



DEFENDING RIGHTS & DISSENT

Formerly Bill of Rights Defense Committee/ Defending Dissent Foundation

1325 G St. NW Suite 557 | Washington, DC 20005 | rightsanddissent.org | info@rightsanddissent.org

August 27, 2021

U.S. Department of Justice
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

To Whom It May Concern:

This letter constitutes a request under the Freedom of Information Act, 5 U.S.C. § 552, et. seq and is submitted on behalf of Defending Rights & Dissent.

Background

On July 27, 2021, US Air Force Veteran Daniel Hale was sentenced to 45 months in prison under the Espionage Act.¹ Hale had given classified documents to a journalist who in turn published a series of stories about them with an online news publication. While neither the journalist nor the publication were named in the indictment the details described led observers to conclude journalist Jeremy Scahill and The Intercept were being referenced. During the sentencing hearing, Judge Liam O’Grady explicitly mentioned Jeremy Scahill and The Intercept by name, affirming what was already known given the facts laid out in court filings.

In August 2014, Daniel Hale’s home was raided by the Federal Bureau of Investigation as part of an Espionage Act investigation. This investigation, per later Department of Justice press releases, was led by the FBI’s Baltimore Field Office.² In spite of this raid, no

¹ See Department of Justice Office of Public Affairs, “Former Intelligence Analyst Sentenced to 45 Months in Prison for Disclosing Classified Information to Reporter” (July 27, 2021). Available at <https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information>

² See Department of Justice Office of Public Affairs, “Former Intelligence Analyst Sentenced to 45 Months in Prison for Disclosing Classified Information to Reporter” (July 27, 2021). Available at

further public actions were taken by the government until May 2019, when the Department of Justice revealed a sealed indictment (dated March 2019).³

The reasons for the five year delay between the initial raid and an indictment is unknown. It is unclear if a decision was made not to charge Hale after the raid and that decision was later reversed, but a sentencing memo filed by Hale's defense at trial would indicate that was the case

According to the indictment,⁴ Hale, while working as a Leidos contractor with the National Geospatial Intelligence Agency, printed five or six classified documents on February 28, 2014. Per the indictment, Hale then printed other documents in April, May, June, and August of 2014.

Per the government's indictment, the documents were published by a news outlet (unnamed in the indictment, but now known to be *The Intercept*) in July 2014, August 2014, April 2015, October 2015, December 2015, and December 2016.⁵ Hale's case has been closely associated with "The Drone Papers," a series of exposes about the US's targeted killing program published by *The Intercept* in October 2015. However, the earliest date of publication corresponds to a piece in *The Intercept* about the terror watchlist guidelines (one amicus brief filed in support of Hale at sentencing asserted that Hale had disclosed the nonclassified terror watchlist guidelines).

In addition to information after Hale's decision to print classified documents, the indictment contains information, including contents of correspondence, long predating Hale's printing of classified documents. It references searches Hale made on an NSA computer nearly one year before he is alleged to have leaked documents as an NGA contractor. It also references the contents of communications to or about a journalist (not named, but now known to be Jeremy Scahill). The earliest contents of a communication about the journalist excerpted in the indictment are from May 2013. The earliest content of a communication with the journalist is June 9, 2013. According to the same indictment, Hale did not begin printing classified documents not relevant to his work until February 2014.

<https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information>

³ See Department of Justice Office of Public Affairs, "Former Intelligence Analyst Charged with Disclosing Classified Information" (May 9, 2019). Available at <https://www.justice.gov/opa/pr/former-intelligence-analyst-charged-disclosing-classified-information>

⁴ A copy of the indictment has been included as an appendix.

⁵ This dates of publication are based off of a table on page 9 of the indictment. A copy of the indictment has been included as an appendix.

Request

We are requesting U.S. Department of Justice National Security Division records created from 2012 to 2021 that mentions or references⁶

- Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.
- Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016
- The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.
- "The Drone Papers" an October 2015 series of articles published by *The Intercept*
- *The Assassination Complex Inside the Government's Secret Drone Warfare Program*, a book published in 2017 based on aforementioned series of articles "The Drone Papers"

Request for Fee Waiver

Defending Rights & Dissent is a 501c3 nonprofit that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. Defending Rights & Dissent is a representative of the news media. The information requested is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government. Defending Rights & Dissent is entitled to a fee waiver.

Defending Rights & Dissent is the publisher of

- the Dissent NewsWire, an online publication that publishes original reporting about news pertaining to civil liberties,
- Reports, books, and other printed publications, including a 48 page report entitled *Still Spying on Dissent: The Enduring Problem of FBI First Amendment Abuse*,

⁶ In a March 17, 2016 opinion a United States District Court for the District of Columbia Judge found requests for records "mentioning" or "referencing" a subject met FOIA's reasonable-description requirement. *See Shapiro v. CIA, No. 14-00019, 2016 WL 1069646 (D.D.C. Mar. 17, 2016) (Cooper, J.)*

- Audio and visual broadcasts, including *Still Spying*, a limited audio series about the history of the FBI and *Primary Sources*, an ongoing limited audio series about issues faced by national security whistleblowers and journalists.

Each of these items involves the gathering of information of potential interest to a segment of the public. Once that information is gathered, through the editorial skills of our staff the raw materials are transformed into distinct works, which we continue to distribute to audiences.

Defending Rights & Dissent has received an award from Project Censored for its original reporting and is a member of The Media Consortium.⁷ In the past, Defending Rights & Dissent has produced original works based on information it has received through Freedom of Information Act requests, state level public records requests, or other similar requests.⁸ Defending Rights & Dissent has engaged in extensive first hand reporting of the arrests and prosecutions of the Trump Inauguration protesters.⁹

⁷ See “Why Is the FBI Harassing Activists in Cascadia?” *Defending Rights & Dissent*, January 5, 2015. Available at <https://rightsanddissent.org/news/why-is-the-fbi-harassing-activists-in-cascadia/>

Member Directory, *The Media Consortium*. Available at <https://www.themediaconsortium.org/member-directory>

⁸ See “DRAD, DC NLG FOIA Request Uncovers That DC Police Spent Over \$300,000 in Weapons, Ammunition to Use against Inauguration Day Protesters,” *Defending Rights & Dissent*, October 30, 2017. Available at <https://rightsanddissent.org/news/drad-dg-nlg-foia-request-uncovers-dc-police-spent-300000-weapons-ammunition-use-inauguration-day-protesters/>

“Who is Robert Wells and Why Did The FBI Consider Him A National Security Threat?” *Defending Rights & Dissent*, June 3, 2016. Available at <https://rightsanddissent.org/news/who-is-robert-wells-and-why-did-the-fbi-consider-him-a-national-security-threat/>

“Senate Passes Bill Aimed at Silencing Pro-Palestinian Activism on Campuses,” *Defending Rights & Dissent*, December 6, 2016. Available at <https://rightsanddissent.org/news/senate-passes-bill-aimed-silencing-pro-palestinian-speech-campuses/>

⁹ See Archive of J20 Articles, *Defending Rights & Dissent*. Available at <https://rightsanddissent.org/news/topics/free-speech-assembly/j20/>

In the past, Defending Rights & Dissent when filing FOIA requests has repeatedly been designated an educational institution, noncommercial scientific institution or representative of the news media requester.¹⁰

The requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government. Press freedom is a cornerstone of US democracy. When journalists publish classified information, how the government chooses to react has serious implications for press freedom. Concerns about so-called “leak investigations,” especially when they involve monitoring the communications of journalists, have aroused significant controversy within the media, complaints from press freedom groups, and concerns by members of Congress. The requested information pertains to a leak investigation in which the contents of communications between a journalist and source found their way into a criminal indictment. The length of time between the commencement of the investigation and a formal indictment have raised questions. That the long awaited indictment coincided with a change of administrations has led to speculation that a decision was made not to indict the leaker under one administration that was reversed for political purposes by a subsequent administration.

Rep. Ilhan Omar has publicly called for Daniel Hale to be pardoned for his role in the release of the Drone Papers, illustrating the public interest in this manner.

How the DOJ prosecutes, FBI investigates, and agencies like the NSA and NGA respond to the printing of classified information by a journalist is information that is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government.

Conclusion

In the event that we are denied a fee waiver, we are willing to pay up to \$50 in costs for the reproduction of the records requested. Should the cost exceed \$50 we ask to be contacted. Should any part of this request be withheld in whole or in part, we ask that specific statutory exemptions to disclosure be cited. Any part of this request is segregable.

