RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

June 16, 2020

The Honorable John Ratcliffe
Director
Office of the Director of National Intelligence
Washington DC, 20511

Dear Director Ratcliffe:

I write to seek information about widespread cybersecurity problems across the intelligence community.

After a series of high-profile cybersecurity lapses at federal agencies, Congress took action in 2014, and gave the Department of Homeland Security (DHS) the authority to require federal agencies to adopt specific cybersecurity technologies and policies to safeguard federal systems. While Congress exempted the intelligence community from the requirement to implement DHS's cybersecurity directives, Congress did so reasonably expecting that intelligence agencies that have been entrusted with our nation's most valuable secrets would of course go above and beyond the steps taken by the rest of the government to secure their systems. Unfortunately, it is now clear that exempting the intelligence community from baseline federal cybersecurity requirements was a mistake.

In the spring of 2017, WikiLeaks published a cache of Central Intelligence Agency (CIA) hacking tools. The CIA's WikiLeaks Task Force investigated this incident, and submitted a report on its findings to the CIA Director in October, 2017. The Department of Justice (DOJ) made public an excerpt from the report in court filings this year, which DOJ subsequently provided to my office. According to the attached redacted excerpt from this CIA report, WikiLeaks' publication "brought to light multiple ongoing CIA failures" that enabled a CIA employee to steal "at least 180 gigabytes" of information, "the largest data loss in CIA history," which he allegedly then provided to WikiLeaks. The report's findings include:

> The CIA's [Center for Cyber Intelligence (CCI)] had prioritized building cyber weapons at the expense of securing their own systems. Day-to-day security practices had become woefully lax....Most of our sensitive cyber weapons were not compartmented, users shared systems administrator-level passwords, there were no effective removable media controls, and historical data was available to users indefinitely. Furthermore, CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed. These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

The lax cybersecurity practices documented in the CIA's WikiLeaks Task Force report do not appear to be limited to just one part of the intelligence community. The Office of the Inspector General of the Intelligence Community revealed in a public summary of a report it published last year that it found a number of deficiencies in the intelligence community's cybersecurity practices. In addition to making two new recommendations for improvements, the Inspector General noted that 20 security-related recommendations from prior evaluations remained unaddressed. According to the Inspector General's report, the specific details of the intelligence community's cybersecurity deficiencies and the Inspector General's recommendations are classified.

The 2017 CIA WikiLeaks Task Force report noted that "This wake-up call presents us with an opportunity to right longstanding imbalances and lapses, to reorient how we view risk… We must care as much about securing our systems as we care about running them if we are to make the necessary revolutionary change." Three years after that report was submitted, the intelligence community is still lagging behind, and has failed to adopt even the most basic cybersecurity technologies in widespread use elsewhere in the federal government. The American people expect you to do better, and they will then look to Congress to address these systematic problems. In order to help Congress and the American people understand the magnitude of the intelligence community's cybersecurity lapses, please provide me with unclassified answers to the following questions by July 17, 2020:

1. On January 10, 2019, DHS' Cybersecurity and Infrastructure Security Agency (CISA) issued a public alert regarding a global Domain Name System (DNS) infrastructure hijacking campaign, which cybersecurity companies attributed to hackers working for the Iranian government. On January 22, 2019, CISA followed up on this warning, and issued an emergency directive that required agencies, within 10 days, to implement multi-factor authentication to protect their .gov domain names. Fifteen months later, the intelligence community has yet to protect its .gov domain names with multi-factor authentication, despite repeated requests from my office. Please explain the reasons for this delay and provide me with an estimate for when you expect to have implemented this cybersecurity best-practice across the intelligence community.

2. On October 16, 2017, CISA issued a directive to federal agencies requiring them to protect their websites and email using encryption and other advanced cybersecurity technologies. This CISA directive included a requirement to adopt DMARC, an anti-phishing technology. The vast majority of federal agencies have complied with this directive and implemented DMARC — nearly 80 percent according to one recent survey. Unfortunately, the intelligence community has lagged behind the rest of the government in DMARC adoption. My staff verified—using publicly available tools—that the Central Intelligence Agency, the National Reconnaissance Office, and your office have all failed to enable DMARC anti-phishing protections which would prevent hackers from sending emails that impersonate your organizations. Please explain the reasons why the intelligence community, and your office in particular, have not adopted DMARC and provide me with an estimate for when you expect to have implemented this cybersecurity best-practice across the intelligence community.

