UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **JACKSON ALEXANDER COSKO,** ***Defendant.***	Mag. No.: **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jason R. Bell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Captain with the United States Capitol Police (the "USCP"), where I have served since April 7, 2002. I am currently assigned to the Investigations Division. I have attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received training and gained experience in search and arrest warrant applications, the executions of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other relevant training.

2. The facts set forth below are based upon my own observations, investigative reports and information provided to me by other law enforcement agents. This affidavit is intended to show only that there is sufficient probable cause for the complaint submitted with this affidavit, and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 119 (Making Public Restricted Personal Information), 18 U.S.C. § 875(d) (Threats in Interstate Communications), 18 U.S.C. § 1030(a)(3) (Unauthorized Access of a Government Computer), 18 U.S.C. § 1028(a)(7) (Identity Theft), and

18 U.S.C. § 1512(b)(3) (Witness Tampering), D.C. Code § 22-801(b) (Second Degree Burglary), D.C. Code § 22-3302(b) (Unlawful Entry) have been committed by Jackson Alexander Cosko ("COSKO"). Section 119 of Title 18 of the United States Code imposes criminal penalties on whoever makes public restricted personal information of certain covered individuals, including U.S. government employees and officers. Section 875(d) of Title 18 of the United States Code imposes criminal penalties on whoever "with intent to extort from any person . . . any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another." Section 1030(a)(3) of Title 18 of the United States Code imposes criminal penalties on whoever intentionally accesses a government-owned computer without authorization or exceeds authorized access. Section 1028(a)(7) of Title 18 of the United States Code imposes criminal penalties on whoever "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." Section 1512(b)(3) of Title 18 of the United States Code imposes criminal penalties on "[w]hoever knowingly uses intimidation, threatens, or corruptly persuades another person, or attempts to do so, . . . with intent to (3) hinder, delay, or prevent the communication to a law enforcement officer or judge of the United States of information relating to the commission or possible commission of a Federal offense." Section 801(b) of Title 22 of the D.C. Code imposes criminal penalties on "whoever shall . . . break and enter, or enter without breaking, any dwelling . . . or other building . . . , whether at the time occupied or not . . . with intent to break and carry away any part thereof or any fixture or other thing attached to or connected with the same, or to commit any criminal offense". Section 3302(b) of Title 22 of the D.C. Code imposes criminal

penalties for "[a]ny person who, without lawful authority, shall enter, or attempt to enter, any public building, or other property, or part of such building, or other property, against the will of the lawful occupant or of the person lawfully in charge thereof or his or her agent[.]"

PROBABLE CAUSE

September 27: The Restricted Personal Information of Three United States Senators Was Published On Wikipedia.org

4. As background, Wikipedia is an online encyclopedia that is accessible to the public at www.wikipedia.org. Wikipedia invites crowd-editing, that is, it permits members of the public not only to view the contents of its encyclopedia entries (or "pages"), but also to edit them. Wikipedia maintains certain records concerning edits to its pages, including records of the Internet Protocol ("IP") addresses associated with particular edits.

5. On or about September 27, 2018, staff of U.S. Senator 1 contacted the USCP Threat Assessment Section ("USCP TAS") to report that unknown person/persons edited the Wikipedia page for U.S Senator 1. The Senator's staff reported that U.S. Senator 1's restricted personal information (including the Senator's private home addresses, personal cell phone numbers, and office numbers) had been published on Wikipedia. U.S. Senator 1 staff provided USCP TAS with a screen shot of the Wikipedia post.

6. A review of the screen shot revealed that the Wikipedia page for U.S. Senator 1 had been edited to include U.S. Senator 1's personal information (as described above) on September 27, 2018, at 21:13 UTC (5:13 p.m. Eastern), using the IP address 143.231.249.130 (the ".130 IP address").

7. On September 27, 2018, USCP TAS was contacted by the staff of U.S Senator 6, who reported the publication of U.S. Senator 1's information, as well as the publication, on Wikipedia, of restricted personal information of two other U.S. Senators.

8. Specifically, U.S. Senator 6's staff reported that restricted personal information belonging to U.S. Senator 2 and U.S Senator 3 had been published on Wikipedia. U.S. Senator 6's staff provided screen shots of the three edited Wikipedia pages that were the subject of their report.

9. A review of the Wikipedia screen shot of U.S. Senator 2's Wikipedia page revealed that the page had been edited on September 27, 2018, at 21:25 UTC (5:25 p.m. Eastern), using the .130 IP address. Specifically, the page had been edited to publish U.S. Senator 2's restricted personal information, including, among other things, U.S. Senator 2's home address and home telephone number.