¹⁰ “Lawmaker wants pardon for Daniel Hale, who leaked drone secrets,” *Washington Post* (August 26, 2021). Available at https://www.washingtonpost.com/local/legal-issues/daniel-hale-pardon-letter/2021/08/26/89ad149e-05c8-11ec-a266-7c7fe02fa374_story.html

We would prefer the records requested in electronic copy. Given precautions to halt the spread of the Coronavirus, Defending Rights & Dissent staff are currently not regularly in the office. Given the global pandemic, if possible we would prefer all records and communications should be sent electronically to Chip@RightsAndDissent.org. If for some reason records must be sent by mail please mail them to:

Charles Gibbons
Policy Director
Defending Rights & Dissent
1325 G St. NW Suite 557
Washington, DC 20005

Sincerely,

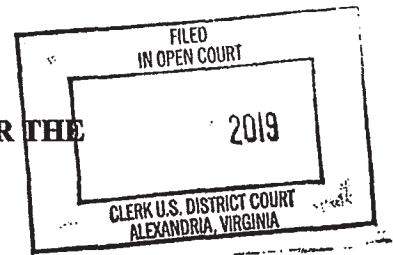
Charles Gibbons
Policy Director
Defending Rights & Dissent

Appendix

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

DANIEL EVERETTE HALE,

Defendant.

Criminal No. 1:19-CR-59

Count 1: 18 U.S.C. § 793(c)
Obtaining National Defense
Information

Count 2: 18 U.S.C. § 793(e)
Retention and Transmission
of National Defense Information

Count 3: 18 U.S.C. § 793(e)
Causing the Communication of
National Defense Information

Count 4: 18 U.S.C. § 798(a)(3)
Disclosure of Classified
Communications Intelligence
Information

Count 5: 18 U.S.C. § 641
Theft of Government Property

INDICTMENT

March 2019 Term – At Alexandria

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

A. The Defendant and His Access to Classified National Defense Information

1. Defendant DANIEL EVERETTE HALE, age 31, is a resident of Nashville, Tennessee.
2. From July 2009 through in or about July 2013, HALE was enlisted in the United States Air Force, where after receiving language and intelligence training, he became a Language

Analyst. While serving on active duty, HALE was assigned to work at the National Security Agency (NSA) from December 2011 to May 2013. HALE deployed in support of a Department of Defense Joint Special Operations Task Force from March 2012 to August 2012, at Bagram Airfield, Afghanistan, working for most of that time as an Intelligence Analyst responsible for identifying, tracking, and targeting threat networks and targets. In connection with his active duty service and work for NSA, HALE held a TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION (TS//SCI) security clearance, and had access to classified national defense information.

3. From December 2013 until August 2014, HALE was employed by a defense contractor known as Leidos. While working for Leidos, HALE was assigned to the National Geospatial-Intelligence Agency (NGA), in Springfield, Virginia, where he worked as a Political Geography Analyst. HALE was required to receive and maintain a TOP SECRET//SCI security clearance in order to work at NGA.

4. Over his many years holding a security clearance, HALE received training regarding classified information, including the definitions of classified information, the levels of classification, and SCI, as well as the proper handling, marking, transportation, and storage of classified materials. HALE received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage requirements. HALE knew that unauthorized removal and retention of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could cause injury to the United States or be used to the advantage of a foreign nation. In particular, HALE had been advised that the unauthorized disclosure of TOP SECRET information reasonably could be expected to cause exceptionally

grave damage to the national security of the United States, and unauthorized disclosure of SECRET information reasonably could be expected to cause serious damage to the national security of the United States, and that violation of the rules governing the handling of classified information could result in criminal prosecution.

5. HALE's work at NGA required the use of classified government computer systems and networks that provided access to classified national defense information. HALE was notified that these computers were monitored for "personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations" by a banner that HALE had to acknowledge by clicking on the "OK" button every time he logged on to his computer.

6. Because HALE held a security clearance and was assigned to NGA as a cleared defense contractor, the United States government entrusted HALE with access to closely held classified national defense information.

B. Background on Classified Information

7. Classified information is defined by Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010) as information in any form that (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one of more of the categories of information set forth in the order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security that the original classification authority can identify and describe.

8. Under Executive Order 13526, the designation SECRET (S) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. The designation TOP SECRET (TS) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause

exceptionally grave damage to national security. NOFORN stands for “No Foreign Dissemination” and denotes that dissemination of that information is limited to United States persons. ORCON stands for “Originator Controlled,” which denotes that the information should not be further disseminated to any third party without the concurrence of the original classification authority.

9. Executive Order No. 13526 also provides that specified officials may create special access programs upon a finding that the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access applicable to information classified at the same level are not sufficient to protect the information from unauthorized disclosure. Special access programs pertaining to intelligence sources, methods, or analytical processes are called SCI programs. One such SCI control system is SI information, which refers to “Special Intelligence.” SI protects information relating to technical and intelligence information derived from the monitoring of foreign communication signals by someone other than the intended recipients. The term COMINT describes communications intelligence.

10. Pursuant to Executive Order No. 13526, classified information can generally only be disclosed to those persons who have been granted an appropriate level United States government security clearance and who possess a valid need to know to perform a lawful and authorized government function. Additionally, classified information only may be processed and retained in and on facilities approved for processing and storage at the appropriate classification level. Classified information may not be removed from official premises without proper authorization.

C. HALE's Communications with an Online News Outlet

11. In April 2013, HALE used his unclassified NSA work computer to search the internet for information on a reporter (the Reporter). Among the results of his search was information pertaining to a scheduled appearance of the Reporter on or about April 29, 2013 at a Washington, D.C. restaurant/bookstore (Bookstore).

12. On or about April 29, 2013, HALE attended a book tour event at the Bookstore, where he met with the Reporter. The next day, on or about April 30, 2013, HALE used his TOP SECRET NSA computer to search for classified information concerning individuals and issues about which the Reporter wrote.

13. In May 2013, HALE sent a text to a close friend and confidant (Confidant) stating “[the Reporter] wants me to tell my story about working with drones at the opening screening of his documentary about the war and the use of drones.”

14. On or about June 8, 2013, HALE sat next to the Reporter at a public event at the Bookstore to promote the Reporter's book (Book 1). After the event, HALE texted a friend that he was then with the Reporter and headed to a restaurant.

15. On or about June 9, 2013, the Reporter sent HALE an email with a link to an article about Edward Snowden in an online publication. That same day, Hale texted a friend that the previous night he had been hanging out with journalists who were focused on his story. Hale wrote that the evening's events might provide him with “life long connections with people who publish work like this.”

16. On or about July 14, 2013, HALE called the Reporter. Three days later, the Reporter sent HALE an email with the subject line, “did you try calling me?” The body of the email consisted of “I'm around.” A few hours later, HALE called the Reporter again.

17. On or about July 19, 2013, HALE sent a text message to the Confidant stating that he was going to New York to meet with the Reporter and two other journalists. The next day, the same day HALE separated from the Air Force, HALE sent an email to the Reporter stating he would take a train to New York City the following week. HALE told the Reporter he would text him when he arrived so they could determine where to meet. Later the same day, HALE emailed the Reporter about watching a “plug” about the Reporter’s book on television. Attached to the email was a link to a news article entitled, “Court rules journalists can’t keep their sources secret,” about the Fourth Circuit Court of Appeals ruling that a “New York Times journalist . . . must testify in the trial of a former Central Intelligence Agency officer accused of leaking classified national defense information to the media.”

18. On or about July 23 and 24, 2013, HALE was in New York City.

19. On or about July 25, 2013, HALE sent the Reporter an email with a copy of his resume attached and subject line, “Hale – unclass resume.” The resume stated that HALE was looking for positions “within the Intelligence Community . . . [and was] [e]specially interested in Counter Terrorism, Counter Intelligence, Electronic Warfare, or stand up and maintenance of SIGINT oriented missions.” HALE listed his “Active TS/SCI clearance & counter intelligence (CI) polygraph” and “4 years active duty Air Force” where he “[p]rocessed numerous documents critical to National Defense.” As part of his duties as an Intelligence Analyst, HALE highlighted his experience operating “payloads on remotely piloted vehicles (RPV) used to support real-time kill/capture operations – over 1540 hours, over 200 specific mission” and his experience as a “[b]ack-up Intelligence De-confliction Officer for Operation Enduring Freedom’s (OEF) intelligence, surveillance and reconnaissance (ISR) platforms – 80 hours, monitored 750 on-

going missions.” Finally, HALE listed his experience working with original classification authorities to declassify information to be used against detainees in trial.

20. On or about August 18, 2013, the Reporter called HALE. The call lasted approximately 35 minutes.

21. On or about September 20, 2013, the Reporter asked HALE to “[j]ust set up a [Jabber] account [so] we can chat on encrypted.” Jabber is a free instant messaging program that uses encryption to protect the content of the messages.

22. In November 2013, HALE texted the Reporter to ask whether he would “be in D.C. this weekend for the anti drone summit.”

23. Between in and about September 20, 2013, and February 27, 2014, HALE and the Reporter had at least three encrypted conversations via Jabber.

D. HALE Prints Multiple Classified Documents Unrelated to His Assigned Work at NGA That Are Published by the Reporter’s News Outlet

24. On or about February 27, 2014, HALE sent a text message to the Reporter asking, “Are you able to get on chat?”

25. On or about February 28, 2014, HALE used a classified work computer assigned to him by NGA to print five documents marked as SECRET and one document marked as TOP SECRET, which were unrelated to his work at NGA.

26. Approximately four hours after printing the six documents, HALE and the Reporter had the following conversation via text message:

HALE: Can you be here Monday?

The Reporter: Where?

The Reporter: I am out in LA for oscars. Back Tuesday.

