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

October 23, 2019

The Honorable Michael E. Horowitz
Chair
Council of the Inspectors General on Integrity and Efficiency
1717 H Street, NW, Suite 825
Washington, DC 20006

Dear Mr. Horowitz:

I write to ask the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to evaluate cybersecurity technologies that better protect the identity of whistleblowers.

As you know, many inspectors general operate online tip lines, through which whistleblowers can submit reports of waste, fraud and abuse. Consistent with federal cybersecurity requirements, these online tip lines use HTTPS encryption to protect whistleblower reports from interception by third parties. While the use of this industry-standard form of encryption to protect whistleblower submissions is a positive step, it still leaves sensitive information about whistleblowers vulnerable to interception. HTTPS encryption only protects the content of submissions, not internet metadata, which can reveal the computer or smartphone that visited an inspector general's website.

The U.S. government has funded the development of technologies that better protect communications metadata for more than 20 years. One of these technologies, the Tor Project, is now used by millions of people around the world each day to circumvent internet censorship and to privately browse the web. The underlying technology used by the Tor Project was originally created by the U.S. Naval Research Lab. Since then, the Tor Project has been supported by a number of different U.S. and foreign government agencies, foundations and non-profit organizations.

In recent years, dozens of news organizations have created secure whistleblowing websites, which use the Tor Project and SecureDrop, a free, open-source whistleblowing software platform maintained by the Freedom of the Press Foundation. In May, the Central Intelligence Agency also began hosting a Tor-based website to receive tips from around the world. These organizations all use the Tor Project because it protects internet metadata that would otherwise reveal to third parties which phone or computer visited a particular website.

Inspectors general depend on tips from whistleblowers to uncover waste, fraud and abuse. It is therefore vital that inspectors general follow the lead of investigative news organizations in embracing cybersecurity technologies that better protect the identity of those who take

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

significant risks to report violations of the law. Accordingly, I urge you to examine SecureDrop, the Tor Project and other similar technologies for potential use by federal inspectors general.

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

Sincerely,

Ron Wyden
United States Senator