

RON WYDEN, OREGON, CHAIRMAN

DEBBIE STABENOW, MICHIGAN	MIKE CRAPO, IDAHO
MARIA CANTWELL, WASHINGTON	CHUCK GRASSLEY, IOWA
ROBERT MENENDEZ, NEW JERSEY	JOHN CORNYN, TEXAS
THOMAS R. CARPER, DELAWARE	JOHN THUNE, SOUTH DAKOTA
BENJAMIN L. CARDIN, MARYLAND	RICHARD BURR, NORTH CAROLINA
SHERROD BROWN, OHIO	ROB PORTMAN, OHIO
MICHAEL F. BENNET, COLORADO	PATRICK J. TOOMEY, PENNSYLVANIA
ROBERT P. CASEY, JR., PENNSYLVANIA	TIM SCOTT, SOUTH CAROLINA
MARK R. WARNER, VIRGINIA	BILL CASSIDY, LOUISIANA
SHELDON WHITEHOUSE, RHODE ISLAND	JAMES LANKFORD, OKLAHOMA
MAGGIE HASSAN, NEW HAMPSHIRE	STEVE DAINES, MONTANA
CATHERINE CORTEZ MASTO, NEVADA	TODD YOUNG, INDIANA
ELIZABETH WARREN, MASSACHUSETTS	BEN SASSE, NEBRASKA
	JOHN BARRASSO, WYOMING

JOSHUA SHEINKMAN, STAFF DIRECTOR
GREGG RICHARD, REPUBLICAN STAFF DIRECTOR

United States Senate

COMMITTEE ON FINANCE

WASHINGTON, DC 20510-6200

December 1, 2021

The Honorable Charles P. Rettig
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Rettig:

We are writing regarding the series of articles published by the website ProPublica that appear to be based on confidential taxpayer information that potentially was leaked or hacked from the Internal Revenue Service (IRS). On June 8, 2021, ProPublica published, “The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax.”¹ This was the first in a series of articles that ProPublica continues to publish with no indication that any progress has been made by any federal agency regarding identification of the source or sources of the taxpayer information. Despite clear and ongoing evidence of a threat of a data breach, in response to a letter sent to you by Senators Grassley and Crapo, you responded in part that “We do not yet know whether there has been a data breach or a threat of a data breach.” Your letter of September 13, 2021, also notes that “We do not yet have any information concerning the source of the alleged taxpayer information published by ProPublica.”

These responses are very troubling, particularly because ProPublica continues to publish what appears to be confidential taxpayer information that is protected by law, and as Commissioner, you have been a proponent of the IRS being allowed access to even more information from taxpayers and a significant and mandatory enforcement budget.² The fact that the source of the information ProPublica continues to publish remains unknown means that the ability of the IRS to safeguard information already entrusted to it also remains unknown. It is possible that ProPublica obtained whatever information it has at one time from a specific source. However, if the ProPublica information was leaked or hacked from the IRS, and the IRS is unable to even determine if a leak or hack took place, this could indicate an ongoing and

¹ “The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax,” ProPublica, June 8, 2021, at <https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax>.

² Franck, Thomas, “IRS chief tells Elizabeth Warren: More transparent bank data can fight tax evasion,” CNBC, September 2, 2021, at <https://www.cnbc.com/2021/09/02/irs-chief-tells-elizabeth-warren-bank-data-can-help-fight-tax-evasion.html>.

persistent problem with IRS information technology (IT) systems and the ability of the IRS to safeguard taxpayer information.

IRS Systems Are Notoriously Ineffective

Even before ProPublica began publishing articles utilizing taxpayer information, significant issues with IRS IT systems were well documented. In fact, the struggles of the IRS to modernize IT systems is something of an old chestnut in tax policy circles. Aside from a reliance on COBOL which is referred to as “geriatric code,” it is also reported that the “IRS main software “Master File” was developed in 1962 and uses nine-track tape for data storage. None of the IRS programs have ever been that well coordinated.”³ In written testimony delivered before the Subcommittee on Government Operations of the House Committee on Oversight and Reform on October 7, 2020, the Government Accountability Office (GAO) Director of Information Technology and Cybersecurity stated the following:

In May 2020, GAO reported that new and continuing deficiencies in information system security controls over financial and tax processing systems included deficiencies related to access controls, segregation of duties, and other areas. These collectively represented a significant deficiency in risks of unauthorized access to, modification of, or disclosure of financial reporting and taxpayer data and disruption of critical operations.⁴