HALE: Right, I understand, do you have time to stop by DC?

The Reporter: Let me see if I can change flight.

HALE: Please do and lemme know.

27. Each of the six classified documents that HALE printed on February 28, 2014, was later published by the Reporter's Online News Outlet.

28. HALE continued to print documents from his TOP SECRET computer unrelated to his work as an NGA contractor that were later published by the Reporter's Online News Outlet.

29. While employed as a cleared defense contractor for NGA, HALE printed from his TOP SECRET computer 36 documents, including four duplicates. Nine documents related to HALE's work at NGA, but 23 did not.

30. Of the 23 documents unrelated to his work that he printed at NGA, HALE provided at least 17 to the Reporter and/or the Reporter's Online News Outlet, which published the documents in whole or in part.

31. Eleven of the published documents were marked as SECRET or TOP SECRET (the Classified Documents). Relevant original classification authorities have since determined that the documents were correctly marked at the appropriate classification level at the time they were printed, and that they remain classified at the same level today.

32. The table displayed on the next page lists the 23 printed documents, unrelated to HALE's work at NGA, with the print job numbers assigned by NGA, the dates of printing, initial publication dates, and classifications:

Document	NGA Print Job#	Date Printed	Date of Initial Publication	Classification
A	10&11	February 28, 2014	October 2015	SECRET
B	12	February 28, 2014	October 2015	SECRET
C	13	February 28, 2014	October 2015	SECRET
D	14&15	February 28, 2014	October 2015	SECRET
E	16	February 28, 2014	October 2015	TOP SECRET
F	17	February 28, 2014	October 2015	SECRET
G	18	April 3, 2014	April 2015	TOP SECRET
H	19	April 19, 2014	N/A	TOP SECRET
I	20	April 20, 2014	August 2014	SECRET
J	21	April 20, 2014	December 2015	SECRET
K	22	April 20, 2014	April 2015	TOP SECRET
L	23&24	April 30, 2014	July 2014	UNCLASSIFIED
M	25	May 14, 2014	August 2014	SECRET
N	26	May 14, 2014	August 2014	UNCLASSIFIED
O	27	May 15, 2014	December 2016	UNCLASSIFIED
P	28	May 15, 2014	December 2016	UNCLASSIFIED
Q	29	May 15, 2014	December 2016	UNCLASSIFIED
R	30	May 15, 2014	December 2016	UNCLASSIFIED
S	31	June 20, 2014	N/A	SECRET
T	32	June 27, 2014	N/A	UNCLASSIFIED
U	33	July 31, 2014	N/A	SECRET
V	34	August 5, 2014	N/A	SECRET
W	35&36	August 5, 2014	N/A	UNCLASSIFIED

33. The 11 Classified Documents that were published by the Reporter's Online News

Outlet, and later in a book authored by the Reporter, are described in further detail below:

- DOCUMENT A – A PowerPoint presentation on counterterrorism operations classified SECRET//SCI
- DOCUMENT B – A document describing a military campaign targeting Al-Qaeda overseas classified SECRET
- DOCUMENT C - A March 2013 PowerPoint on military operations classified SECRET
- DOCUMENT D – A PowerPoint presentation on counterterrorism operations classified SECRET

- DOCUMENT E – Information gathered by NSA on specific named targets classified TOP SECRET
- DOCUMENT F – A PowerPoint slide outlining the effects of the military campaign targeting Al-Qaeda overseas classified SECRET
- DOCUMENT G – PowerPoint presentation outlining U.S. military technical capabilities classified TOP SECRET
- DOCUMENT I – A report listing the accomplishments of an intelligence agency tasked with preventing terrorist attacks classified SECRET
- DOCUMENT J – A PowerPoint presentation classified SECRET
- DOCUMENT K – An intelligence report on an Al-Qaeda operative classified TOP SECRET
- DOCUMENT M – Information on the Terrorist Identities Datamart Environment classified SECRET

34. HALE did not have a “need to know” the classified information contained in the 11 Classified Documents he printed.

35. All of the Classified Documents HALE printed bore standard markings indicating they contained highly classified information of the United States, including SECRET, and TOP SECRET, as well as SCI, information.

36. At the time HALE obtained the documents, he knew that they had been or would be obtained, taken, made, or disposed of unlawfully.

37. HALE was never authorized to remove the Classified Documents from NGA and retain or transmit them, and neither the Reporter nor any of the employees at the Reporter’s Online News Outlet were entitled to receive or possess them.

38. The documents provided to the Reporter by HALE and published by the Reporter's Online News Outlet were compiled and published in a book authored by the Reporter (Book 2).

E. Evidence Stored in HALE's Home

39. On August 8, 2014, HALE possessed Document T on his home computer. HALE also possessed two thumb drives. The first thumb drive contained one page of Document A that HALE had attempted to delete. This page was marked "SECRET." The second thumb drive contained the "Tor" software and "Tails" operating system.

40. Tor and Tails were recommended by the Reporter's Online News Outlet in an article published on the Reporter's Online News Outlet's website, which provided readers with instructions on how to anonymously "leak" documents to the Reporter's Online News Outlet. The article published by the Reporter's Online News Outlet explained that the Tor browser allows users to anonymously surf the web by "hiding your real IP address from the websites that you visit. If your network is being monitored, the eavesdroppers will only know that you are using Tor but not what you're doing." The article went on to explain that the Tails operating system, which can be installed via a USB stick, will prevent someone who has hacked into your computer from "spy[ing] on everything you do." It "strip[s] metadata from a variety of types of documents...[and] leaves no traces that it was ever run on your computer."

41. On or about August 8, 2014, HALE's cell phone contact list included the contact information for the Reporter.

COUNT 1
(18 U.S.C. § 793(c)—Obtaining National Defense Information)

THE GRAND JURY FURTHER CHARGES THAT:

42. The General Allegations within Paragraph 1 through 41 of this Indictment are re-alleged and incorporated by reference.

43. Beginning on or about February 28, 2014, and continuing to on or about May 14, 2014, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, for the purpose of obtaining information respecting the national defense, unlawfully obtained documents connected with the national defense, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

knowing and having reason to believe at the time he obtained Documents A-G, I-K, and M that they had been or would be obtained, taken, made, or disposed of by any person contrary to the provisions of Title 18, United States Code, Chapter 37.

(In violation of Title 18, United States Code, Section 793(c).)

COUNT 2**(18 U.S.C. § 793(e)—Retention and Transmission of National Defense Information)****THE GRAND JURY FURTHER CHARGES THAT:**

44. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

45. Beginning on or about February 28, 2014, and continuing to on or about December 17, 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, having unauthorized possession of, access to, and control over the following documents related to the national defense, willfully: (a) retained the documents and failed to deliver them to the officer or employee of the United States entitled to receive them; and (b) communicated, delivered, and transmitted such documents to a person not entitled to receive them. Specifically, HALE retained the following documents relating to the national defense, and transmitted them to the Reporter and/or the Reporter's Online News Outlet:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

(In violation of Title 18, United States Code, Section 793(e).)

COUNT 3**(18 U.S.C. § 793(e)—Causing the Communication of National Defense Information)****THE GRAND JURY FURTHER CHARGES THAT:**

46. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

47. Beginning on or about February 28, 2014, and continuing to on or about December 17, 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, having unauthorized possession of, access to, and control over documents related to the national defense of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

did willfully communicate, deliver, transmit and cause to be communicated, delivered, and transmitted, and attempt to communicate, deliver and transmit and cause to be communicated, delivered, and transmitted the same to persons not entitled to receive them, through the publication, dissemination, and distribution to the general public of articles and books concerning Classified Documents A-G, I-K, and M.

(In violation of Title 18, United States Code, Section 793(e).)

COUNT 4**(18 U.S.C. § 798(a)(3)—Disclosure of Classified Communication Intelligence Information)****THE GRAND JURY FURTHER CHARGES THAT:**

48. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

49. Beginning on or about February 28, 2014, and continuing to in or about October 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, did willfully communicate, furnish, transmit, and otherwise make available to an unauthorized person any classified information concerning the communication intelligence activities of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
K	February 28, 2014	April 2015	TOP SECRET

(In violation of Title 18, United States Code, Sections 798(a)(3).)

COUNT 5
(18 U.S.C. § 641—Theft of Government Property)

THE GRAND JURY FURTHER CHARGES THAT:

50. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

51. Between on or about February 28, 2014, and continuing to in or about December 2016, in the Eastern District of Virginia, and elsewhere, the defendant, DANIEL EVERETTE HALE, did knowingly and unlawfully steal and convert to his own use or the use of another, and without authority, conveyed and disposed of records and things of value of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
L	April 30, 2014	July 2014	UNCLASSIFIED
M	May 14, 2014	August 2014	SECRET
N	May 14, 2014	August 2014	UNCLASSIFIED
O	May 15, 2014	December 2016	UNCLASSIFIED
P	May 15, 2014	December 2016	UNCLASSIFIED
Q	May 15, 2014	December 2016	UNCLASSIFIED
R	May 15, 2014	December 2016	UNCLASSIFIED
T	June 27, 2014	N/A	UNCLASSIFIED

The aggregate value of said records and things of value being more than \$1,000.

