

UNCLASSIFIED

U.S. HOUSE OF REPRESENTATIVES  
PERMANENT SELECT COMMITTEE  
ON INTELLIGENCE

HVC-304, THE CAPITOL  
WASHINGTON, DC 20515  
(202) 225-4121

DAMON NELSON  
STAFF DIRECTOR

TIMOTHY S. BERGREEN  
MINORITY STAFF DIRECTOR

July 27, 2017

The Honorable Daniel Coats  
Director of National Intelligence  
Washington, D.C. 20511

Dear Director Coats:

The House Intelligence Committee views the protection of classified information, which is essential to defending the national security of the United States, as a key oversight responsibility. Unauthorized disclosures, whether the result of disgruntled employees or for the advancement of partisan political ideology, are crimes that can result in the Intelligence Community's loss of access to critical intelligence information and can endanger the lives of sources. All leaks of classified information must be vigorously prosecuted, and the Committee is working to ensure law, policy and funding are aligned to maximize the prosecution of these crimes.

As you are aware, since the 2016 U.S. Presidential election, there have been numerous leaks alleging inappropriate or unlawful activity by individuals associated with President Trump. These allegations are generally sourced from "current and former Administration officials." Whether true, partially true, or entirely untrue, these leaks have undermined our political processes and emboldened and aided our adversaries. Separate and aside from the real and present danger associated with Russian aggression, these leaks damage our national security and are an affront to the brave men and women who serve in silence within the Intelligence Community. Classified information is held secret for good reason, and our intelligence apparatus simply cannot function capably amid the continual exposure of classified information.

To assist the Committee in understanding how U.S. person information contained in intelligence reports could be leaked to the media, we are actively reviewing the policies, procedures and practices of the Intelligence Community concerning the dissemination of U.S. person information. Although we are still conducting our review, we have found evidence that current and former government officials had easy access to U.S. person information, and it is possible that these officials used this information to achieve partisan political purposes, including the selective, anonymous leaking of such information.

The Intelligence Community, its leaders, law enforcement personnel, and policy makers may have valid reasons for unmasking U.S. person identities and may do so in compliance with law and policy. However, the Committee has found that senior government officials offered

UNCLASSIFIED

UNCLASSIFIED

remarkably few individualized justifications for access to this U.S. person information. For example, this Committee has learned that one official, whose position had no apparent intelligence-related function, made *hundreds* of unmasking requests during the final year of the Obama Administration. Of those requests, only one offered a justification that was not boilerplate and articulated why that specific official required the U.S. person information for the performance of his or her official duties.

The Committee also understands that Obama-era officials sought the identities of Trump transition officials within intelligence reports. However, there was no meaningful explanation offered by these officials as to why they needed or how they would use this U.S. person information, and thus, the Committee is left with the impression that these officials may have used this information for improper purposes, including the possibility of leaking. More pointedly, some of the requests for unminimized U.S. person information were followed by anonymous leaks of those names to the media.

Although the Committee has yet to complete its review, we have identified a significant issue that will require changes to federal law. Specifically, we have found that the Intelligence Community's U.S. person unmasking policies are inadequate to prevent abuse, such as political spying.


To address this serious deficiency in the application of current policy as well as the lack of statutory requirements, I will introduce a bill to require individual, fact-based justifications for each request for U.S. person information sourced from disseminated intelligence reports. This new *statutory* requirement should be consistent with the current *policy* imposed on rank-and-file intelligence officials, which to-date has shown no sign of abuse.

The new law must, however, require conformity at the top levels of government. Cabinet members and other senior political leaders cannot be permitted to continue to seek access to U.S. person information within disseminated intelligence reports without documenting a specific, fact-based requirement for the information. In addition, the Committee is examining other requirements to enhance auditing and oversight in this area.

To accomplish these changes to federal law without undermining the important and lawful activities of the Intelligence Community, I request that the Office of Director of National Intelligence provide the HPSCI staff technical assistance in the drafting of legislation. It is my goal to complete drafting during the August recess, and your commitment to working with the Committee will ensure the best outcome for the American people's privacy and security.

Thank you for your continued cooperation with the Committee's review. If you have any questions, please contact me at (202) 225-4121.

Sincerely,



DEVIN NUNES  
Chairman

UNCLASSIFIED