

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

JUDICIAL WATCH, INC., )  
425 Third Street, S.W., Suite 800 )  
Washington, DC 20024, )

Plaintiff, )

v. )

OFFICE OF THE DIRECTOR OF )  
NATIONAL INTELLIGENCE, )  
Washington, DC 20511, )

and )

MICHAEL DEMPSEY, )  
in his official capacity as Acting )  
Director of National Intelligence, )  
Washington, DC 20511, )

and )

WILLIAM EVANINA, )  
in his official capacity as National )  
Counterintelligence Executive, )  
Washington, DC 20511, )

and )

U.S. DEPARTMENT OF STATE, )  
2201 C Street, N.W. )  
Washington, DC 20520, )

and )

REX W. TILLERSON, )  
in his official capacity as )  
U.S. Secretary of State, )  
2201 C Street, N.W. )  
Washington, DC 20520, )

Defendants. )

Civil Action No.

\_\_\_\_\_ )

## **COMPLAINT**

This Administrative Procedure Act (“APA”) lawsuit challenges Defendants’ refusal to conduct an assessment and prepare a report of whether Hillary Rodham Clinton’s email practices as U.S. Secretary of State may have damaged U.S. national security, as required by Intelligence Community Directive 732. As grounds for its lawsuit, Plaintiff alleges as follows:

### **I.**

#### **JURISDICTION AND VENUE**

1. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331.
2. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e).

### **II.**

#### **PARTIES**

3. Plaintiff Judicial Watch, Inc. is a not-for-profit, educational organization incorporated under the laws of the District of Columbia and headquartered at 425 Third Street S.W., Suite 800, Washington, DC 20024.

4. Defendant Office of the Director of National Intelligence is an agency of the U.S. Government and is headquartered in Washington, DC 20511.

5. Defendant Michael Dempsey is Acting Director of National Intelligence and has his principal place of business at the Office of the Director of National Intelligence, Washington, DC 20511. Defendant Dempsey is being sued in his official capacity.

6. Defendant William Evanina is National Counterintelligence Executive and has his principal place of business at the Office of the Director of National Intelligence, Washington, DC 20511. Defendant Evanina is being sued in his official capacity.

7. Defendant U.S. Department of State is an agency of the U.S. Government and is headquartered at 2201 C Street N.W., Washington, DC 20520.

8. Defendant Rex W. Tillerson is U.S. Secretary of State and has his principal place of business at the U.S. Department of State, 2201 C Street N.W., Washington, DC 20520. Defendant Tillerson is being sued in his official capacity.

### III.

#### **LEGAL BACKGROUND**

9. As defined by the National Security Act of 1947, the Intelligence Community consists of the Office of the Director of National Intelligence (“ODNI”) and 16 separate, federal agencies and/or agency components. 50 U.S.C. § 3003(4). Included among these agencies and/or components is the U.S. Department of State’s Bureau of Intelligence and Research.

10. The agencies and/or agency components of the Intelligence Community work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

11. The Director of National Intelligence (“DNI”) serves as head of the Intelligence Community and is charged by statute with “protect[ing] intelligence sources and methods from unauthorized disclosure,” among other duties and responsibilities. 50 U.S.C. §§ 3023(b)(1) and 3024(i)(1). ODNI exists to assist the DNI in carrying out his or her duties and responsibilities. *Id.* at § 3025(b).

12. The National Counterintelligence Executive (“NCIX”) serves as head of the Office of the National Counterintelligence Executive within the ODNI and is charged by statute with overseeing and coordinating the “production of counterintelligence damage assessments,” among other duties and responsibilities. 50 U.S.C. §§ 3383(b), (c), and (d)(4).

13. Intelligence Community Directive (“ICD”) 732, issued on June 27, 2014, requires a damage assessment be conducted whenever there is “an actual or suspected unauthorized disclosure or compromise of classified national intelligence that may cause damage to U.S. national security.” ICD 732(D)(2).

14. If a disclosure or compromise involves classified national intelligence originating from or affecting only one Intelligence Community member, the head of that member organization is required to conduct a damage assessment in coordination with the NCIX. ICD 732(D)(4).

15. If a disclosure or compromise involves classified national intelligence that originates from or otherwise affects more than one Intelligence Community member, a “Community damage assessment” must be conducted by the affected member organizations and “other representatives as directed by the DNI.” ICD 732(D)(5).