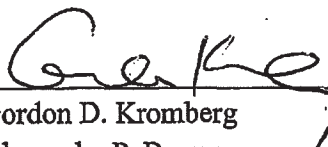
(All in violation of Title 18, United States Code, Section 641.)

A TRUE BILL:

UNDER SEAL
FOREPERSON OF THE GRAND JURY

G. Zachary Terwilliger
United States Attorney
Eastern District of Virginia

John C. Demers
Assistant Attorney General
National Security Division
U.S. Department of Justice



Gordon D. Kromberg
Alexander P. Berrang
Assistant United States Attorneys

Heather M. Schmidt
Senior Trial Attorney
Counterintelligence-Export Control Section
National Security Division
U.S. Department of Justice

Chip Gibbons <chip@bordc.org>

NSD FOIA #21-359

Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov>
To: "chip@rightsanddissent.org" <chip@rightsanddissent.org>

Mon, Oct 18, 2021 at 11:05 AM

Chip Gibbons

Defending Rights & Dissent

chip@rightsanddissent.org

Re: FOIA/PA #21-359

Dear Mr. Gibbons:

This is to acknowledge your email dated August 27, 2021 for information pertaining to records from 2012 to 2021 that mentions or reference Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014. Leak investigations resulting from the Intercept publishing classified information about the US drone program between April 2015 and December 2016. Our FOIA office received your Freedom of Information Act request on August 27, 2021.

In response to the COVID-19 public health emergency, the NSD FOIA staff is teleworking full time. Our FOIA operations have been diminished while we are teleworking and our FOIA intake and FOIA processing will be slower than normal.

Our policy is to process FOIA requests on a first-in, first-out basis. Consistent with this policy, every effort will be made to respond to your request as quickly as possible. The actual processing time will depend upon the complexity of the request, whether it involves sensitive or voluminous records, and whether consultations with other agencies or agency components are appropriate.

You may contact our Government Information Specialist, Arnetta Mallory, for any further assistance and to discuss any aspect of your request at:

U.S. Department of Justice

Records and FOIA Unit

3 Constitution Square

[175 N Street N.E. 12th Floor](#)

(202) 233-2639

Sincerely,

Arnetta Mallory

Government Information Specialist

Fwd: NSD FOIA #21-359

----- Forwarded message -----

From: **Mallory, Arnetta (NSD)** <Arnetta.Mallory@usdoj.gov>

Date: Fri, Jan 14, 2022 at 1:05 PM

Subject: NSD FOIA #21-359

To: Chip Gibbons <chip@rightsanddissent.org>

Dear Mr. Gibbons,

The National Security Division is still searching for possible responsive documents to your request. Once our search is complete, we will let you know the results.

Sincerely,

Arnetta Mallory

From: Chip Gibbons <chip@rightsanddissent.org>
Sent: Thursday, January 13, 2022 2:02 PM
To: Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov>
Subject: [EXTERNAL] Re: NSD FOIA #21-359

Pursuant to 5 U.S.C. § 552(a)(7)(B)(ii), I request an estimated date of completion for NSD FOIA #21-359.

Thank you,

On Mon, Oct 18, 2021 at 11:05 AM Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov> wrote:

Chip Gibbons

Defending Rights & Dissent

chip@rightsanddissent.org

Re: FOIA/PA #21-359

Dear Mr. Gibbons:

This is to acknowledge your email dated August 27, 2021 for information pertaining to records from 2012 to 2021 that mentions or reference Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014. Leak investigations resulting from the Intercept publishing classified information about the US drone program between April 2015 and December 2016. Our FOIA office received your Freedom of Information Act request on August 27, 2021.

In response to the COVID-19 public health emergency, the NSD FOIA staff is teleworking full time. Our FOIA operations have been diminished while we are teleworking and our FOIA intake and FOIA processing will be slower than normal.

Our policy is to process FOIA requests on a first-in, first-out basis. Consistent with this policy, every effort will be made to respond to your request as quickly as possible. The actual processing time will depend upon the complexity of the request, whether it involves sensitive or voluminous records, and whether consultations with other agencies or agency components are appropriate.

You may contact our Government Information Specialist, Arnetta Mallory, for any further assistance and to discuss any aspect of your request at:

U.S. Department of Justice
Records and FOIA Unit
3 Constitution Square
[175 N Street N.E. 12th Floor](#)
[Washington, DC 20530](#)
(202) 233-2639

Sincerely,

Arnetta Mallory
Government Information Specialist

Fwd: NSD FOIA #21-359

----- Forwarded message -----

From: **Chip Gibbons** <chip@rightsanddissent.org>
Date: Tue, Feb 22, 2022 at 1:47 PM
Subject: Re: NSD FOIA #21-359
To: Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov>

When do you estimate that you will be done with the search?

On Fri, Jan 14, 2022 at 1:05 PM Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov> wrote:

Dear Mr. Gibbons,

The National Security Division is still searching for possible responsive documents to you request. Once our search is complete, we will let you know the results.

Sincerely,

Arnetta Mallory

From: Chip Gibbons <chip@rightsanddissent.org>
Sent: Thursday, January 13, 2022 2:02 PM
To: Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov>
Subject: [EXTERNAL] Re: NSD FOIA #21-359

Pursuant to 5 U.S.C. § 552(a)(7)(B)(ii), I request an estimated date of completion for NSD FOIA #21-359.

Thank you,

On Mon, Oct 18, 2021 at 11:05 AM Mallory, Arnetta (NSD) <Arnetta.Mallory@usdoj.gov> wrote:

Chip Gibbons
Defending Rights & Dissent
chip@rightsanddissent.org



DEFENDING RIGHTS & DISSENT

Formerly Bill of Rights Defense Committee/ Defending Dissent Foundation

1325 G St. NW Suite 557 | Washington, DC 20005 | rightsanddissent.org | info@rightsanddissent.org

August 27, 2021

National Security Agency
9800 Savage Rd. Suite 6272
Ft. George G. Meade MD 20755-6000

To Whom It May Concern:

This letter constitutes a request under the Freedom of Information Act, 5 U.S.C. § 552, et. seq and is submitted on behalf of Defending Rights & Dissent.

Background

On July 27, 2021, US Air Force Veteran Daniel Hale was sentenced to 45 months in prison under the Espionage Act.¹ Hale had given classified documents to a journalist who in turn published a series of stories about them with an online news publication. While neither the journalist nor the publication were named in the indictment the details described led observers to conclude journalist Jeremy Scahill and The Intercept were being referenced. During the sentencing hearing, Judge Liam O’Grady explicitly mentioned Jeremy Scahill and The Intercept by name, affirming what was already known given the facts laid out in court filings.

In August 2014, Daniel Hale’s home was raided by the Federal Bureau of Investigation as part of an Espionage Act investigation. This investigation, per later Department of Justice press releases, was led by the FBI’s Baltimore Field Office.² In spite of this raid, no

¹ See Department of Justice Office of Public Affairs, “Former Intelligence Analyst Sentenced to 45 Months in Prison for Disclosing Classified Information to Reporter” (July 27, 2021). Available at <https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information>

² See Department of Justice Office of Public Affairs, “Former Intelligence Analyst Sentenced to 45 Months in Prison for Disclosing Classified Information to Reporter” (July 27, 2021). Available at <https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information>

further public actions were taken by the government until May 2019, when the Department of Justice revealed a sealed indictment (dated March 2019).³

The reasons for the five year delay between the initial raid and an indictment is unknown. It is unclear if a decision was made not to charge Hale after the raid and that decision was later reversed, but a sentencing memo filed by Hale's defense at trial would indicate that was the case

According to the indictment,⁴ Hale, while working as a Leidos contractor with the National Geospatial Intelligence Agency, printed five or six classified documents on February 28, 2014. Per the indictment, Hale then printed other documents in April, May, June, and August of 2014.

Per the government's indictment, the documents were published by a news outlet (unnamed in the indictment, but now known to be *The Intercept*) in July 2014, August 2014, April 2015, October 2015, December 2015, and December 2016.⁵ Hale's case has been closely associated with "The Drone Papers," a series of exposes about the US's targeted killing program published by *The Intercept* in October 2015. However, the earliest date of publication corresponds to a piece in *The Intercept* about the terror watchlist guidelines (one amicus brief filed in support of Hale at sentencing asserted that Hale had disclosed the nonclassified terror watchlist guidelines).

In addition to information after Hale's decision to print classified documents, the indictment contains information, including contents of correspondence, long predating Hale's printing of classified documents. It references searches Hale made on an NSA computer nearly one year before he is alleged to have leaked documents as an NGA contractor. It also references the contents of communications to or about a journalist (not named, but now known to be Jeremy Scahill). The earliest contents of a communication about the journalist excerpted in the indictment are from May 2013. The earliest content of a communication with the journalist is June 9, 2013. According to the same indictment, Hale did not begin printing classified documents not relevant to his work until February 2014.

Request

³ See Department of Justice Office of Public Affairs, "Former Intelligence Analyst Charged with Disclosing Classified Information" (May 9, 2019). Available at <https://www.justice.gov/opa/pr/former-intelligence-analyst-charged-disclosing-classified-information>

⁴ A copy of the indictment has been included as an appendix.