10. A review of the Wikipedia screen shot of U.S. Senator 3's Wikipedia page revealed that the page had been edited on September 27, 2018, at 21:54 UTC (5:54 p.m. Eastern), using the IP address 143.231.249.136 (the ".136 IP address"). Specifically, the page had been edited to publish U.S. Senator 3's restricted personal information, including, among other things, U.S. Senator 3's home address and home telephone number.

11. The above-described edits to the Wikipedia pages of U.S. Senators 1, 2, and 3 occurred roughly contemporaneously with public – and highly publicized – Senate proceedings related to a nomination for the U.S. Supreme Court. That nomination was and is pending before the Senate at all relevant times herein.

12. An open source search of the .130 and .136 IP addresses revealed that both IP addresses belong to the U.S. House of Representatives in Washington, DC.

13. USCP contacted the House of Representatives Security Operations Center ("SOC") to request a search of network activity using those two IP addresses, to determine whether a valid account user could be associated with those IP addresses. The SOC determined that the .130 IP address was assigned to the open Wi-Fi network assigned to the House of Representatives. Based on my training and experience, I know that this indicates that, at the time that the restricted personal information of U.S. Senators 1 and 2 was published on Wikipedia, the actor was using a portable computer device that connected to the internet (and Wikipedia) through the .130 IP address.

14. The SOC determined that the .136 IP address was assigned to a House of Representatives wired network. Based on my training and experience, I know that this indicates that, at the time that the restricted personal information of U.S. Senator 3 was published on Wikipedia, the actor was connected to the internet (and Wikipedia) using a valid House of Representatives user account.

October 1: The Restricted Personal Information of Two Additional United States Senators Was Published On Wikipedia.org

15. On October 1, 2018, USCP TAS was contacted by Witness 1, a staff member for U.S. Senator 4, who reported observing Twitter postings showing that the restricted personal information of U.S. Senator 5 and U.S. Senator 4 had been published on Wikipedia. Witness 1 provided USCP TAS with screen shots of the Wikipedia pages.

16. A review of the screen shot of the Wikipedia page for U.S. Senator 5 revealed that the page had been edited on October 1, 2018, at 21:52 UTC (5:52 p.m. Eastern), using the IP address 156.33.195.125 (the ".125 IP address"). Specifically, the page had been edited to publish restricted personal information belonging to U.S. Senator 5, including, among other things, U.S. Senator 5's home address and home telephone number.

17. A review of the screen shot of the Wikipedia page for U.S. Senator 4 revealed that the page had been edited on October 1, 2018, at 21:50 UTC (5:50 p.m. Eastern), using the .125 IP address. The screen shot also showed that the edit had been a "mobile edit" which indicates that a mobile device (rather than a desktop computer) was used to make the edit. The screen shot further showed that the page had been edited to publish restricted personal information belonging to U.S. Senator 4, including, among other things, U.S. Senator 4's home address and home telephone number.

18. Further review of the screen shot of the Wikipedia page for U.S. Senator 4 revealed that the following statements were also included in the edit of the page:

a. "He dares call for an investigation of ME?!?!?!?"

b. "I am the Golden God!"

c. "Also It's my legal right as an American to post his info."

d. "We are malicious and hostile"

e. "Send us bitcoins"

f. "Wednesday night will be the doxxed next."

19. USCP TAS conducted an open source search of the .125 IP address, which revealed that the .125 IP address belonged to the open Wi-Fi network of the U.S. Senate in Washington, DC.

20. The Senate Chief Information Officer reported to USCP that the above-described activity was conducted using mobile devices which had been connected to the Senate Guest Wi-Fi network, and which had the following identifying information:

- 192.168.80.108; MAC address: C8:D0:83:99:7A:25; Apple
- 192.168.94.241; MAC address: A4:08:EA:8F:8D:25; Murata Technologies

Investigation Reveals that COSKO Is Involved in Publishing U.S. Senator 3's Restricted Personal Information on Wikipedia

21. The SOC conducted further analysis of the .136 IP address to determine the identity of the relevant user. The SOC found that the computer workstation identified as TX18DC154 had connected to Wikipedia.org during the time that U.S. Senator 3's restricted personal information was published on Wikipedia on September 27, 2018. That is, at the time that U.S. Senator 3's restricted personal information was published on Wikipedia using the .136 IP address, computer workstation TX18DC154 was connected to Wikipedia using the .136 IP address. The SOC advised USCP that they used additional "House cybersecurity tools" which allowed them to identify the actual user who was logged on to computer workstation, TX18DC154.

