FOIA Control Desk on March 17, 2022 and assigned FOIA Log Number DOC-NIST-2022-001064.

After speaking with the program office assigned to this request, we are unable to process your FOIA request as submitted because the document descriptions are overly broad. For example, there is no defined start date for this request that is identified. NIST has been working on the field of quantum and encryption for many years and a search start date would help scope the material. NIST has also had staff changes and technology updates throughout the years (in both mail and file storage) and this would help us focus the search.

FOIA requests do not include the scope of publicly available materials. The following links will contain some information on NIST research involving post-quantum cryptography that is already available that may help you as well: https://csrc.nist.gov/Projects/post-quantum-cryptography (this is the top page for post-quantum cryptography). The next links are some sub pages that you may find useful: https://csrc.nist.gov/publications/search?keywords-lg=PQC&sortBy-lg=relevance&viewMode-lg=brief&ipp-lg=25&topicsMatch-lg=ANY&controlsMatch-lg=ANY (this link is for published papers that ITL hosts), https://www.nist.gov/fusion-search?s=PQC&start=0&sort=relevance (this link is a search result on all of NIST post-quantum cryptography), and https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (this last link is for applied work in post-quantum cryptography migration).

Email meta data is unclear, and the example cited is public meta data on public message emails. This information would be publicly available. After speaking with the program office, we were notified that you are on the mailing list for post-quantum cryptography and have been from the start of that service.

Meetings between NIST and NSA that mentions the word “quantum” is well beyond the scope of Post-Quantum Cryptography. NIST has a long history in quantum information, standards and technology, which include, as example, atomic clocks; bose-einstine condensates; quantum bell testing; Laser Ion traps, Quantum Dots; Quantum Economic

Development Consortium; Quantum Mathematics; Quantum Communications; etc. Clarification of the scope of your request will help ensure the response is not overwhelming to yourself and will focus the response to the specific materials you are interested in.

In addition, NIST is only required to search records in our custody and control. If you are interested in records from other federal agencies, you will need to make a FOIA request directly to them. Other agency FOIA contacts can be found at www.foia.gov and on the agencies' websites.

The FOIA, which can be found in Title 5 of the United States Code, section 552, provides that a person may obtain access to federal agency records, except to the extent that such records are protected from public disclosure. The FOIA does not, however, provide access to records held by Congress or the federal courts, by state or local government agencies, or by private businesses or individuals.

A FOIA request can be made for any agency record that is not publicly available. If you wish to pursue your request, please describe as best as possible the records you are requesting. In your description include information such as the date and place the records were created, the file descriptions, subject matter, persons involved, and other pertinent details that will help identify the records. For your convenience, FOIA information can be viewed from http://www.nist.gov/director/foia/ . Other helpful FOIA information can be found at: http://www.usdoj.gov/oip/index.html.

If we do not receive clarification or a revised request by COB, June 2, 2022, we will assume that you are no longer interested in receiving the documents requested and your FOIA request will be closed.

Sincerely,

Catherine S. Fletcher
Freedom of Information Act Officer