⁵ This dates of publication are based off of a table on page 9 of the indictment. A copy of the indictment has been included as an appendix.

We are requesting National Security Agency records created from 2012 to 2021 that mentions or references⁶

- Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.
- Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016
- The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.
- "The Drone Papers" an October 2015 series of articles published by *The Intercept*
- *The Assassination Complex Inside the Government's Secret Drone Warfare Program*, a book published in 2017 based on aforementioned series of articles "The Drone Papers"

Request for Fee Waiver

Defending Rights & Dissent is a 501c3 nonprofit that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. Defending Rights & Dissent is a representative of the news media. The information requested is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government. Defending Rights & Dissent is entitled to a fee waiver.

Defending Rights & Dissent is the publisher of

- the Dissent NewsWire, an online publication that publishes original reporting about news pertaining to civil liberties,
- Reports, books, and other printed publications, including a 48 page report entitled *Still Spying on Dissent: The Enduring Problem of FBI First Amendment Abuse*,
- Audio and visual broadcasts, including *Still Spying*, a limited audio series about the history of the FBI and *Primary Sources*, an ongoing limited audio series about issues faced by national security whistleblowers and journalists.

⁶ In a March 17, 2016 opinion a United States District Court for the District of Columbia Judge found requests for records "mentioning" or "referencing" a subject met FOIA's reasonable-description requirement. *See Shapiro v. CIA, No. 14-00019, 2016 WL 1069646 (D.D.C. Mar. 17, 2016) (Cooper, J.)*

Each of these items involves the gathering of information of potential interest to a segment of the public. Once that information is gathered, through the editorial skills of our staff the raw materials are transformed into distinct works, which we continue to distribute to audiences.

Defending Rights & Dissent has received an award from Project Censored for its original reporting and is a member of The Media Consortium.⁷ In the past, Defending Rights & Dissent has produced original works based on information it has received through Freedom of Information Act requests, state level public records requests, or other similar requests.⁸ Defending Rights & Dissent has engaged in extensive first hand reporting of the arrests and prosecutions of the Trump Inauguration protesters.⁹

In the past, Defending Rights & Dissent when filing FOIA requests has repeatedly been designated an educational institution, noncommercial scientific institution or representative of the news media requester.¹⁰

⁷ See “Why Is the FBI Harassing Activists in Cascadia?” *Defending Rights & Dissent*, January 5, 2015. Available at <https://rightsanddissent.org/news/why-is-the-fbi-harassing-activists-in-cascadia/>

Member Directory, *The Media Consortium*. Available at <https://www.themediaconsortium.org/member-directory>

⁸ See “DRAD, DC NLG FOIA Request Uncovers That DC Police Spent Over \$300,000 in Weapons, Ammunition to Use against Inauguration Day Protesters,” *Defending Rights & Dissent*, October 30, 2017. Available at <https://rightsanddissent.org/news/drad-dg-nlg-foia-request-uncovers-dc-police-spent-300000-weapons-ammunition-use-inauguration-day-protesters/>

“Who is Robert Wells and Why Did The FBI Consider Him A National Security Threat?” *Defending Rights & Dissent*, June 3, 2016. Available at <https://rightsanddissent.org/news/who-is-robert-wells-and-why-did-the-fbi-consider-him-a-national-security-threat/>

“Senate Passes Bill Aimed at Silencing Pro-Palestinian Activism on Campuses,” *Defending Rights & Dissent*, December 6, 2016. Available at <https://rightsanddissent.org/news/senate-passes-bill-aimed-silencing-pro-palestinian-speech-campuses/>

⁹ See Archive of J20 Articles, *Defending Rights & Dissent*. Available at <https://rightsanddissent.org/news/topics/free-speech-assembly/j20/>

¹⁰ “Lawmaker wants pardon for Daniel Hale, who leaked drone secrets,” *Washington Post* (August 26, 2021). Available at

The requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government. Press freedom is a cornerstone of US democracy. When journalists publish classified information, how the government chooses to react has serious implications for press freedom. Concerns about so-called “leak investigations,” especially when they involve monitoring the communications of journalists, have aroused significant controversy within the media, complaints from press freedom groups, and concerns by members of Congress. The requested information pertains to a leak investigation in which the contents of communications between a journalist and source found their way into a criminal indictment. The length of time between the commencement of the investigation and a formal indictment have raised questions. That the long awaited indictment coincided with a change of administrations has led to speculation that a decision was made not to indict the leaker under one administration that was reversed for political purposes by a subsequent administration.

Rep. Ilhan Omar has publicly called for Daniel Hale to be pardoned for his role in the release of the Drone Papers, illustrating the public interest in this manner.

How the DOJ prosecutes, FBI investigates, and agencies like the NSA and NGA respond to the printing of classified information by a journalist is information that is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government.

Conclusion

In the event that we are denied a fee waiver, we are willing to pay up to \$50 in costs for the reproduction of the records requested. Should the cost exceed \$50 we ask to be contacted. Should any part of this request be withheld in whole or in part, we ask that specific statutory exemptions to disclosure be cited. Any part of this request is segregable.

We would prefer the records requested in electronic copy. Given precautions to halt the spread of the Coronavirus, Defending Rights & Dissent staff are currently not regularly in the office. Given the global pandemic, if possible we would prefer all records and communications should be sent electronically to Chip@RightsAndDissent.org. If for some reason records must be sent by mail please mail them to:

https://www.washingtonpost.com/local/legal-issues/daniel-hale-pardon-letter/2021/08/26/89ad149e-05c8-11ec-a266-7c7fe02fa374_story.html

Charles Gibbons
Policy Director
Defending Rights & Dissent
1325 G St. NW Suite 557
Washington, DC 20005

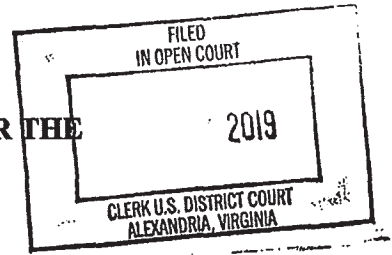
Sincerely,

Charles Gibbons
Policy Director
Defending Rights & Dissent

Appendix
UNDER SEAL

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division



UNITED STATES OF AMERICA

v.

DANIEL EVERETTE HALE,

Defendant.

Criminal No. 1:19-CR-59

Count 1: 18 U.S.C. § 793(c)
Obtaining National Defense
Information

Count 2: 18 U.S.C. § 793(e)
Retention and Transmission
of National Defense Information

Count 3: 18 U.S.C. § 793(e)
Causing the Communication of
National Defense Information

Count 4: 18 U.S.C. § 798(a)(3)
Disclosure of Classified
Communications Intelligence
Information

Count 5: 18 U.S.C. § 641
Theft of Government Property

INDICTMENT

March 2019 Term – At Alexandria

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

A. The Defendant and His Access to Classified National Defense Information

1. Defendant DANIEL EVERETTE HALE, age 31, is a resident of Nashville, Tennessee.
2. From July 2009 through in or about July 2013, HALE was enlisted in the United States Air Force, where after receiving language and intelligence training, he became a Language

Analyst. While serving on active duty, HALE was assigned to work at the National Security Agency (NSA) from December 2011 to May 2013. HALE deployed in support of a Department of Defense Joint Special Operations Task Force from March 2012 to August 2012, at Bagram Airfield, Afghanistan, working for most of that time as an Intelligence Analyst responsible for identifying, tracking, and targeting threat networks and targets. In connection with his active duty service and work for NSA, HALE held a TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION (TS//SCI) security clearance, and had access to classified national defense information.

3. From December 2013 until August 2014, HALE was employed by a defense contractor known as Leidos. While working for Leidos, HALE was assigned to the National Geospatial-Intelligence Agency (NGA), in Springfield, Virginia, where he worked as a Political Geography Analyst. HALE was required to receive and maintain a TOP SECRET//SCI security clearance in order to work at NGA.

4. Over his many years holding a security clearance, HALE received training regarding classified information, including the definitions of classified information, the levels of classification, and SCI, as well as the proper handling, marking, transportation, and storage of classified materials. HALE received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage requirements. HALE knew that unauthorized removal and retention of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could cause injury to the United States or be used to the advantage of a foreign nation. In particular, HALE had been advised that the unauthorized disclosure of TOP SECRET information reasonably could be expected to cause exceptionally

grave damage to the national security of the United States, and unauthorized disclosure of SECRET information reasonably could be expected to cause serious damage to the national security of the United States, and that violation of the rules governing the handling of classified information could result in criminal prosecution.

5. HALE's work at NGA required the use of classified government computer systems and networks that provided access to classified national defense information. HALE was notified that these computers were monitored for "personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations" by a banner that HALE had to acknowledge by clicking on the "OK" button every time he logged on to his computer.

6. Because HALE held a security clearance and was assigned to NGA as a cleared defense contractor, the United States government entrusted HALE with access to closely held classified national defense information.

B. Background on Classified Information

7. Classified information is defined by Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010) as information in any form that (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one of more of the categories of information set forth in the order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security that the original classification authority can identify and describe.