16. ICD 732 also plainly contemplates that the damage assessment result in a formal, written report. It sets forth detailed requirements concerning the preparation, contents, and use of the report, including the distribution of copies of the completed report. *See* ICD 732(D)(7) and (E). ICD 732 also specifies the roles and responsibilities of various officials, including the NCIX and the heads of the Intelligence Community members, in preparing and using the assessment. ICD 732(E). Conducting a damage assessment and preparing a report also undoubtedly entail creating other records about the assessment. *See* 44 U.S.C. § 3101 (requiring federal agencies to make and preserve records documenting their activities).

17. National intelligence may be classified at one of three levels: “Top Secret,” “Secret,” and “Confidential.” According to Executive Order (“EO”) 12356, issued on December 29, 2009, “Top Secret” applies to “information, the unauthorized disclosure of which reasonably

could be expected to cause exceptionally grave damage to the national security.” “Secret” applies to “information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.” “Confidential” applies to “information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.”

#### IV.

#### **FACTUAL ALLEGATIONS**

##### A.

#### **Secretary Clinton’s Email Practices**

18. During her tenure as U.S. Secretary of State from January 2009 to February 2013, Hillary Rodham Clinton used at least one unofficial, unsecure email account, one or more unofficial, unsecure email server(s), and multiple unofficial, unsecure devices to send and receive email when conducting official, State Department business.

19. Secretary Clinton continued to maintain her official, State Department emails on one or more unsecure, unofficial server(s) and device(s) after her tenure at the department ended.

20. In December 2014, Secretary Clinton returned approximately 30,000 emails to the State Department.

21. After a year-long investigation into Secretary Clinton’s email practices, the FBI concluded that emails sent or received by the Secretary on her unsecure, unofficial email system contained “Top Secret,” “Secret,” and “Confidential” information. In a July 5, 2016 statement, FBI Director James B. Comey described the FBI’s findings as follows;

From the group of 30,000 e-mails returned to the State Department, 110 emails in 52 e-mail chains have been determined by the owning agency to contain classified information at the time they were sent or received. Eight of those chains contained information that was Top Secret at the time they were sent; 36 chains

contained Secret information at the time; and eight contained Confidential information, which is the lowest level of classification. Separate from those, about 2,000 additional e-mails were “up-classified” to make them Confidential; the information in those had not been classified at the time the e-mails were sent.

\* \* \*

With respect to the thousands of e-mails that were not among those produced to State, agencies have concluded that three of those were classified at the time they were sent or received, one at the Secret level and two at the confidential level.

22. The FBI also found that Secretary Clinton and her colleagues “were extremely careless in their handling of very sensitive, highly classified information” and that “it is possible that hostile actors gained access to Secretary Clinton’s personal e-mail account.”

## **B.**

### **Plaintiff’s Investigation**

23. An integral part of Plaintiff’s mission is educating the public about the operations and activities of the government and government officials.

24. To this end, Plaintiff undertakes investigations of the federal government and federal officials by making extensive use of the Freedom of Information Act (“FOIA”), among other investigative tools. After submitting a FOIA request to an agency, Plaintiff analyzes the response it receives and disseminates its findings to the public.

25. Plaintiff submits over 400 FOIA requests annually. If an agency fails to respond to a request within the time required by FOIA, or if the agency withholds responsive records, Plaintiff often files suit. Plaintiff currently has over 50 FOIA lawsuits pending against the federal government.

26. On March 2, 2015, the *New York Times* reported that Secretary Clinton exclusively used an unofficial email account, hosted on a “clintonemail.com” server, for all her official email communications during her entire, four-year tenure at the State Department.

27. Plaintiff immediately commenced an investigation into Secretary Clinton's email practices and the impact of those practices, including on the Intelligence Community, the State Department, and the government generally.

28. To this end, Plaintiff reviewed relevant FOIA requests it had submitted to the State Department, as well as lawsuits it had brought seeking to compel compliance with FOIA, to determine how these requests and lawsuits had been impacted by Secretary Clinton's email practices and how to remedy that impact. Plaintiff successfully reopened some previously closed FOIA lawsuits, including one, *Judicial Watch, Inc. v. U.S. Department of State*, Case No, 13-1363 (EGS) (D. District of Columbia), in which Plaintiff subsequently was granted discovery regarding Secretary Clinton's email practices.