In a recent audit, GAO also “identified new information system control deficiencies related to access controls and security management that contributed to IRS’s continuing significant deficiency in its internal control over financial reporting systems.”⁵ When this report was published in May 2021, there were a total of 120 open recommendations to the IRS with 96 of those recommendations falling within the audit area of information systems.⁶ Among the open recommendations, GAO “identified one deficiency in access controls related to cryptography (i.e., encryption).”⁷ Specifically, “IRS did not enforce cryptographic protocols used for authentication and data integrity in a system environment that processes taxpayer data in accordance with agency policy and National Institute of Standards and Technology guidance.”⁸

GAO is not the only oversight entity that has recently identified IRS deficiencies with encryption of taxpayer data. On September 27, 2021, the Treasury Inspector General for Tax Administration (TIGTA) issued a report titled, “The Data at Rest Encryption Program Has Made

³ Vaughan-Nichols, Steven, J., “Where’s my check? COBOL’s role in delay of stimulus and unemployment payments,” ZDNet, April 20, 2020, at <https://www.zdnet.com/article/wheres-my-check-cobol-unemployment-and-taxes/>.

⁴ GAO, “Information Technology, IRS Needs to Address Operational Challenges and Opportunities to Improve Management,” GAO-21-178T, Washington, DC, October 7, 2020, at <https://www.gao.gov/products/gao-21-178t>.

⁵ GAO, “Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls, GAO-21-401R, Washington, DC, May 4, 2021, at <https://www.gao.gov/products/gao-21-401r>.

⁶ Id

⁷ Id

⁸ Id

Progress With Identifying Encryption Solutions, but Project Management Needs Improvement.”⁹ The report notes that “[t]he IRS has made progress to identify and test encryption and key management solutions for use with certain types of systems. However, it *has not deployed this technology*.”¹⁰ The protection of the vast amounts of taxpayer information collected and maintained by the IRS is critical to maintaining a basic level of confidence in the fair application and enforcement of our nation’s tax laws. We believe many taxpayers would be shocked that the IRS has not already implemented a functioning system for protecting the information stored on its systems. According to the IRS, more than 167 million individual income tax returns had been filed by the week ending October 22, 2021, for the 2021 filing season.¹¹

More recently, in a September 28, 2021 report on IRS information security modernization, TIGTA reported on ineffectiveness of risk management. TIGTA concluded that:

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA [Federal Information Security Modernization Act] requirements, taxpayer data could be vulnerable to *inappropriate and undetected use, modification, or disclosure*.¹²

IRS Contractor Relationships Introduce Additional Security Vulnerabilities

The IRS’s relationships with contractors represent an additional vulnerability to the security of IRS systems. Private contractors serve a vital role in helping the IRS efficiently perform its duties, which makes it vitally important adequate security measures are in place.

For example, TIGTA has previously recommended that the IRS implement end-to-end encryption in transferring taxpayer data to Private Collection Agencies (PCAs).¹³ The IRS utilizes PCAs as part of a very successful program to pursue and collect tax debt that the IRS has elected not to pursue. It is important that any taxpayer information that is transferred as part of this program is fully protected against unauthorized access and disclosure. The September 27, 2021 TIGTA report notes that “the IRS verified the taxpayer information was being encrypted through e-mail verification with the PCAs.”¹⁴ However, the IRS dropped the ball on its end. According to TIGTA, “PCA information residing at the IRS had not been encrypted in the production environment.”¹⁵

⁹ TIGTA, “The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement,” September 27, 2021, Report Number: 2021-20-066, at <https://www.treasury.gov/tigta/auditreports/2021reports/202120066fr.pdf>.

¹⁰ TIGTA, “The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement,” September 27, 2021, Report Number: 2021-20-066, at <https://www.treasury.gov/tigta/auditreports/2021reports/202120066fr.pdf> (emphasis added).

¹¹ IRS, Filing Season Statistics for Week Ending October 22, 2021, at <https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-october-22-2021>.

¹² TIGTA, “Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation,” Report Number: 2021-20-072, Washington DC, September 28, 2021, at <https://www.treasury.gov/tigta/auditreports/2021reports/202120072fr.pdf> (emphasis added).

¹³ TIGTA, “Private Collection Agency Security Over Taxpayer Data Needs Improvement,” July 30, 2018, Report No. 2018-20-039, at <https://www.treasury.gov/tigta/auditreports/2018reports/201820039fr.pdf>.

