United States Senate
WASHINGTON, DC 20510

February 22, 2018

Kevin K. McAleenan
Acting Commissioner
U.S. Customs and Border Protection
1300 Pennsylvania Ave. NW
Washington, DC 20229

Dear Mr. McAleenan:

We write to ask that U.S. Customs and Border Protection (CBP) immediately act to utilize the anti-forgery and anti-tamper features in e-Passports, which have gone unused by CBP since their implementation in 2007.

The U.S. government played a central role in the global adoption of e-Passports. These high-tech passports have smart chips—which store traveler information—and cryptographic signatures, an important security feature that verifies the validity and legitimacy of the passport and its issuing government agency. For more than a decade, the United States has required that countries on the visa-waiver list issue machine-readable e-Passports. Since 2015, the United States has further required that all visitors from countries on the visa-waiver list enter the United States with an e-Passport. Despite these efforts, CBP lacks the technical capabilities to verify e-Passport chips.

CBP has deployed e-Passport readers at many ports of entry, which CBP personnel use to download data from the smart chips in e-Passports. However, CBP does not have the software necessary to authenticate the information stored on the e-Passport chips. Specifically, CBP cannot verify the digital signatures stored on the e-Passport, which means that CBP is unable to determine if the data stored on the smart chips has been tampered with or forged. CBP has been aware of this security lapse since at least 2010, when the Government Accountability Office (GAO) released a report highlighting the gap in technology. Eight years after that publication, CBP still does not possess the technological capability to authenticate the machine-readable data in e-Passports.

It is past time for CBP to utilize the digital security features it required be built into e-Passports. To that end, we ask that you take the following steps:

1. Work with the relevant subject matter experts at the General Services Administration to determine the true cost of developing or acquiring the technical capacity to validate the digital signatures in e-Passports.
2. Develop and implement a plan to properly authenticate e-Passports by January 1, 2019.

We appreciate your prompt attention to this matter and look forward to hearing about developments to address these concerning deficiencies.

Sincerely,

Ron Wyden
United States Senator

Claire McCaskill
United States Senator