22. The SOC identified the user as Jackson Alexander Cosko, who the SOC confirmed was a current fellow working in the Washington DC office of U.S. Representative A, of the House of Representatives. Based on my training and experience at the USCP, I know that House of Representatives computers are password protected, and that the SOC's determination meant that the computer had been accessed by someone who possessed COSKO's user identification and password

23. The SOC advised that COSKO had logged into computer workstation TX18DC154 at 5:45:27 p.m. (Eastern), approximately nine (9) minutes before U.S. Senator 3's restricted personal information was published on Wikipedia (from the .136 IP address, which was being used by TX18DC154 at that time).

October 2: COSKO Entered the Office of U.S. Senator 7 Without Authorization

24. On October 2, 2018 at approximately 10:27 p.m., USCP Communications received a call from Witness 2, a staff member for U.S. Senator 7. Witness 2 reported that it had entered the Senator's office and observed COSKO in the Senator's office using the computer of Witness 3, another member of U.S. Senator 7's staff. Witness 2 was familiar with COSKO, and immediately recognized COSKO in U.S. Senator 7's office.

25. Witness 2 reported that COSKO was a former staff member with Senator 7's office. Witness 2 stated that COSKO'S employment with the Senator's office had ended several months ago – that is, that COSKO was asked to resign – and that COSKO did not have permission or authorization to be in the Senator's office on October 2, 2018. Similarly, COSKO did not have permission or authorization to access or use Witness 3's government-owned computer in the Senator's office (or to otherwise access Witness 3's government account) on October 2, 2018.

26. Witness 2 stated that, after Witness 2 confronted COSKO in the Senator's office, COSKO typed a few keys on the keyboard of the computer, grabbed something from the desk where the computer was located, got up, and left the office.

27. Witness 2 then examined the computer. The screen of the computer was dark. Witness 2 hit a key, or moved the computer mouse, and the screen became active. When the screen became active, Witness 2 saw that the computer was logged into Witness 3's account.

28. Shortly thereafter, Witness 3 returned to the desk and logged into the computer. Witness 3 saw that there was a web application open, that Witness 3 did not recall ever using or accessing. Witness 3 stated that it did not believe that it had ever used that particular application. Witness 3 further reported that it did not give COSKO permission to use its computer or login credentials. Based on my training and experience, and based on the above information from

Witness 2 and Witness, I believe that COSKO necessarily used Witness 3's login credentials to access the computer.

29. USCP reviewed surveillance footage that revealed that COSKO entered the northwest door of the Dirksen Senator Office Building at approximately 10:10 p.m. after being processed through security. COSKO also had a black backpack with him when he entered the building.

30. COSKO was later observed, on surveillance camera, exiting the same building entrance at approximately 10:21 p.m. (Eastern). with the same black backpack in his possession. Additional surveillance camera footage showed COSKO walking towards Union Station.

October 2: Threats and Witness Tampering

31. Witness 2 further stated that, at approximately 10:25 p.m. (Eastern) on October 2, 2018, Witness 2 received a threatening email from livefreeorpwn@gmail.com. The email was titled, "I own EVERYTHING." The body of the email stated: "If you tell anyone I will leak it all. Emails signal conversations gmails. Senators children's health information and socials." Signal is a popular messaging application which enables chats/conversations. In context, based on my training and experience, I believe that "socials" appears to be reference to social security numbers and/or other restricted personal information. Based on my training and experience, I believe that a "gmail.com" email account is operated by Google LLC, and involves the use of Google email servers that are not located in Washington, DC.

CONCLUSION

Based on all of the foregoing evidence, and based on my training and experience, I respectfully submit that there is probable cause to believe that COSKO entered the office of U.S. Senator 7 without authorization and with intent to commit a criminal offense therein, accessed the

government-owned computer (and account) of Witness 3 without authorization, used the means of identification of Witness 3 without authorization, made public the restricted personal information of U.S. Senators, and made threatening statements directed to Witness 2 with the intent to hinder, delay, or prevent Witness 2 from reporting to law enforcement, in violation of 18 U.S.C. § 119 (Making Public Restricted Personal Information), 18 U.S.C. § 875(d) (Threats in Interstate Communications), 18 U.S.C. § 1030(a)(3) (Unauthorized Access of a Government Computer), 18 U.S.C. § 1028(a)(7) (Identity Theft), 18 U.S.C. § 1512(b)(3) (Witness Tampering), D.C. Code § 22-801(b) (Second Degree Burglary), and D.C. Code § 22-3302(b) (Unlawful Entry) have been committed.

Respectfully submitted,

Jason Bell
Captain
United States Capitol Police

Subscribed and sworn to before me on October 3, 2018:

DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE
FOR THE DISTRICT OF COLUMBIA