United States Senate
WASHINGTON, DC 20510

March 1, 2021

VIA ELECTRONIC TRANSMISSION

The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security

Dear Secretary Mayorkas:

We write to request details regarding the Department of Homeland Security's response to a recently uncovered fraud case and data breach involving U.S. Citizenship and Immigration Services (USCIS) personnel at embassies in Jordan and Russia.

According to the Department of Justice, on January 26, 2021, Haitham Sad, a Jordanian citizen who formerly worked as an Immigration Assistant for USCIS at the U.S. Embassy in Amman, Jordan, pleaded guilty to conspiracy to steal U.S. government records and defraud the U.S. refugee program.[1] Mr. Sad admitted that his crimes were part of a broader fraud scheme that involved Aws Abduljabbar, an Iraqi living in Amman, and Olesya Krasilova, a Russian citizen formerly employed as an Immigration Assistant at the USCIS field office in the U.S. Embassy in Moscow.[2]

Sad and Krasilova, both of whom were employed as "foreign service nationals" or "locally employed staff" of USCIS, used their access to a State Department database called the Worldwide Refugee Admissions Processing System (WRAPS) to steal highly confidential information about U.S. refugee applicants.[3] They then sent the information to Abduljabbar in Jordan, who used the information to assist applicants who were seeking admission to the United States under the U.S. Refugee Admissions Program.[4] According to news reports, "[h]aving access to the case files from successful applications gave the fraudsters a template to help others craft their own applications, cutting out information that had sunk others and highlighting the factors that had worked in previous cases."[5] As a former chief of policy at USCIS put it, the narratives of successful applicants were repurposed for other applicants.[6]

---

[1] Department of Justice, Former U.S. Government Employee Pleads Guilty To Conspiracy To Steal U.S. Government Records and Defraud U.S. Refugee Program (January 26, 2021), available at https://www.justice.gov/usao-dc/pr/former-us-government-employee-pleads-guilty-conspiracy-steal-us-government-records-and.
[2] Signed Plea Statement of Offense, https://www.justice.gov/usao-dc/press-release/file/1360711/download at 14.
[3] *Id* at 1 and 7.
[4] *Id* at 7.
[5] Stephen Dinan, Sophisticated Insider Threat at DHS immigration agency forces pause to Iraqi refugee program, The Washington Times (February 15, 2021), available at https://www.washingtontimes.com/news/2021/feb/15/iraqi-refugee-program-paused-after-insider-threat-/.
[6] *Id.*

These data breaches appear to have continued undetected for nearly a decade. Sad stated that he worked to obtain the information from the WRAPS database for "around eight years."[7] He also admitted that he was able to access information on at least 270 Iraq cases *after* his employment by USCIS ended in January 2016.[8] Between 2016 and 2019, Krasilova allegedly accessed nearly 600 unique cases through the WRAPS system.[9] Furthermore, during a four month span between October 2018 and February 2019, Krasilova took more than 700 pieces of confidential information.[10] She emailed screenshots from her USCIS email account to her personal email account and, from there, sent them to Sad, who forwarded them to Abduljabbar. In all, Krasilova received more than $20,000 in compensation for providing the information to Sad and Abduljabbar.[11] In 2019, Krasilova also attempted to recruit other foreign service nationals working for USCIS to participate in the conspiracy, though it is unclear whether those efforts were successful.[12]

According to reports, Sad and Krasilova were able to fly beneath the radar and avoid detection for an extended period of time because, when a new version of the WRAPS system with enhanced tracking and security features was installed in 2013, the older system that did not have the security features remained active. The WRAPS system is managed by the State Department's Refugee Processing Center.[13] Sad and Krasilova continued to use the older system to access the sensitive data, and as a result, they successfully avoided detection until the older system was updated in mid-2019 with new features that exposed their illegal activities. That was approximately six years after the newer system had first been installed.[14]

This fact pattern raises many serious questions, not only because of the sensitive nature of the data stolen, but also because the theft could have seemingly been prevented by simple, common sense measures such as checking for security vulnerabilities. As members of the Judiciary Committee, we are responsible for ensuring that U.S. immigration laws, including U.S. refugee laws, are properly enforced. We must also ensure that proper safeguards are in place to prevent foreign adversaries from obtaining access to confidential government records. Accordingly, please answer the following no later than March 15, 2021.

