May 12, 2025

The Honorable Russell T. Vought
Director
Office of Management and Budget
Executive Office of the President
725 17th Street, NW
Washington, DC 20503

Subject: Response to OMB Request for Information on Deregulation

Director Vought,

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the Office of Management and Budget's (OMB) Request for Information (RFI) regarding deregulatory actions aimed at reducing unnecessary burdens while promoting innovation, economic growth, and public welfare. ITI is the premier global trade association for the technology sector, representing the world's leading innovation companies. Our members design and manufacture hardware, develop software and services, and provide the digital infrastructure that underpins the modern economy.

We commend the Administration's efforts to identify opportunities to modernize regulatory frameworks in ways that enhance competitiveness, lower compliance costs, and accelerate the deployment of emerging technologies. In that spirit, we offer targeted recommendations to reform, streamline, or clarify several current laws, regulations, and government programs that have broad implications for innovation, investment, and economic resilience. To guide OMB's review, our response is organized by topics of critical importance to the technology industry, including cybersecurity, semiconductors, and telecommunications. Within each topic, we identify specific regulations or programs that warrant reevaluation or amendment, provide background on their impact, and explain the reasons why reforms would reduce unnecessary burdens while promoting innovation, economic resilience, and national security. This structure reflects the breadth of ITI's membership and the cross-cutting nature of today's technology landscape.

1. ***Cybersecurity related regulations***

a. *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*

- **Agency:** CISA
- **Title/Section of CFR to be rescinded:** 6 CFR Part 226 [Docket No. CISA-2022-0010] RIN 1670-AA04.
- **Rule Type:** Proposed Rule
- **Name of Regulation/Program Being Rescinded:** Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.

- **Justification:** ITI supports the **consolidation and harmonization** of federal cyber incident reporting requirements under CIRCIA. However, ITI strongly emphasizes that **this is not a call to rescind or nullify CIRCIA itself**. Rather, ITI advocates for:
    - **Reciprocity**: A report submitted under CIRCIA should suffice for compliance with all other federal cyber incident reporting regulations.
    - **Revision**: CIRCIA should be revised to address overbroad elements, especially regarding the definition and scope of covered entities and incidents, and its failure to recognize "substantially similar" regulations for reciprocity.
    - **Regulatory Streamlining**: The Office of Management and Budget (OMB) should rescind duplicative or redundant cyber incident reporting mandates where CIRCIA already applies.

  The 2023 CIRC report summarizes the many problems associated with the fragmented and duplicative incident reporting landscape in the U.S. Domestic and international efforts need to be streamlined and consolidated under CIRCIA to improve security outcomes, reduce compliance burdens, and increase operational clarity.
- **Agency Contact Information:** Cybersecurity and Infrastructure Security Agency 1110 N. Glebe Rd. Arlington, VA 20598-0630 1-844-Say-CISA or email SayCISA@cisa.dhs.gov.
- **Background for the Regulation Being Rescinded:** In 2023, the Cybersecurity Incident Reporting Council (CIRC) released a detailed report summarizing the fragmented incident reporting landscape. The report provides actionable recommendations to streamline cybersecurity incident reporting in the U.S. The report is available at: Harmonization of Cyber Incident Reporting to the Federal Government. Additionally, ITI developed a set of global incident reporting principles. We recommend that consolidation efforts under CIRCIA adhere to these principles, particularly regarding the initial 72-hour reporting timeline and limiting scope to confirmed incidents of substance. ITI's principles are available at: ITI Global Policy Principles - Security Incident Reporting. To further inform harmonization efforts, ITI published a Global Cyber Incident Reporting Policy Index cataloguing key international reporting regimes: ITI Global Cybersecurity Incident Reporting Policy Index. Finally, ITI submitted comments on the proposed CIRCIA rule identifying specific recommendations for improvement: ITI CIRCIA NPRM Response.
- **Additional Recommendation – Definitional Consistency:** Definitional consistency across cybersecurity regulations is a critical element of harmonization. Currently, the definition of "cybersecurity incident" varies significantly across federal regulations, creating confusion and unnecessary compliance costs for businesses. For instance, OMB M-17-12 defines a cybersecurity incident broadly to include occurrences that "actually or imminently jeopardize" systems, whereas CIRCIA defines incidents more narrowly, focusing solely on actual jeopardy. Similarly, TSA's Security Directive Pipeline-2021-01B and sector-specific rules under the FTC Safeguards Act, HIPAA, ISO 27000, and NYDFS Cybersecurity Regulation adopt varying, and at times conflicting, definitions. We recommend that a standardized definition be adopted across all relevant regulations, preferably aligned with longstanding and internationally recognized standards, such as those developed by NIST. While sector-specific needs may necessitate additional reporting categories (e.g., tracking near-misses or attempted intrusions), such categories should be clearly delineated and not conflated with confirmed cybersecurity incidents. A uniform baseline definition will reduce ambiguity,

