U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

DIS-3 OT:RR:RDL:FAP
CBP-AP-2022-105931 MMC

August 9, 2022

Mr. Andrew Free
Muck Rock News Dept. MR12821
411A Highland Ave
Somerville, MA 02144

RE: Freedom of Information Act Appeal; Password Protected Responses; CBP-2022-072754

Dear Mr. Free:

This is in response to your July 18, 2022, request indicating your intent to appeal the May 3, 2022, no records found decision of the Freedom of Information Act (hereinafter "FOIA") Division, Privacy and Diversity Office, U.S. Customs and Border Protection ("CBP").

In your original request you sought (a) the legal authority from which your FOIA Office claims it derives the power to place nonexempt public records responsive to FOIA requests into a password-protected document. (b) the Standard Operating Procedure used by your FOIA Office to assign non-exempt records a password. (c) any contract materials with any third-party reflecting monies paid by your agency to outside contractors for password protecting FOIA documents. (d) any record reflecting the total time FOIA Office personnel dedicated during FY20, FY21 and FY22 (to date) to password-protecting records. (e) any governing policy denoting when password protection is appropriate, and when it is not.

The FOIA Division indicated that it found no records responsive to your request. You are now questioning the adequacy of the FOIA Division's search. We are not aware of any contracts or records that track time dedicated to password-protecting records. However, with respect to authority, standard operating procedure and policy, we offer the following:

Background: Safeguarding Personally Identifiable Information

Every staff member of the Department of Homeland Security (DHS) is charged with safeguarding the collection, maintenance, use, and dissemination of personally identifiable information.

There are two kinds of personally identifiable information "Personally Identifiable Information" and "Sensitive Personally Identifiable Information". DHS defines "Personally Identifiable Information" (PII), as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive Personally Identifiable Information (SPII) requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of SPII include but are not limited to your Social Security number (SSN), passport number, alien number, fingerprint number and driver's license or state identification number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.

General policies exist at DHS to safeguard the collecting, assessing, using and sharing of SPII. When a requestor has an account in FOIA Online, the requester accesses the responsive records containing SPII by going in to their FOIA Online account. However, when a requestor does not have a FOIA Online account, the SPII must be transmitted outside of the DHS network via email. DHS policy states that SPII should be encrypted, or password protected if emailed outside the DHS network.

Publicly Available Documents

Concerning your request for specific information about password protecting documents and the purpose for doing so, we direct you to two publications found on the DHS website. Please see the Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Revision 3, Published by the DHS Privacy Office, December 4, 2017 available on line at: https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information See also: Instruction on the Collection, Use, Retention and Dissemination of Personally Identifiable Information https://www.dhs.gov/publication/collection-use-retention-and-dissemination-personally-identifiable-information

Judicial Review and OGIS

In the event that you are dissatisfied with the disposition of your appeal, you may obtain judicial review of this FOIA decision pursuant to the provisions of 5 U.S.C. §552(a) (4)(B) in the United States District Court in the District in which you reside, in the district where the agency records are situated, or in the United States District Court for the District of Columbia.

As part of the 2007 FOIA amendments, the Office of Government Information Services (OGIS) was created to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974.

You may contact OGIS in any of the following ways:

National Archives and Records Administration, Office of Government Information Services
8601 Adelphi Road (OGIS) College Park, MD20740: Phone 202-741-5770: Fax 202-741-5769:
Toll Free 1 877 684-6448: www.archives.gov/ogis

Sincerely,

Shari Suzuki

Shari Suzuki, Chief
FOIA Appeals and Policy Branch
Regulations and Rulings
Office of Trade