8. Under Executive Order 13526, the designation SECRET (S) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. The designation TOP SECRET (TS) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause

exceptionally grave damage to national security. NOFORN stands for “No Foreign Dissemination” and denotes that dissemination of that information is limited to United States persons. ORCON stands for “Originator Controlled,” which denotes that the information should not be further disseminated to any third party without the concurrence of the original classification authority.

9. Executive Order No. 13526 also provides that specified officials may create special access programs upon a finding that the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access applicable to information classified at the same level are not sufficient to protect the information from unauthorized disclosure. Special access programs pertaining to intelligence sources, methods, or analytical processes are called SCI programs. One such SCI control system is SI information, which refers to “Special Intelligence.” SI protects information relating to technical and intelligence information derived from the monitoring of foreign communication signals by someone other than the intended recipients. The term COMINT describes communications intelligence.

10. Pursuant to Executive Order No. 13526, classified information can generally only be disclosed to those persons who have been granted an appropriate level United States government security clearance and who possess a valid need to know to perform a lawful and authorized government function. Additionally, classified information only may be processed and retained in and on facilities approved for processing and storage at the appropriate classification level. Classified information may not be removed from official premises without proper authorization.

C. HALE's Communications with an Online News Outlet

11. In April 2013, HALE used his unclassified NSA work computer to search the internet for information on a reporter (the Reporter). Among the results of his search was information pertaining to a scheduled appearance of the Reporter on or about April 29, 2013 at a Washington, D.C. restaurant/bookstore (Bookstore).

12. On or about April 29, 2013, HALE attended a book tour event at the Bookstore, where he met with the Reporter. The next day, on or about April 30, 2013, HALE used his TOP SECRET NSA computer to search for classified information concerning individuals and issues about which the Reporter wrote.

13. In May 2013, HALE sent a text to a close friend and confidant (Confidant) stating “[the Reporter] wants me to tell my story about working with drones at the opening screening of his documentary about the war and the use of drones.”

14. On or about June 8, 2013, HALE sat next to the Reporter at a public event at the Bookstore to promote the Reporter's book (Book 1). After the event, HALE texted a friend that he was then with the Reporter and headed to a restaurant.

15. On or about June 9, 2013, the Reporter sent HALE an email with a link to an article about Edward Snowden in an online publication. That same day, Hale texted a friend that the previous night he had been hanging out with journalists who were focused on his story. Hale wrote that the evening's events might provide him with “life long connections with people who publish work like this.”

16. On or about July 14, 2013, HALE called the Reporter. Three days later, the Reporter sent HALE an email with the subject line, “did you try calling me?” The body of the email consisted of “I'm around.” A few hours later, HALE called the Reporter again.

17. On or about July 19, 2013, HALE sent a text message to the Confidant stating that he was going to New York to meet with the Reporter and two other journalists. The next day, the same day HALE separated from the Air Force, HALE sent an email to the Reporter stating he would take a train to New York City the following week. HALE told the Reporter he would text him when he arrived so they could determine where to meet. Later the same day, HALE emailed the Reporter about watching a “plug” about the Reporter’s book on television. Attached to the email was a link to a news article entitled, “Court rules journalists can’t keep their sources secret,” about the Fourth Circuit Court of Appeals ruling that a “New York Times journalist . . . must testify in the trial of a former Central Intelligence Agency officer accused of leaking classified national defense information to the media.”

18. On or about July 23 and 24, 2013, HALE was in New York City.

19. On or about July 25, 2013, HALE sent the Reporter an email with a copy of his resume attached and subject line, “Hale – unclass resume.” The resume stated that HALE was looking for positions “within the Intelligence Community . . . [and was] [e]specially interested in Counter Terrorism, Counter Intelligence, Electronic Warfare, or stand up and maintenance of SIGINT oriented missions.” HALE listed his “Active TS/SCI clearance & counter intelligence (CI) polygraph” and “4 years active duty Air Force” where he “[p]rocessed numerous documents critical to National Defense.” As part of his duties as an Intelligence Analyst, HALE highlighted his experience operating “payloads on remotely piloted vehicles (RPV) used to support real-time kill/capture operations – over 1540 hours, over 200 specific mission” and his experience as a “[b]ack-up Intelligence De-confliction Officer for Operation Enduring Freedom’s (OEF) intelligence, surveillance and reconnaissance (ISR) platforms – 80 hours, monitored 750 on-

going missions.” Finally, HALE listed his experience working with original classification authorities to declassify information to be used against detainees in trial.

20. On or about August 18, 2013, the Reporter called HALE. The call lasted approximately 35 minutes.

21. On or about September 20, 2013, the Reporter asked HALE to “[j]ust set up a [Jabber] account [so] we can chat on encrypted.” Jabber is a free instant messaging program that uses encryption to protect the content of the messages.

22. In November 2013, HALE texted the Reporter to ask whether he would “be in D.C. this weekend for the anti drone summit.”

23. Between in and about September 20, 2013, and February 27, 2014, HALE and the Reporter had at least three encrypted conversations via Jabber.

D. HALE Prints Multiple Classified Documents Unrelated to His Assigned Work at NGA That Are Published by the Reporter’s News Outlet

24. On or about February 27, 2014, HALE sent a text message to the Reporter asking, “Are you able to get on chat?”

25. On or about February 28, 2014, HALE used a classified work computer assigned to him by NGA to print five documents marked as SECRET and one document marked as TOP SECRET, which were unrelated to his work at NGA.

26. Approximately four hours after printing the six documents, HALE and the Reporter had the following conversation via text message:

HALE: Can you be here Monday?

The Reporter: Where?

The Reporter: I am out in LA for oscars. Back Tuesday.

HALE: Right, I understand, do you have time to stop by DC?

The Reporter: Let me see if I can change flight.

HALE: Please do and lemme know.

27. Each of the six classified documents that HALE printed on February 28, 2014, was later published by the Reporter's Online News Outlet.

28. HALE continued to print documents from his TOP SECRET computer unrelated to his work as an NGA contractor that were later published by the Reporter's Online News Outlet.

29. While employed as a cleared defense contractor for NGA, HALE printed from his TOP SECRET computer 36 documents, including four duplicates. Nine documents related to HALE's work at NGA, but 23 did not.

30. Of the 23 documents unrelated to his work that he printed at NGA, HALE provided at least 17 to the Reporter and/or the Reporter's Online News Outlet, which published the documents in whole or in part.

31. Eleven of the published documents were marked as SECRET or TOP SECRET (the Classified Documents). Relevant original classification authorities have since determined that the documents were correctly marked at the appropriate classification level at the time they were printed, and that they remain classified at the same level today.

32. The table displayed on the next page lists the 23 printed documents, unrelated to HALE's work at NGA, with the print job numbers assigned by NGA, the dates of printing, initial publication dates, and classifications:

Document	NGA Print Job#	Date Printed	Date of Initial Publication	Classification
A	10&11	February 28, 2014	October 2015	SECRET
B	12	February 28, 2014	October 2015	SECRET
C	13	February 28, 2014	October 2015	SECRET
D	14&15	February 28, 2014	October 2015	SECRET
E	16	February 28, 2014	October 2015	TOP SECRET
F	17	February 28, 2014	October 2015	SECRET
G	18	April 3, 2014	April 2015	TOP SECRET
H	19	April 19, 2014	N/A	TOP SECRET
I	20	April 20, 2014	August 2014	SECRET
J	21	April 20, 2014	December 2015	SECRET
K	22	April 20, 2014	April 2015	TOP SECRET
L	23&24	April 30, 2014	July 2014	UNCLASSIFIED
M	25	May 14, 2014	August 2014	SECRET
N	26	May 14, 2014	August 2014	UNCLASSIFIED
O	27	May 15, 2014	December 2016	UNCLASSIFIED
P	28	May 15, 2014	December 2016	UNCLASSIFIED
Q	29	May 15, 2014	December 2016	UNCLASSIFIED
R	30	May 15, 2014	December 2016	UNCLASSIFIED
S	31	June 20, 2014	N/A	SECRET
T	32	June 27, 2014	N/A	UNCLASSIFIED
U	33	July 31, 2014	N/A	SECRET
V	34	August 5, 2014	N/A	SECRET
W	35&36	August 5, 2014	N/A	UNCLASSIFIED

33. The 11 Classified Documents that were published by the Reporter's Online News

Outlet, and later in a book authored by the Reporter, are described in further detail below:

- DOCUMENT A – A PowerPoint presentation on counterterrorism operations classified SECRET//SCI
- DOCUMENT B – A document describing a military campaign targeting Al-Qaeda overseas classified SECRET
- DOCUMENT C - A March 2013 PowerPoint on military operations classified SECRET
- DOCUMENT D – A PowerPoint presentation on counterterrorism operations classified SECRET

- DOCUMENT E – Information gathered by NSA on specific named targets classified TOP SECRET
- DOCUMENT F – A PowerPoint slide outlining the effects of the military campaign targeting Al-Qaeda overseas classified SECRET
- DOCUMENT G – PowerPoint presentation outlining U.S. military technical capabilities classified TOP SECRET
- DOCUMENT I – A report listing the accomplishments of an intelligence agency tasked with preventing terrorist attacks classified SECRET
- DOCUMENT J – A PowerPoint presentation classified SECRET
- DOCUMENT K – An intelligence report on an Al-Qaeda operative classified TOP SECRET
- DOCUMENT M – Information on the Terrorist Identities Datamart Environment classified SECRET

34. HALE did not have a “need to know” the classified information contained in the 11 Classified Documents he printed.

35. All of the Classified Documents HALE printed bore standard markings indicating they contained highly classified information of the United States, including SECRET, and TOP SECRET, as well as SCI, information.