3. According to media reports, the Joint Worldwide Intel Communications System (JWICS), the intelligence community's classified computer network for top secret information, does not currently use multi-factor authentication, an industry-standard cybersecurity protection. In a presentation at the Department of Defense Intelligence Information System Worldwide Conference on August 20, 2019, Jean Schaffer, the Defense Intelligence Agency's (DIA) cyber and enterprise operations chief, stated that DIA was looking to upgrade JWICS to support multi-factor authentication. Please explain why JWICS does not currently require multi-factor authentication and why this is consistent with federal cybersecurity best practices detailed by the National Institute of Standards and Technology in Special Publication 800-63B.

4. Do you intend to adopt each of the 22 cybersecurity recommendations of the Inspector General of the Intelligence Community? If yes, please provide an estimate for when you expect to have implemented each of these recommendations. If no, please explain why.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator

17 October 2017

WikiLeaks Task Force

Final Report

[redacted]

Intelligence Brief

Intelligence Brief

17 October 2017

[redacted] **Memo To:** **Director, Central Intelligence Agency**
Deputy Director, Central Intelligence Agency
Chief Operating Officer, Central Intelligence Agency

[redacted] **From:** **WikiLeaks Task Force,** [redacted]

[redacted] **Subject:** **WikiLeaks Task Force Final Report**

[redacted] Executive Summary

[redacted] WikiLeaks' announcement on 7 March that it possessed cyber tools from CIA's Center for Cyber Intelligence (CCI), dubbed "Vault 7," marked the largest data loss in CIA history. In its initial public disclosure, WikiLeaks provided the names and brief descriptions of multiple tools that CIA developed for cyber operations. Since 7 March, WikiLeaks has published more comprehensive descriptions of 35 tools, including internal CIA documents associated with each tool. [redacted]

- [redacted] We assess that in spring 2016 a CIA employee stole at least 180 gigabytes to as much as 34 terabytes of information. This is roughly equivalent to 11.6 million to 2.2 billion pages in Microsoft Word. This data loss includes [redacted] cyber tools that resided on the Center for Cyber Intelligence (CCI) software development network (DevLAN). We cannot determine the precise scope of the loss because, like other mission systems[a] at that time, DevLAN did not require user activity monitoring or other safeguards that exist on our enterprise system.
- [redacted]
- [redacted] To date, WikiLeaks has released user and training guides and limited source code from two parts of DevLAN: Stash, a source code repository, and Confluence, a collaboration and communication platform. All of the documents reveal, to varying degrees, CIA's tradecraft in cyber operations.

[redacted]

[redacted] This product is intended for internal Agency use. [redacted]

[a] We define a mission system as any computer-based capability that collects, stores, processes, or communicates information that is managed by a mission component [redacted]

[redacted]

[redacted] Critical Context

[redacted] **CCI:** The WikiLeaks breach occurred at CCI, whose mission is to transform intelligence through [redacted] cyber operations. It would be unfair to lay the blame for the breach with the current management, as the breach occurred before most joined CCI. Equally, CCI correctly notes that the mission system in question complied with all Agency requirements at the time of the breach. However, in a press to meet growing and critical mission needs, CCI had prioritized building cyber weapons at the expense of securing their own systems. Day-to-day security practices had become woefully lax. The Development Network (DevLAN) on which CCI's work product resided had been certified and accredited, but CCI had not worked with CIMC to develop or deploy user activity monitoring or robust server audit capability. Most of our sensitive cyber weapons were not compartmented, users shared systems administrator-level passwords, there were no effective removable media controls, and historical data was available to users indefinitely. Furthermore, CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed. These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security.

[redacted]

[redacted] **Mission Systems:** CIA has moved too slowly to put in place the safeguards that we knew were necessary given successive breaches to other US Government agencies. For nearly a decade WikiLeaks has exploited the digital realm to profoundly reshape opportunities for individuals sworn to protect our nation's secrets to leak classified or sensitive information. While CIA was an early leader in securing our enterprise information technology (IT) system, we failed to correct acute vulnerabilities to our mission IT systems. Because the stolen data resided on a mission system that lacked user activity monitoring and a robust server audit capability, we did not realize the loss had occurred until a year later, when WikiLeaks publicly announced it in March 2017. Had the data been stolen for the benefit of a state adversary and not published, we might still be unaware of the loss—as would be true for the vast majority of data on Agency mission systems.