29. Plaintiff also served dozens of new FOIA requests either directly implicating Secretary Clinton's emails or concerning or relating to Secretary Clinton's email practices. These included requests concerning the handling and storage of the Secretary's emails, the devices on which the Secretary accessed her email, the State Department's response to the public revelation of the Secretary's email practices, attempts to recover the Secretary's emails, the national security ramifications of Secretary Clinton's email practices, and the presence of classified information in the Secretary's emails, among other matters. A substantial number of these requests led to further litigation.

30. Plaintiff's investigation into Secretary Clinton's email practices and the impact of those practices also has included retaining and consulting with computer and cybersecurity experts. Plaintiff has published extensively about its investigation and its findings to date, including in its 2016 book, "Clean House." Plaintiff's representatives have appeared in the media on numerous occasions to discuss Plaintiffs' investigations and findings to date, and

Plaintiff has hosted and produced several of its own, much-viewed video programs, which have included discussions by experts and commentators, about the Secretary's email practices and the impact of those practices.

31. Plaintiff's investigation into Secretary Clinton's email practices and the impact of those practices constituted a significant portion of the organization's programmatic efforts in 2015 and 2016.

32. Plaintiff anticipates that its investigation will continue to be a significant part of its programmatic efforts in 2017. The organization currently has approximately 13 lawsuits pending before the courts that either implicate or directly concern Secretary Clinton's emails or email practices, as well as multiple pending FOIA requests not in litigation.

### C.

#### **Defendants' Refusal to Conduct a Damage Assessment**

33. On or about September 14, 2016, ODNI announced that no Intelligence Community-wide damage assessment into Secretary Clinton's email practices would be conducted and that no individual Intelligence Community member would conduct such an assessment. *See* Bill Gertz, "DNI declined required damage assessment of Clinton's leaked email secrets," *Washington Free Beacon*, Sept. 14, 2016. Then-Director James Clapper reportedly decided that the required assessment would not be conducted. *Id.*

34. On September 16, 2016, Plaintiff sent a FOIA request to ODNI seeking access to records about the decision not to conduct the required assessment. The request was submitted as an additional part of Plaintiff's on-going investigation into the email matter and its impact. When ODNI failed to respond to the request within the time required by FOIA, Plaintiff filed suit. *See Judicial Watch, Inc. v. Office of the Director of National Intelligence*, Case No. 17-

0053 (RDW) (D. District of Columbia). As of the date of this complaint, ODNI was still searching for responsive records and no responsive records have been produced.

35. On January 10, 2017, Plaintiff sent a letter to then-Director Clapper, National Counterintelligence Executive Evanina, and then-Secretary John Kerry formally requesting that “the damage assessment required by ICD 732 be commenced without further delay.” A true and correct copy of Plaintiff’s letter is attached hereto as Exhibit A and incorporated herein by reference.

36. To date, Plaintiff has received no response to its January 10, 2017 request, and Plaintiff is not aware of any report or announcement indicating that the assessment and resulting report required by ICD 732 has been conducted and prepared. On information and belief, no assessment has been conducted and no report has been prepared.

37. A damage assessment report and records about an assessment conducted pursuant to ICD 732 are the quintessential types of records that Plaintiff would request and obtain under FOIA, then analyze and make available to the public as part of its educational mission.

38. If the Intelligence Community had conducted a damage assessment of Secretary Clinton’s email practices during her tenure at the State Department as required by ICD 732, Plaintiff undoubtedly would have submitted a FOIA request for the report of the assessment and for any other records about the assessment as part of its ongoing investigation. The only reason Plaintiff has not requested such records is because Defendants have failed and refused to conduct the required assessment.

39. Prior damage assessments reports prepared by the Intelligence Community, or at least portions of such reports and other records about damage assessments, have been made public through FOIA or otherwise. For example, in May 2014, a FOIA lawsuit compelled the

disclosure of records about the damage assessment prepared after former National Security Agency contractor Edward Snowden's compromise of classified national intelligence. *See Leopold v. U.S. Dep't of Defense*, Case No. 14-cv-0197 (TSC) (D. District of Columbia).

40. Plaintiff's investigation into Secretary Clinton's email practice and the impact of those practices continues to date.

41. Because no damage assessment has been undertaken, Plaintiff is unable to request and obtain any and all releasable portions of the assessment report, as well as any and all releasable records about the assessment, and analyze and disseminate these records to the public. As a result, Plaintiff is being deprived of information that would aid its investigation into Secretary Clinton's email practices and the impact of those practices, including on the Intelligence Community, the State Department, and the government generally, and is being harmed in its ability to carry out its educational mission.