1. Please describe the steps DHS has taken to identify individuals with ties to Mr. Aws Abduljabbar who have also applied for U.S. refugee status.

---

[7] Signed Plea Statement of Offense, https://www.justice.gov/usao-dc/press-release/file/1360711/download at 8.
[8] *Id.*
[9] *Id* at 9.
[10] *Id* at 9-10.
[11] *Id* at 10.
[12] *Id* at 12.
[13] *Id* at 4.
[14] *Id* at 5-6 and 9; *see also* Stephen Dinan, Sophisticated Insider Threat at DHS immigration agency forces pause to Iraqi refugee program, The Washington Times (February 15, 2021), available at https://www.washingtontimes.com/news/2021/feb/15/iraqi-refugee-program-paused-after-insider-threat-/.

2. If DHS has identified any such individuals, please describe the steps taken to re-evaluate those individuals' refugee applications and hold anyone accountable who knowingly provided false information or knowingly relied on stolen information when preparing their applications.

3. Please describe all steps DHS has taken to identify and notify individuals in the U.S. immigration system whose personal information may have been breached and disseminated without their consent as a result of this fraud scheme.

4. Does DHS believe there is a security risk for individuals whose information may have been breached and disseminated without their consent?

5. How many foreign service nationals or locally employed staff are currently employed by USCIS at U.S. embassies?

6. Please describe the procedures that USCIS uses to vet these individuals and ensure that they do not pose a security risk prior to making offers of employment.

7. Please describe the levels and types of access provided to foreign service nationals or locally employed staff employed by USCIS at U.S. embassies.

8. Has USCIS re-evaluated the level of access granted to foreign services nationals or locally employed staff in light of this case? Please describe any policy changes that have been considered and/or implemented as a result.

9. Were the procedures outlined in response to question 6 followed for Mr. Sad and Ms. Krasilova when they first applied to work for USCIS? Please provide copies of their original applications and records of all background checks completed prior to their offers of employment.

10. Has USCIS conducted an investigation to determine whether any other embassy personnel were involved in or aware of the fraud scheme orchestrated by Mr. Abduljabbar? If yes, please describe the results of the investigation and describe any employment actions taken as a result. If USCIS has not undertaken such an investigation, please explain why not.

11. Has USCIS conducted an investigation to determine why the original WRAPS system was not deactivated when a new system was installed in 2013?

12. Has USCIS undertaken an investigation to determine how Mr. Sad was able to continue to access the WRAPS system after he was no longer associated with USCIS? What steps has USCIS taken to ensure that former embassy employees who do not have a need for access are unable to access USCIS and State Department computer systems?

We anticipate that your written reply and most responsive documents will be unclassified. Please send all unclassified material directly to the committee. In keeping with the requirements of Executive Order 13526, if any of the responsive documents do contain classified information, please segregate all unclassified material within the classified documents, provide all unclassified information directly to the committee, and provide a classified addendum to the Office of Senate Security. Although the committee complies with all laws and regulations governing the handling of classified information, it is not bound, absent its prior agreement, by any handling restrictions.

Should you have questions, please contact Daniel Parker or Drew Robinson of Ranking Member Grassley's staff at 202-224-5225 or Seth Williford of Senator Tillis's staff at 202-224-6342. Thank you for your attention to this important matter.

Sincerely,

Charles E. Grassley
Ranking Member
Senate Judiciary Committee

Thom Tillis
Ranking Member
Subcommittee on Intellectual Property
Senate Judiciary Committee

cc:

Hon. Antony Blinken
Secretary, U.S. Department of State

Mr. Todd J. Brown
Acting Assistant Secretary, Bureau of Diplomatic Security

Ms. Tracy Renaud
Senior Official Performing the Duties of the Director, U.S. Citizenship and Immigration Services

Mr. Joseph V. Cuffari
Inspector General, U.S. Department of Homeland Security