Congress of the United States
House of Representatives
Washington, D.C. 20515

April 7, 2025

The Honorable Russell Vought
Director
Office of Management and Budget
725 17th Street NW
Washington, DC 20503

Dear Director Vought:

We write to urge you to use the existing authorities of the Office of Management and Budget (OMB) to address the burdensome and conflicting cyber regulatory landscape. There is ample evidence that cybersecurity regulatory compliance is unnecessarily sprawling and resource-intensive. The Cybersecurity and Infrastructure Security Agency (CISA) estimates there are more than three dozen federal requirements for cyber incident reporting alone—a number that does not capture specific state, local, Tribal, territorial, or international requirements.[1]

The resources required for regulated entities to comply are immense. For example, a proposed change to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule aimed to improve cybersecurity would cost regulated entities and health-plan sponsors an astounding $9 billion combined in just the first year.[2] According to testimony before the Subcommittee on Cybersecurity and Infrastructure Protection, "bank Chief Information Security Officers [CISOs] now spend 30-50 percent of their time on compliance and examiner management. The cyber teams they oversee spend as much as 70 percent of their time on those same functions."[3] Additionally, a quarter of the requests for information banks receive are duplicative, uncoordinated agency requests.[4] Again, in testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, an energy sector witness explained "managing compliance obligations with disparate regulations and across agencies may in fact harm the cybersecurity posture of organizations, particularly where limited resources are allocated to compliance activities over managing risk, maturing capabilities, and creating effective security programs."[5]

---

[1] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 FR 23644, Apr. 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.
[2] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 FR 898, Jan. 6, 2025, https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information.
[3] "Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime", 119th Cong. (2025), Testimony of Heather Hogsett, https://bpi.com/wp-content/uploads/2025/03/Testimony-of-Heather-Hogsett-Regulatory-Harm-or-Harmonization-Examining-the-Opportunity-to-Improve-the-Cyber-Regulatory-Regime.pdf.
[4] *Id.*
[5] "Enhancing Cybersecurity by Eliminating Inconsistent Regulations", 118th Cong. (2024), Testimony of Maggie O'Connell, https://oversight.house.gov/wp-content/uploads/2024/07/OConnell-Testimony.pdf.

Such oppressive requirements force entities of all sizes to choose between spending precious resources on security or on compliance. This unnecessary tradeoff puts entities at risk. The U.S. cyber regulatory regime should facilitate valuable and actionable information sharing that reinforces the security measures companies undertake to defend against, and respond to, cyber incidents. As nation-state and criminal actors increasingly target U.S. networks and critical infrastructure in cyberspace, we can no longer allow compliance burdens to hinder the agility of U.S.-based companies to respond to threats in a timely manner.

Compliance burdens imposed on companies can be reduced by streamlining cybersecurity requirements, which multiple stakeholders have testified as being unnecessarily duplicative.[6] For example, in 2020, four federal agencies established cybersecurity requirements for states aimed at securing data. According to the U.S. Government Accountability Office (GAO), the percentage of conflicting parameters for these requirements ranged from 49 to 79 percent.[7] Entities subject to these requirements should not bear the brunt of the federal government's lack of coordination.

For several years, Congress has recognized the importance of streamlining cybersecurity requirements and took steps to address it. In 2022, Congress passed the bipartisan Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which required CISA to develop a new regulation to set the standard for cyber incident reporting.[8] Additionally, the Streamlining Federal Cybersecurity Regulations Act introduced in both the Senate and House in the 118th Congress establishes an interagency committee within the Office of the National Cyber Director (ONCD) to harmonize regulatory regimes.[9] However, CISA's proposed CIRCIA rule, if enacted as written, undermines Congressional intent by imposing another layer of duplication by increasing compliance costs and capturing more entities than envisioned by lawmakers.[10]

As the agency tasked with overseeing regulations across the federal government, we recognize the crucial role OMB can and will play in improving our nation's cyber posture. Therefore, we urge OMB to act now by prioritizing the review of existing and future federal cyber regulations. OMB, in coordination with ONCD and CISA, must thoroughly examine the existing cyber regulatory landscape for duplication and redundancy across the federal government, and identify opportunities for reciprocity within and between agencies.

---

[6] *See* "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking", 118th Cong. (2024). and "Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime", 119th Cong. (2025).

[7] "Efforts Initiated to Harmonize Regulations, but Significant Work Remains", U.S. Government Accountability Office, Testimony of David B. Hinchman before the U.S. Homeland Security and Government Affairs Committee of the U.S. Senate, June 5, 2024, https://www.gao.gov/assets/gao-24-107602.pdf.

[8] Text - H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022. (2022, March 15). https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[9] Text - S.4630 - 118th Congress (2023-2024): Streamlining Federal Cybersecurity Regulations Act. (2024, December 2). https://www.congress.gov/bill/118th-congress/senate-bill/4630/text.

[10] Congressman Andrew R. Garbarino, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 FR 23644, Apr. 4, 2024, https://www.regulations.gov/comment/CISA-2022-0010-0464.

Specifically, OMB could use existing authority granted under Executive Order (EO) 12866: Regulatory Planning and Review. This EO enables OMB's Office of Information and Regulatory Affairs (OIRA) to periodically review existing significant regulations[11] "to confirm that regulations are both compatible with each other and not duplicative or inappropriately burdensome in the aggregate."[12] The process set forth in EO 12866 has spanned administrations,[13] and forms the basis of two EOs issued by President Trump.[14] Additionally, in line with President Trump's 10-to-1 deregulation initiative,[15] OMB must not issue any new cyber regulations without repealing at least ten existing rules and ensuring the net total cost of new and repealed regulation are less than zero.

As Congress continues its work to streamline cyber regulations, we urge OMB to take these steps to rein in the cyber regulatory landscape to dramatically improve the security and resiliency of U.S. networks and critical infrastructure. Eliminating the duplicative landscape of cyber regulations is the fastest, most cost-effective way to materially improve the nation's cybersecurity.

To support Congress's continued efforts to streamline cyber regulations and the oversight responsibilities of our Committees over issues related to cybersecurity and regulatory matters, including the identification of any legal barriers that Congress must address through legislation, we request a briefing on OMB's plans to streamline cyber regulations by April 28, 2025.

Per Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security." Additionally, under House Rule X, the Committee on Oversight and Government Reform is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time".

---

[11] A "significant regulatory action" is defined by EO 12866 as "any regulatory action that is likely to result in a rule that may: (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order."

[12] Exec. Order No. 12866, Regulatory Planning and Review, 58 FR 51735, Sept. 30, 1993, https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf.

[13] Office of Management and Budget (OMB): An Overview. (2025, March 23). https://www.congress.gov/crs-product/RS21665.

[14] *See* Exec. Order No. 13771, Reducing Regulation and Controlling Regulatory Costs (2017) and Exec. Order No. 14192, Unleashing Prosperity Through Deregulation (2025).

[15] "Fact Sheet: President Donald J. Trump Launches Massive 10-to-1 Deregulation Initiative", The White House, Jan. 31, 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-launches-massive-10-to-1-deregulation-initiative/.

We appreciate your prompt attention to this matter and look forward to working with you to enhance our nation's cyber resiliency and security.

Sincerely,

MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security

JAMES COMER
Chairman
Committee on Oversight and Government Reform

CLAY HIGGINS
Chairman
Subcommittee on Federal Law Enforcement

NANCY MACE
Chairwoman
Subcommittee on Cybersecurity, Information Technology, and Government Innovation

ANDY BIGGS
Member of Congress
Committee on Oversight and Government Reform