¹⁴ Id

¹⁵ Id

Moreover, the TIGTA report raises questions about any other contractors the IRS has allowed to access taxpayer information. For example, a 2018 article published by Bloomberg Tax describes how “[a] contract with ... Palantir Technologies will give the IRS new firepower to pursue tax cheats by connecting the dots in millions of tax filings, bank transactions, phone records, and even social media posts.”¹⁶ In reporting on an earlier contract with Palantir, the story notes that in 2013 the IRS “spent \$30.8 million on a five-year contract with 13 Federal LLC, a Palantir subsidiary, and granted it access to files for more than 1 million people, according to a privacy audit report.”¹⁷ No doubt these contractors do important work that facilitates the fair and effective working of our federal tax system. However, this is a massive amount of taxpayer information. And it is critical that the IRS ensure contractors are complying with their obligation to safeguard it. These requirements are documented in IRS Publication 4812, Contractor Security & Privacy Controls. In part, this publication requires that

Contractors and subcontractors shall have adequate programs in place to protect the information received from unauthorized use, access, and disclosure. The contractor’s programs for protecting information received must include documented notification to employees and subcontractors (at any tier) regarding, the importance of protecting returns and return information.¹⁸

IRS is Expanding Private Data Acquisitions and Requesting Unprecedented Funding

In a contract that may have been finalized by Treasury and the IRS with Babel Street, Inc., the IRS seeks “a third-party digital media search and reporting solution that captures information from public facing digital media records that can be used in taxpayer compliance and tax administration cases.”¹⁹ Such data apparently will be obtained for the IRS by artificial intelligence (AI)-enabled software that scrubs the internet for information on taxpayers, including current and historical publicly posted communications, images, videos, and cached pages of those taxpayers. The “solution,” according to a solicitation/contract order by Treasury to Babel Street, Inc. is supposed to provide: “Secure access to publicly available information without posing a security and public policy perception risk.”

Gathering troves of taxpayer information from anywhere it can possibly be found by AI algorithmic robots should be counted as a public policy perception risk in and of itself. Having the IRS gather such information to combine with troves of personal taxpayer information already possessed by the IRS amplifies our concerns about data security in IRS systems.

The IRS appears to be expanding its collection of information on taxpayers to house it in systems with known security deficiencies and shortfalls. Meanwhile, the IRS and Treasury are advocating for an unprecedented, nearly \$80 billion, amount of mandatory funding from general

¹⁶ “Palantir Deal May Make IRS ‘Big Brotherish’ While Chasing Cheats” Bloomberg Tax, November 15, 2018, at [Palantir Deal May Make IRS ‘Big Brother-ish’ While Chasing Cheats \(bloombergtax.com\)](https://www.bloombergtax.com).

¹⁷ Id

¹⁸ U.S. Department of the Treasury, Internal Revenue Service. Contractor Security & Privacy Controls. IRS Pub 4812, at [Publication 4812 \(Rev. 11-2021\) \(irs.gov\)](https://www.irs.gov/publications/pub4812).

¹⁹ See Contract No. 2032H8-21-C-00039 at https://s3.documentcloud.org/documents/21098526/babel-street-irs_redacted.pdf.

taxpayer resources. In the funding scheme being advocated, the IRS is to be provided with a mandatory stream of \$80 billion, *after which* the IRS would report to Congress on how it plans to use the funds—that is; fund now, plan later. Such a scheme, in the face of ongoing alleged privacy leaks of what appear to be IRS information, the source(s) of which no federal agency appears to have any knowledge, and in the face of known serious deficiencies in IRS data protections, defines irresponsibility.

As we enter month six with no information about how ProPublica obtained protected taxpayer information, the risks we highlighted in this letter are of growing concern. It is our constitutional obligation to ensure that IRS enforcement remains effective, and that requires the IRS to properly secure taxpayer information. Accordingly, we request responses to the following questions by December 15, 2021.

1. Do you have any update regarding the responses provided to Senators Grassley and Crapo in your letter of September 13, 2021, where you stated you did “not yet know whether there has been a data breach or a threat of a data breach,” and did “not yet have any information concerning the source of the alleged taxpayer information published by ProPublica”?
2. How many full-time equivalent employees have been tasked to determine whether or not IRS data and systems have been compromised in any way, such as through a leak or hack, since the publication of articles by ProPublica in June of 2021?
3. What is the status of the IRS’s efforts to resolve the 120 open GAO recommendations—particularly the recommendations relating to information systems, that are noted in the May 4, 2021, GAO publication “Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls?”
 - a. What is the timeline for ensuring that the IRS resolves all recommendations?
4. What is the status of the IRS’s efforts to resolve the deficiency related to encryption identified in GAO’s May 4 report as well as to fully comply with the recommendations made by TIGTA in the September 2021, report on data at rest encryption?
5. In a “Management’s Response” provided in response to a TIGTA recommendation to encrypt taxpayer data before it is provided to PCAs, the IRS notes that it “will implement a solution that will ensure that data at rest is encrypted prior to being transferred from the IRS to PCAs.”
 - a. How many contractors of any type, not just PCAs, has the IRS provided taxpayer information to that has not been encrypted over the past year and the past 10 years?
 - b. How is the IRS transmitting the data and what safeguards are used to ensure taxpayer data is subject to all the protections afforded by law?