facilitate compliance, and enhance the quality of information reported to federal agencies.

- **Explain Reasons for the Rescission:** The fragmentation of cybersecurity governance and compliance regimes impedes security outcomes and should be avoided both domestically and internationally. Proliferating governance regimes targeting the same technologies—but with inconsistent, contradictory, or duplicative requirements—diverts critical resources away from actual security improvements toward burdensome compliance activities. The resulting inefficiencies undermine private sector innovation, increase costs for consumers, and weaken national and economic security. A harmonized, risk-based, and streamlined reporting framework under CIRCIA, incorporating definitional consistency, would better serve both government and industry objectives.
- **Text of Relevant Statutory Authority:** Federal Register - Cyber Incident Reporting for Critical Infrastructure Act CIRCIA Reporting Requirements
- **Name of Agency Head:** Sean Plankey (nominated)
- **Title of Agency Head:** Director of CISA (nominated)

b. *Defense Federal Acquisition Regulation Supplement: Disclosure of Information Regarding Foreign Obligations*

- **Agency**: Department of Defense
- **Title/Section of CFR to be rescinded**: DFARS Case 2018–D064 Disclosure of Information Regarding Foreign Obligations
- **Rule Type**: Proposed Rule
- **Name of Regulation/Program Being Rescinded**: Defense Federal Acquisition Regulation Supplement: Disclosure of Information Regarding Foreign Obligations
- **Justification**: The Rule proposes Sections 252.239-70YY and 252.239-70ZZ to implement the disclosures required by Section 1655(a) of the National Defense Authorization Act (NDAA) for Fiscal Year 2019 for offerors and contractors, respectively. In doing so, the proposed regulatory language exceeds the legislative requirements—and thereby DoD's delegated authority—by expanding the scope of the disclosure requirements to scenarios that were not intended to be covered by the underlying legislation.
- **Background for the Regulation Being Rescinded**: The proposed rule significantly exceeds the statutorily mandated requirements. This puts up unnecessary yet harmful barriers for any contractor seeking to do business with the Department of Defense. A detailed breakdown of our concerns can be found here: https://www.itic.org/dotAsset/27799595-c0c6-46bf-ab75-c6c57607b437.pdf In short, Sec. 1655 delineates different disclosure requirements for commercial and non-commercial products, whereas the proposed Rule conflates the disclosure requirements for non-commercial products and commercial products as defined in Sec. 1655(a)(1) and Sec. 1655(a)(2) respectively. This expands the scope of covered products, systems, and services unjustifiably. COTS products are intended for broad use by commercial entities and are not exclusively designed for government use cases. Subjecting effectively all products produced by the defense industrial base to these disclosure requirements will create countless false positives. Simultaneously, it will

raise the barriers to market entry and exacerbate the current decline in innovative market participants. This erases any benefit to risk management, contradicts the Department's objective to build and foster a resilient and innovative defense industrial base, reduces operational efficiency and complicates successful mission delivery.

- **Explain Reasons for the Rescission**: The decision to consider commercial products as in scope for all disclosures in the Rule is contrary to the statutory text. Sec. 1655(a)(1) explicitly limits disclosure requirements to non-commercial products, systems, and services developed for the Department. Consequently, the regulatory implementation of Sec. 1655(a)(1) must not apply to any commercial products, including COTS. As proposed, Sections 252.239-70YY(c)(1)(i) and 252.239-70ZZ(c)(1)(i) would expand the scope of disclosures pursuant to Sec. 1655(a)(1) from "non-commercial products" to "any product, system, or service that DoD is using or intends to use." However, the underlying statute does not support such a scope expansion. We urge the Department to limit the disclosure requirements pursuant to Sec. 1655(a)(1) to non-commercial products, systems, and services as was intended by Congress.
- **Text of Relevant Statutory Authority**: https://www.federalregister.gov/documents/2024/11/15/2024-26058/defense-federal-acquisition-regulation-supplement-disclosure-of-information-regarding-foreign
- **Name of Agency Head**: Pete Hegseth
- **Title of Agency Head**: Secretary of Defense

c. *Cyber Threat and Incident Reporting and Information Sharing and Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems*