— [redacted] The Agency for years has developed and operated IT mission systems outside the purview and governance of enterprise IT, citing the need for mission functionality and speed. While often fulfilling a valid purpose, this "shadow IT" exemplifies a broader cultural issue that separates enterprise IT from mission IT, has allowed mission system owners to determine how or if they will police themselves, and has placed the Agency at unacceptable risk.

[redacted]

[redacted]

[redacted] This wake-up call presents us with an opportunity to right longstanding imbalances and lapses, to reorient how we view risk, [redacted]. We must recognize when we are taking smart risks and when operational shortcuts or waivers create unwarranted risk to our work and to the Agency. We must care as much about securing our systems as we care about running them if we are to make the necessary revolutionary change.

[redacted]

[redacted] Recommendations

[redacted]

[redacted] The WikiLeaks Vault 7 disclosures have brought to light multiple ongoing CIA failures that our recommendations are designed to address:

- [redacted] We failed to equip the mission system in question with user activity monitoring and robust server audit capability, which could have deterred, detected, and possibly prevented the theft. [redacted]
- [redacted] We failed to empower any single officer with the ability to ensure that all Agency information systems are built secure and remain so throughout their life cycle. Because no one had that ability, no one was accountable—and the mission system in question, like many [redacted] others, lacked appropriate security. [redacted]
- [redacted] We failed to ensure that our ability to secure our information systems against emerging threats kept pace with the growth of such systems across the Agency. [redacted]
- [redacted]
- [redacted]
- [redacted] We failed to recognize or act in a coordinated fashion on warning signs that a person or persons with access to CIA classified information posed an unacceptable risk to national security. *(See recommendations B1, B2, B3, B4, B6, B7, B8, B9, and C8.)*

[redacted]

[redacted]

[b] A "zero-day" exploit is software designed to exploit a previously unknown or unpatched computer vulnerability.

Recommendation A5:

Enhance information technology security guidelines and classified information handling restrictions for zero-day exploits and offensive cyber tools, consistent with Executive Order 13526, Classified National Security Information. We judge the vulnerability of and threat to this information is exceptional and warrants additional security protections, to include requiring segmentation of knowledge, tools, and people through physical and logical infrastructure, policy and procedural controls, and enforcing strict need-to-know access to the tools and exploits.

[redacted]

[redacted] The WikiLeaks disclosures revealed resource-driven gaps and weaknesses in CIA's insider threat program. There have been seams in communication between components such as the Office of Medical Services, Human Resources, Security, Counterintelligence Mission Center, and line management that have sometimes prevented us from connecting the dots to corporately detect and address insider threats. [redacted]

— [redacted] We have been slow—due to resource choices and cultural resistance—to extend state-of-the-art audit and user activity monitoring technology to mission systems not connected to the main enterprise network. [redacted]

[redacted] Recommendation [redacted]

[redacted] Frequent personnel security reviews and training have focused on enterprise "privileged users," defined as individuals designated and entrusted by managers to perform elevated functions on a network, system, or application. This does not include privileged users on mission systems or those with extraordinary access or capabilities, such as EDG developers. [redacted]

[redacted]

[redacted]

Data in Confluence, a collaboration and communication platform, and some data in Stash, a source code repository, have been released by WikiLeaks; we assess WikiLeaks possesses all of the Confluence and Stash data.[51] However, we now assess with moderate confidence that WikiLeaks does not possess the Gold folder of final versions of all developed tools and source code that resided on the Development Network (DevLAN), even though WikiLeaks claims it has released only a small slice of the archive it possesses. The Gold folder was better protected; WikiLeaks so far has released data in Stash despite the availability of newer, easier to exploit versions of tools in Gold; and Gold's size, several terabytes, made it harder to export.

[redacted]

[redacted] We are making educated assumptions about the scope and timing of the loss, in part because we lacked effective monitoring and auditing of this mission system. [redacted]

[redacted]

The WikiLeaks disclosures revealed gaps and weaknesses in CIA's Insider Threat program, which has traditionally relied on close coordination between the Office of Security and CIMC. Among the gaps are the seams in communication between components such as the Office of General Counsel, Medical Services, Human Resources, security, counterintelligence, and line management that have sometimes prevented us from connecting the dots to corporately detect and address Insider Threat issues. [redacted]