36. At the time HALE obtained the documents, he knew that they had been or would be obtained, taken, made, or disposed of unlawfully.

37. HALE was never authorized to remove the Classified Documents from NGA and retain or transmit them, and neither the Reporter nor any of the employees at the Reporter’s Online News Outlet were entitled to receive or possess them.

38. The documents provided to the Reporter by HALE and published by the Reporter's Online News Outlet were compiled and published in a book authored by the Reporter (Book 2).

E. Evidence Stored in HALE's Home

39. On August 8, 2014, HALE possessed Document T on his home computer. HALE also possessed two thumb drives. The first thumb drive contained one page of Document A that HALE had attempted to delete. This page was marked "SECRET." The second thumb drive contained the "Tor" software and "Tails" operating system.

40. Tor and Tails were recommended by the Reporter's Online News Outlet in an article published on the Reporter's Online News Outlet's website, which provided readers with instructions on how to anonymously "leak" documents to the Reporter's Online News Outlet. The article published by the Reporter's Online News Outlet explained that the Tor browser allows users to anonymously surf the web by "hiding your real IP address from the websites that you visit. If your network is being monitored, the eavesdroppers will only know that you are using Tor but not what you're doing." The article went on to explain that the Tails operating system, which can be installed via a USB stick, will prevent someone who has hacked into your computer from "spy[ing] on everything you do." It "strip[s] metadata from a variety of types of documents...[and] leaves no traces that it was ever run on your computer."

41. On or about August 8, 2014, HALE's cell phone contact list included the contact information for the Reporter.

COUNT 1
(18 U.S.C. § 793(c)—Obtaining National Defense Information)

THE GRAND JURY FURTHER CHARGES THAT:

42. The General Allegations within Paragraph 1 through 41 of this Indictment are re-alleged and incorporated by reference.

43. Beginning on or about February 28, 2014, and continuing to on or about May 14, 2014, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, for the purpose of obtaining information respecting the national defense, unlawfully obtained documents connected with the national defense, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

knowing and having reason to believe at the time he obtained Documents A-G, I-K, and M that they had been or would be obtained, taken, made, or disposed of by any person contrary to the provisions of Title 18, United States Code, Chapter 37.

(In violation of Title 18, United States Code, Section 793(c).)

COUNT 2**(18 U.S.C. § 793(e)—Retention and Transmission of National Defense Information)****THE GRAND JURY FURTHER CHARGES THAT:**

44. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

45. Beginning on or about February 28, 2014, and continuing to on or about December 17, 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, having unauthorized possession of, access to, and control over the following documents related to the national defense, willfully: (a) retained the documents and failed to deliver them to the officer or employee of the United States entitled to receive them; and (b) communicated, delivered, and transmitted such documents to a person not entitled to receive them. Specifically, HALE retained the following documents relating to the national defense, and transmitted them to the Reporter and/or the Reporter's Online News Outlet:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

(In violation of Title 18, United States Code, Section 793(e).)

COUNT 3**(18 U.S.C. § 793(e)—Causing the Communication of National Defense Information)****THE GRAND JURY FURTHER CHARGES THAT:**

46. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

47. Beginning on or about February 28, 2014, and continuing to on or about December 17, 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, having unauthorized possession of, access to, and control over documents related to the national defense of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
M	May 14, 2014	August 2014	SECRET

did willfully communicate, deliver, transmit and cause to be communicated, delivered, and transmitted, and attempt to communicate, deliver and transmit and cause to be communicated, delivered, and transmitted the same to persons not entitled to receive them, through the publication, dissemination, and distribution to the general public of articles and books concerning Classified Documents A-G, I-K, and M.

(In violation of Title 18, United States Code, Section 793(e).)

COUNT 4**(18 U.S.C. § 798(a)(3)—Disclosure of Classified Communication Intelligence Information)****THE GRAND JURY FURTHER CHARGES THAT:**

48. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

49. Beginning on or about February 28, 2014, and continuing to in or about October 2015, in the Eastern District of Virginia and elsewhere, the defendant, DANIEL EVERETTE HALE, did willfully communicate, furnish, transmit, and otherwise make available to an unauthorized person any classified information concerning the communication intelligence activities of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
K	February 28, 2014	April 2015	TOP SECRET

(In violation of Title 18, United States Code, Sections 798(a)(3).)

COUNT 5
(18 U.S.C. § 641—Theft of Government Property)

THE GRAND JURY FURTHER CHARGES THAT:

50. The General Allegations within Paragraph 1 through 41 of this Indictment are incorporated by reference.

51. Between on or about February 28, 2014, and continuing to in or about December 2016, in the Eastern District of Virginia, and elsewhere, the defendant, DANIEL EVERETTE HALE, did knowingly and unlawfully steal and convert to his own use or the use of another, and without authority, conveyed and disposed of records and things of value of the United States, namely:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
L	April 30, 2014	July 2014	UNCLASSIFIED
M	May 14, 2014	August 2014	SECRET
N	May 14, 2014	August 2014	UNCLASSIFIED
O	May 15, 2014	December 2016	UNCLASSIFIED
P	May 15, 2014	December 2016	UNCLASSIFIED
Q	May 15, 2014	December 2016	UNCLASSIFIED
R	May 15, 2014	December 2016	UNCLASSIFIED
T	June 27, 2014	N/A	UNCLASSIFIED

The aggregate value of said records and things of value being more than \$1,000.

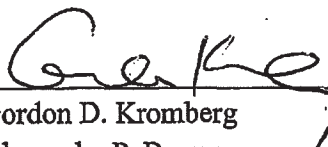
(All in violation of Title 18, United States Code, Section 641.)

A TRUE BILL:

UNDER SEAL
FOREPERSON OF THE GRAND JURY

G. Zachary Terwilliger
United States Attorney
Eastern District of Virginia

John C. Demers
Assistant Attorney General
National Security Division
U.S. Department of Justice



Gordon D. Kromberg
Alexander P. Berrang
Assistant United States Attorneys

Heather M. Schmidt
Senior Trial Attorney
Counterintelligence-Export Control Section
National Security Division
U.S. Department of Justice



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

Case: 112682
24 September 2021

CHARLES GIBBONS
POLICY DIRECTOR
DEFENDING RIGHTS & DISSENT
1325 G STREET NW SUITE 557
WASHINGTON DC 20005

Dear Charles Gibbons:

This responds to your Freedom of Information Act (FOIA) request of 27 August 2021, for:

We are requesting National Security Agency records created from 2012 to 2021 that mentions or references

- Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.
- Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016
- The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.
- "The Drone Papers" an October 2015 series of articles published by *The Intercept*
- *The Assassination Complex Inside the Government's Secret Drone Warfare Program*, a book published in 2017 based on aforementioned series of articles "The Drone Papers"

This letter acknowledges that we have received your request and provides some administrative information. Your request has been assigned Case Number 112682. There is certain information relating to this processing about which FOIA and applicable Department of Defense (DoD) and NSA regulations require we inform you.

Due to the large volume of requests being received by this Agency, we are experiencing delays in processing. We have begun to process your request and will provide a more substantive response to you as soon as we are able. Until further processing is done, we do not know if there will be assessable fees. Therefore, we have not addressed your request for a fee waiver at this time.

FOIA Case: 112682

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Division (P132), 9800 Savage Road STE 6932, Ft. George G. Meade, MD 20755-6932 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA Division. The telephone number of the FOIA Division is 301-688-6527.

Sincerely,

A handwritten signature in black ink, appearing to read "Michelle W.", is positioned above the typed name.

FOIA Customer Representative



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

Case: 112682
30 September 2021

CHARLES GIBBONS
POLICY DIRECTOR
DEFENDING RIGHTS & DISSENT
1325 G STREET NW SUITE 557
WASHINGTON DC 20005

Dear Charles Gibbons:

This responds to your Freedom of Information Act (FOIA) request of 27 August 2021, for "Agency records created from 2012 to 2021 that mentions or references" the following:

- Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.
- Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016
- The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.
- "The Drone Papers" an October 2015 series of articles published by *The Intercept*
- *The Assassination Complex Inside the Government's Secret Drone Warfare Program*, a book published in 2017 based on aforementioned series of articles "The Drone Papers"

Your letter was received on 27 August 2021, and assigned Case Number 112682. Please refer to this case number when contacting us about your request. There are no assessable fees for this request. Because there are no assessable fees for this request, we did not address your fee category or your request for a fee waiver. Your request has been processed under the provisions of the FOIA.

