



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 19136D
13 February 2007

Mr. John L. Young
CRYPTOME
Suite 6E
251 West 89th Street
New York, NY 10024

Dear Mr. Young:

This is an interim response to your Freedom of Information Act (FOIA) request of 16 November 2000 for "information and documents on the invention, discovery and development of 'non-secret encryption' (NSE) and public key cryptography (PKC) by United Kingdom, United States, or any other nation's intelligence and cryptology agencies, prior to, parallel with, or subsequent to, the PKC work of Diffie-Hellman-Merkle." This request was narrowed on 8 September 2001 to be for documents in the year 1970, or the earliest year other than 1970, concerning NSE, as described in the paper by J.H. Ellis, "The Possibility of Secure Non-Secret Digital Encryption," CESG Report, January 1070; and documents concerning PKC by the US or other nations. A copy of this narrowed request is enclosed. For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. As such, you are allowed two hours of search and the duplication of 100 pages at no cost. You have already paid search and estimated duplication costs. Final assessment of fees related to duplication, or any remaining refund that you may be due, will be addressed in our final response. Your request has been processed under the FOIA, and some of the documents you requested are enclosed. Certain information, however, has been deleted from the enclosures and nine documents (163 pages) have been withheld in their entirety.

Some of the information withheld was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraphs (b), (c) and (g) of Section 1.4 and remains classified TOP SECRET, SECRET, and CONFIDENTIAL as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Some of the information is exempt from automatic declassification in accordance with Section 3.3(b)(1) and (6) of E.O. 12958, as amended. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

Furthermore, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

In addition, some of the information has been deleted from the enclosures pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as attorney-client privileged information.

Since some documents were withheld in their entirety and information was withheld from the enclosures, you may construe this as a partial denial of your request. You are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DC34), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Please be advised that records responsive to your request include documents originating with another government agency, as well as NSA documents containing the other government's agency's information. Because we are unable to make determinations as to the releasability of the other agency's information, the subject documents have been referred to the appropriate agency for review. We will respond to you further when consultation with the other agency has been completed.

Sincerely,

A handwritten signature in black ink, appearing to read "Louis F. Giles". The signature is fluid and cursive, with the first name "Louis" and last name "Giles" clearly distinguishable.

LOUIS F. GILES
Director of Policy

Encls:
a/s

CRYPTOME 251 WEST 89TH ST SUITE 6E NEW YORK NY 10024 212-873-8700

Attention: FOIA Office

April 20, 2003

By fax to: 301-688-4762

Pamela N. Phillips
Chief, FOIA/PA Services
FOIA Office (DC321)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

Re FOIA Case: 19136A

Dear Ms. Phillips,

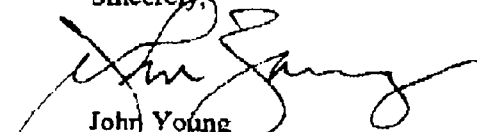
We last spoke by telephone on May 23, 2003, when you responded to my letter inquiry on that date. You said then my request was No. 45 in the easy queue. Could you say when NSA expects to answer my FOIA request of October 9, 1999:

"Under the Freedom of Information Act I request any and all information and documents on:

The invention, discovery and development of "non-secret encryption" (NSE) and public key cryptography (PKC) by United Kingdom, United States, or any other nation's intelligence and cryptology agencies, prior to, parallel with, or subsequent to, the PKC work of Diffie-Hellman-Merkle."

Thank you very much.

Sincerely,



John Young
E-mail: jya@pipeline.com
Fax: 212-787-6102