**COUNT I**  
**(Administrative Procedure Act Violation)**

42. Plaintiff realleges paragraphs 1 through 41 as if fully stated herein.

43. Under the APA, a reviewing court shall "compel agency action unlawfully withheld or unreasonably delayed" and "hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. §§ 706(1) and (2)(A).

44. Defendants have a mandatory, non-discretionary duty under ICD 732 to conduct a damage assessment of Secretary Clinton's email practices during her tenure at the State Department and prepare a report of their findings.

45. Defendants' failure and/or refusal to conduct the required damage assessment and prepare a report of their findings constitutes "agency action unlawfully withheld or unreasonably

delayed” and/or final agency action that is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.”

46. Defendants’ unlawful failure and/or refusal to conduct the required damage assessment and prepare a report of their findings is causing Plaintiff irreparable harm because it prevents Plaintiff from requesting, obtaining, and disseminating any and all releasable portions of the assessment report, as well as any and all releasable records about the assessment, under FOIA. More specifically, Defendants are injuring Plaintiff not only in its ability to obtain information for its investigation into Secretary Clinton’s email practices and the impact of those practices, a matter that is of substantial importance to Plaintiff, but Defendants also are injuring Plaintiff in its ability to carry out its educational mission.

47. Plaintiff has no adequate or available administrative remedy.

48. Plaintiff has no adequate remedy at law.

WHEREFORE, Plaintiff respectfully requests that the Court: (1) declare Defendants’ failure and/or refusal to conduct a damage assessment of Secretary Clinton’s email practices during her tenure at the State Department and prepare a report in accordance with ICD 732 to be “agency action unlawfully withheld or unreasonably delayed” and is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;” (2) order Defendants to conduct the required damage assessment and prepare a report in accordance with ICD 732 so that Plaintiff may request and obtain all releasable portions of the report and related records under FOIA; (3) grant Plaintiff an award of attorneys’ fees and other litigation costs reasonably incurred in this action; and (4) grant Plaintiff such other relief as the Court deems just and proper.

Dated: March 21, 2017

Respectfully submitted,

/s/ Michael Bekesha

Michael Bekesha

D.C. Bar No. 995749

JUDICIAL WATCH, INC.

425 Third Street S.W., Suite 800

Washington, DC 20024

(202) 646-5172

*Counsel for Plaintiff*

# **Exhibit A**



**Judicial  
Watch**<sup>®</sup>  
*Because no one  
is above the law!*

**VIA CERTIFIED MAIL**

January 10, 2017

Mr. James R. Clapper  
Director of National Intelligence  
Office of the Director of National Intelligence  
Washington, DC 20511

Mr. William Evanina  
National Counterintelligence Executive  
Office of the Director of National Intelligence  
Washington, DC 20511

Mr. John F. Kerry  
U.S. Secretary of State  
U.S. Department of State  
2201 C Street, N.W.  
Washington, DC 20520

**Re: Damage Assessment Arising from Secretary Hillary Rodham Clinton's Use  
of An Unofficial Email Account/Server**

Gentlemen:

As you undoubtedly are aware, during her 2009-13 tenure as U.S. Secretary of State, Hillary Rodham Clinton used at least one unsecure, unofficial email account and one or more unsecure, unofficial email servers and devices to conduct official, State Department business. Secretary Clinton continued to maintain her official, State Department emails on one or more unsecure, unofficial servers and devices after her tenure at the department ended. She returned a portion of these emails to the State Department in December 2014. On July 5, 2016, FBI Director James B. Comey issued the following assessment of the emails returned by then-Secretary Clinton:

From the group of 30,000 e-mails returned to the State Department, 110 emails in 52 e-mail chains have been determined by the owning agency to contain classified information at the time they were sent or received. Eight of those chains contained information that was Top Secret at the time they were sent; 36 chains contained Secret information at the time; and eight contained Confidential information, which is the lowest level of classification. Separate from those,

January 10, 2017  
Page 2

about 2,000 additional e-mails were “up-classified” to make them Confidential; the information in those had not been classified at the time the e-mails were sent.

<https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system>. Director Comey’s assessment continued: “With respect to the thousands of e-mails that were not among those produced to State, agencies have concluded that three of those were classified at the time they were sent or received, one at the Secret level and two at the confidential level. *Id.* The assessment also found that Secretary Clinton and her colleagues “were extremely careless in their handling of very sensitive, highly classified information” and “it is possible that hostile actors gained access to Secretary Clinton’s personal e-mail account.” *Id.*

According to Executive Order 12356, the classification “Top Secret” “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.” The classification “Secret” “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.” The classification “Confidential” “shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.”