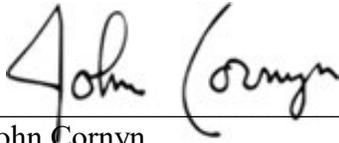
6. How many contractors does the IRS have active contracts with that involve the sharing of protected taxpayer information and how many contracts have involved sharing of taxpayer information over the past 10 years?
7. Please identify the holders of all contracts and sub-contracts over the past 10 years where protected taxpayer information has been transmitted outside the IRS or access granted to individuals employed by a contractor or sub-contractor.
8. Of taxpayer information provided to contractors, IRS Publication 4812 requires that “Contractors and subcontractors shall have adequate programs in place to protect the information received from unauthorized use, access, and disclosure.”
 - a. Please provide examples of any contract language that the IRS requires contractors to agree to that concerns the protection of taxpayer information.
 - b. How does the IRS monitor compliance with the requirements of IRS Publication 4812 and how often does it confirm compliance?
 - c. Does the IRS require that all contractors maintain activity logs that detail all instances of contractor employee access to taxpayer information?
 - d. Does the IRS have regular access to activity logs maintained by contractors or do they need to be specifically requested?
 - e. Is the IRS aware of the unauthorized use, access, or disclosure of taxpayer information, by any contractor, sub-contractor, or employee over the past 10 years? Please break down incidents by contractor self-reported incidents and incidents detected by the IRS or TIGTA.
9. Several of the stories published by ProPublica disclose taxpayer information of specific taxpayers. Has the IRS examined data held by the IRS on those specific taxpayers and determined the full universe of individuals, including IRS employees, contractors and sub-contractors that have potentially been able to access that information?
10. Why does the IRS need data from AI-enabled programs and algorithms that scrape data from the internet about taxpayers? What protections will the IRS put in place to ensure that whatever troves of such data are aggregated to analyze and profile an individual, they will be secure and fully protected from release and will not be used for any improper targeting efforts by the IRS?
11. Out of \$44.9 billion requested in the partisan Build Back Better bill for IRS enforcement, to include funds for, inter alia, “investigative technology” and “digital asset monitoring and compliance activities,” how much would the IRS plan to use on additional digital surveillance of taxpayers, and for what reasons?

Thank you for your attention to these important matters.

Sincerely,



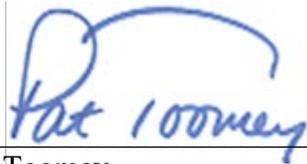
Mike Crapo
U.S. Senator



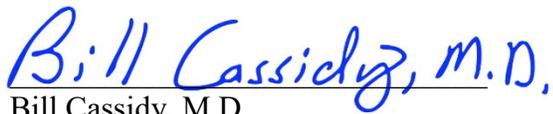
John Cornyn
U.S. Senator



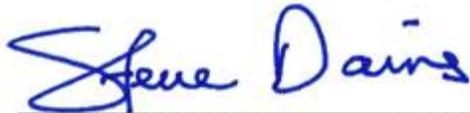
Richard Burr
U.S. Senator



Pat Toomey
U.S. Senator



Bill Cassidy, M.D.
U.S. Senator



Steve Daines
U.S. Senator



Ben Sasse
U.S. Senator



Charles E. Grassley
U.S. Senator



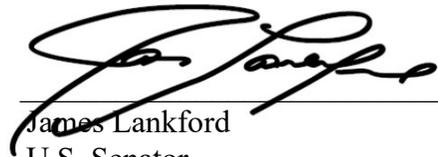
John Thune
U.S. Senator



Rob Portman
U.S. Senator



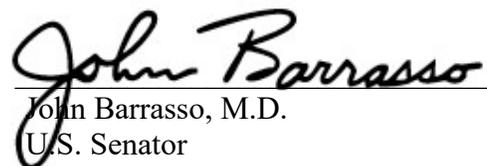
Tim Scott
U.S. Senator



James Lankford
U.S. Senator



Todd Young
U.S. Senator



John Barrasso, M.D.
U.S. Senator