Your request seeks records about alleged NSA activities and/or programs. However, your request appears to be premised on media reports that purport to describe documents originating from NSA or that discuss alleged NSA intelligence activities and programs. Thus, we cannot acknowledge the existence or non-existence of specific documents purported to be originated

FOIA Case: 112682

by NSA, nor can we acknowledge the accuracy or inaccuracy of media reports about alleged NSA activities, to include any media publication of documents purported to be originated by NSA.

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612.

The appropriate email address to submit an appeal is
FOIA_PA_Appeals@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

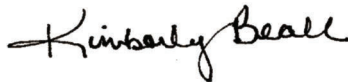
FOIA Case: 112682

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd- OGIS
College Park, MD 20740
ogis@nara.gov | 877-684-6448 | (Fax) 202-741-5769

Finally, in order to correct the misinformation flowing from certain unauthorized disclosures of classified national security information, and to reassure the American public as to the numerous safeguards that protect privacy and civil liberties, since June 6, 2013, the Director of National Intelligence has declassified certain information pertaining to surveillance conducted by the NSA pursuant to law. I generally refer you to <http://icontherecord.tumblr.com/tagged/decclassified> for information about declassified NSA activities and programs.

Sincerely,

A handwritten signature in black ink that reads "Kimberly Beall". The signature is written in a cursive, flowing style.

KIMBERLY BEALL
Acting Chief, FOIA/PA Division
NSA Initial Denial Authority



NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

November 1, 2021

To Whom It May Concern:

I am writing to appeal a determination made in NSA FOIA Case: 112682. A determination was made that the existence or nonexistence of the information I requested was properly classified. The reasons given to support this claim were based on an erroneous reading of the initial request.

In 2014, the FBI raided the home of a then National Geospatial-Intelligence Agency contractor (and Air Force Veteran who had previously been assigned to the NSA) for suspicion of violating the Espionage Act. In 2019, the Department of Justice brought an indictment against this same individual. In 2021, this individual pleaded guilty to one count of violating the Espionage Act.

On August 27, 2021, I filed requests with four separate agencies, including the National Security Agency, based on the indictment filed in open court. The indictment concerned the unauthorized printing and release of a number of classified documents to a media outlet (referred to hereinafter as "the leaked documents.") Although the indictment did not name the media outlet, the judge named the reporter in open court, the defendant mentioned as part of his plea a specific book, and the reporter has since publicly acknowledged he was the recipient of the documents.

The specified requested information all pertained to the leak investigation that culminated in this indictment. As the individual the Justice Department accused of leaking the information pled guilty and has been sentenced, this is not an active criminal investigation.

The pertinent part of the request read as follows:

We are requesting National Security Agency records created from 2012 to 2021 that mentions or reference

- *Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.*
- *Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016*
- *The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.*
- *"The Drone Papers" an October 2015 series of articles published by The Intercept*



- *The Assassination Complex Inside the Government's Secret Drone Warfare Program, a book published in 2017 based on aforementioned series of articles "The Drone Papers"*

The above information is hereinafter referred to as the "requested records."

On September 30, 2021, we received a response from the NSA. The response stated, "your request appears to be premised on media reports that purport to describe documents originating from NSA or that discuss alleged NSA intelligence activities and programs." It reasoned "we cannot acknowledge the existence or non-existence of specific documents purported to be originated by NSA, nor can we acknowledge the accuracy or inaccuracy about alleged NSA activities, to include any media publication of documents purported to be originated by the NSA."

This is based on a deeply erroneous reading of the FOIA request. The FOIA request is not based on media reports, but an indictment filed in open court. Two of the five bulleted descriptions of the requested records used the phrase "leak investigation." The remaining three bulleted descriptions of the requested records were records that mentioned or referenced publications that were at the heart of a criminal prosecution of a whistleblower. The specific request followed a lengthy background section explaining the investigation with specific citations to a Department of Justice press release and to the indictment itself. A copy of the indictment was included as an appendix.¹ Anyone reading the response would understand that the requested records covered a specific leak investigation, one which resulted in a criminal prosecution.

While it could be argued that any criminal investigation into the publication of the leaked documents requires a comment on their existence, the US government already confirmed their existence by filing an indictment. Fulfilling our request would not require NSA to confirm the authenticity of the leaked documents, *the US Attorney's Office already did that by including a table in the indictment of when documents were printed and when they were published.*

Concerns that acknowledging the existence or nonexistence of the requested records would require the NSA to confirm NSA intelligence activities and programs reported in the media are equally non-applicable. At its core, the request pertains not to the contents of the leaked documents published by the media, but records detailing the NSA's and other US government agencies' reactions to the publishing of the leaked documents. In choosing to execute a search warrant, secure an indictment and conviction, the Department of Justice willfully confirmed in a pretty large way that the US government had reactions to the publishing of the leaked documents.

¹ A copy of the original FOIA request, including the original appendix, is being included with this appeal.



The NSA is mentioned in the indictment five times. These include two references to searches carried out by the indicted party when he was assigned to the NSA. For examples, paragraphs 11 through 12 of the indictment reads:

In April 2013, HALE used his unclassified NSA work computer to search the internet for information on a reporter(the Reporter). Among the results of his search was information pertaining to a scheduled appearance of the Reporter on or about April 29, 2013 at a Washington, D.C. restaurant/bookstore (Bookstore).

On or about April 29, 2013, HALE attended a book tour event at the Bookstore, where he met with the Reporter. The next day ,on or about April 30,2013,HALE used his TOP SECRET NSA computer to search for classified information concerning individuals and issues about which the Reporter wrote.

Additionally, the table in the indictment listing the documents printed without authorization describes one of them ("Document E") as being "Information gathered by NSA on specific named targets classified TOP SECRET." This is far greater disclosure of information about the NSA than responding to our FOIA request would entail.

While it is conceivable that legitimate redactions could be made when processing the request, a wholesale refusal to acknowledge the existence or nonexistence of the information is not warranted. For the reasons outlined above, I am appealing this determination made in regards to NSA FOIA Case: 112682.

Sincerely,

Chip Gibbons
Policy Director
Defending Rights & Dissent





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

Case: 112682/Appeal: 5568
30 November 2021

Chip Gibbons
Policy Director
Defending Rights & Dissent
1325 G St. NW Suite 557
Washington, DC 20005

Dear Chip Gibbons:

Thank you for your correspondence of 1 November 2021, appealing the response from the National Security Agency (NSA or Agency) to your 27 August 2021 Freedom of Information Act (FOIA) request. You had requested "Agency records created from 2012 to 2021 that mentions or references" the following:

- Leak investigations resulting from the Intercept publishing information about the US terror watch list in July and August 2014.
- Leak investigations resulting from The Intercept publishing classified information about the US drone program between April 2015 and December 2016.
- The Intercept's publishing of 17 documents printed at the National Geospatial Intelligence Agency.
- "The Drone Papers" an October 2015 series of articles published by The Intercept.
- *The Assassination Complex Inside the Government's Secret Drone Warfare Program*, a book published in 2017 based on aforementioned series of articles "The Drone Papers".

Your initial request and appeal have been processed under the FOIA.

I have reviewed your request, the Agency's 30 September 2021 response to you, and your letter of appeal. Based on my review, I have determined that NSA's response was correct. Therefore, I am denying your appeal for the reasons explained below.

The appropriate response in this case is to neither confirm nor deny the existence or nonexistence of any responsive material pertaining to any NSA programs or activities. To do otherwise would result in the exposure of information, sources, methods or activities, which could harm our national security and severely undermine the NSA mission. For example, if NSA denied having information in cases where none exists, but remained silent in cases where information did exist, it would identify programs or activities in which NSA was or was not engaged. Moreover, whether or not a particular activity or program exists, as well as any Agency involvement in such an activity or program, may be classified or protected information and must remain so. The information you have provided does not confirm any specific Agency activity or

Case: 112682/Appeal: 5568

program. Your appeal is, therefore, denied because the FOIA exempts the release of classified¹ and/or protected² information.

You are hereby advised of your right pursuant to 5 U.S.C. § 552(a)(4)(B) to seek judicial review of this matter in the United States District Court in the district in which you reside, in which you have your principal place of business, in which the Agency records would normally be situated (U.S. District Court of Maryland), or in the District of Columbia.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd - OGIS
College Park, MD 20740
ogis@nara.gov / (877) 684-6448 / (202) 741-5770 / Fax (202) 741-5769

Sincerely,



LINDA M. KIYOSAKI
Freedom of Information/Privacy Act Appeal Authority

¹ The first exemption under the FOIA indicates that the FOIA does not apply to matters that are authorized by Executive Order to be kept secret and are properly classified in the interest of national defense or foreign relations. The fact of the existence or non-existence of any records responsive to your request is an appropriately classified matter. Paragraph 3.6(a) of Executive Order 13526 ("Classified National Security Information") specifically authorizes this type of response, also known as a Glomar response, to such requests made under the FOIA.

² The third exemption under the FOIA authorizes the withholding of information specifically protected from disclosure by statute. The fact of the existence or non-existence of any records responsive to your request is currently exempted from disclosure by the following statutes: Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).