Intelligence Community Directive (“ICD”) No. 732 requires a damage assessment be conducted when there is “an actual or suspected unauthorized disclosure or compromise of classified national intelligence that may cause damage to U.S. national security” or “an actual or suspected loss, misuse, or unauthorized access to or modification of classified national intelligence that could adversely affect national security.” The National Security Act of 1947, as amended, mandates that the Director of National Intelligence “shall protect intelligence sources and methods from unauthorized disclosure” (50 U.S.C. § 3024(i)(1)), and ICD No. 700 requires that agency heads within the Intelligence Community, including the Department of State, “[p]rotect national intelligence and intelligence sources, methods, and activities from unauthorized disclosure.” Assessing the damage from actual or suspected, unauthorized disclosure plainly is an important part of protecting intelligence sources, methods, and activities.

Then-Secretary Clinton’s use and maintenance of at least one unsecure, unofficial email account and one or more unsecure, unofficial email servers and devices to send, receive, and store Top Secret, Secret, and Confidential information plainly constitutes, at a minimum, a suspected, unauthorized disclosure or compromise of classified national intelligence or a suspected loss, misuse, or unauthorized access to or modification of classified national intelligence that may cause damage to or could adversely affect national security. It is our understanding, however, that no damage assessment under ICD No. 732 was undertaken or is planned. *See, e.g.,* Bill Gertz, “DNI declined required damage assessment of Clinton’s leaked email secrets,” *Washington Free Beacon*, Sept. 14, 2016 (quoting Office of the Director of National Intelligence Spokesmen Joel D. Melstad as saying, “ODNI is not leading an [intelligence community]-wide damage assessment and is not aware of any individual IC element conducting such formal assessments.”).

January 10, 2017

Page 3

Judicial Watch, Inc. (“Judicial Watch”) is a not-for-profit educational organization that seeks to promote transparency, accountability, and integrity in government and fidelity to the rule of law. For more than 20 years, Judicial Watch has used the Freedom of Information Act (“FOIA”) and other public records laws and investigative tools to gather information about the operations and activities of the federal government. We submit over 400 FOIA requests annually, analyze the responses we receive, and disseminate our findings to the public. Judicial Watch has served dozens of FOIA requests either directly implicating Secretary Clinton’s emails or concerning or relating to her email practices, attempts to recover her emails, and the handling and storage of her emails, among other related subjects. Judicial Watch’s investigatory efforts regarding Secretary Clinton’s emails have constituted a substantial portion of the organization’s programmatic efforts over the past eighteen months.

A damage assessment such as the one required by ICD No. 732 is a quintessential type of record that Judicial Watch would request and obtain under FOIA, analyze, and then make available to the public in carrying out its educational mission. Prior damage assessments, or at least portions of such assessments, have been made public through FOIA or otherwise. In May 2014, for example, a FOIA lawsuit compelled the disclosure of a Defense Intelligence Agency damage assessment of former National Security Agency Contractor Edward Snowden’s compromise of classified material. *See Leopold v. U.S. Dep’t of Defense*, Case No. 14-cv-0197 (TSC) (D. District of Columbia).

The failure to undertake the required assessment harms Judicial Watch by depriving it of information it ordinarily would request and obtain under FOIA, thus damaging its ability to carry out its public interest mission of obtaining and disseminating information about the federal government’s operations and activities. This is especially the case given Judicial Watch’s extensive investigation into Secretary Clinton’s emails, email practices, and related subjects. Accordingly, Judicial Watch respectfully requests that the damage assessment required by ICD No. 372 be commenced without further delay.

Should the required assessment not be undertaken, we are prepared to file suit in an appropriate federal district court seeking to compel compliance with ICD No. 732, so that we might seek and obtain access to the assessment. *See, e.g., Federal Election Commission v. Atkins*, 524 U.S. 11 (1998); *Action Alliance of Senior Citizens v. Heckler*, 789 F.2d 931 (D.C. Cir. 1986). Please advise us no later than February 10, 2017 if an assessment will be undertaken. If we do not hear from you by that date, we will assume no assessment will be undertaken and will act accordingly.

Thank you for your attention to this matter.

Sincerely,



Thomas J. Fitton  
President