



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

**Via electronic mail (dni\_pao\_outreach@dni.gov)**

May 7, 2020

Mr. Richard Grenell  
Director of National Intelligence  
Office of the Director of National Intelligence  
Washington, DC 20511

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

Director Grenell:

As you undoubtedly are aware, during her 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, 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-comev-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-svstem>. 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.”

In addition, the State Department’s Bureau of Diplomatic Security also investigated Secretary Clinton’s use of at least one unsecure, unofficial email account. In September 2019, the State Department concluded:

[T]he use of a private email system to conduct official business added an increased degree of risk of compromise as a private system lacks the network monitoring and intrusion detection capabilities of State Department networks.

DS Office of Information Security, DS Report on Security Incidents Related to Potentially Classified Emails sent to Former Secretary of State Clinton’s Private Email Server, US. State Department (Sept. 13, 2019, available at <https://www.grassley.senate.gov/sites/default/files/documents/2019-10-17%20State%20Dept.%20to%20CEG%20-%20Classified%20Emails.pdf>). In addition, the State Department concluded that there were at least 598 instances where State Department employees failed to safeguard classified information. *Id.*

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.”).

Judicial Watch, Inc. 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 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 several years.

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. Department of Defense*, Case No. 14-cv-00197 (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.

Thank you for your attention to this matter.

Sincerely,



Thomas J. Fitton  
President