- **Agency**: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).
- **Title/Section of CFR to be rescinded**: 48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 39, and 52 [FAR Case 2021-017; Docket No. FAR-2021-0017; Sequence No. 1] RIN 9000-AO34 and 48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 37, 39 and 52 [FAR Case 2021-019; Docket No. FAR-2021-0019; Sequence No. 1] RIN 9000-AO35.
- **Rule Type**: Proposed Rules
- **Name of Regulation/Program Being Rescinded**: Cyber Threat and Incident Reporting and Information Sharing and Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems.
- **Justification**: The Cases lack proportionality in the type and breadth of access that they establish which are not proportionate to the risk, impact, and scope of the triggering event. Details can be found here: https://iticdc.sharepoint.com/:b:/s/PublicSectorInternal/EWC7oXuW0jJMhlxS_-APKw4Bwuy3YAe5g8G5nu46JfPrxA?e=zTYEeJ.
- **Agency Contact Information**: Call 1-800-488-3111. Email ncsccustomer.service@gsa.gov.
- **Background for the Regulation Being Rescinded**: The two proposed rules were opened in response to EO 14028. While both rules contain good elements, there are also a number of elements that are concerning to industry. Relating to both cases, problematic measure include the scope of federal access rights, the applicability to commercial and COTS products, requirement flow down, the applicability to new

solicitations, funding, and definitions. Related to FAR Case 2021-017, we see opportunity to adjust the guidance around regulatory harmonization, Software Bills of Materials (SBOMs), and the IPv6 requirements. Lastly, FAR Case 2021-019 can be improved by amending the sections on data localization, the expansion of FAR Part 39, indemnification, the need for federated single sign on, the unique administrative account requirements, FedRAMP, non-cloud FIS, and government-related data issues. We summarize our specific concerns and recommendations here: https://iticdc.sharepoint.com/:b:/s/PublicSectorInternal/EWC7oXuW0jJMhlxS_-APKw4Bwuy3YAe5g8G5nu46JfPrxA?e=zTYEeJ

- **Explain Reasons for the Rescission**: The two proposed rules were opened in response to EO 14028. While both rules contain good elements, there are also a number of elements that are concerning to industry. Relating to both cases, problematic measure include the scope of federal access rights, the applicability to commercial and COTS products, requirement flow down, the applicability to new solicitations, funding, and definitions. Related to FAR Case 2021-017, we see opportunity to adjust the guidance around regulatory harmonization, Software Bills of Materials (SBOMs), and the IPv6 requirements. Lastly, FAR Case 2021-019 can be improved by amending the sections on data localization, the expansion of FAR Part 39, indemnification, the need for federated single sign on, the unique administrative account requirements, FedRAMP, non-cloud FIS, and government-related data issues. We summarize our specific concerns and recommendations here: https://iticdc.sharepoint.com/:b:/s/PublicSectorInternal/EWC7oXuW0jJMhlxS_-APKw4Bwuy3YAe5g8G5nu46JfPrxA?e=zTYEeJ
- **Text of Relevant Statutory Authority**: https://www.federalregister.gov/documents/2023/11/01/2023-24025/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing-extension https://www.federalregister.gov/documents/2023/10/03/2023-21327/federal-acquisition-regulation-standardizing-cybersecurity-requirements-for-unclassified-federal
- **Name of Agency Head**: Stephen Ehikian
- **Title of Agency Head**: Acting Administrator, GSA

d. *Federal Acquisition Security Council Rule*

- **Agency**: Federal Acquisition Security Council (FASC)
- **Title/Section of CFR to be rescinded**: 41 CFR Parts 201 and 201-1
- **Rule Type**: Final Rule
- **Name of Regulation/Program Being Rescinded**: Federal Acquisition Security Council Rule
- **Justification**: This rule should not be rescinded. Instead, all government-wide supply chain risk management policy should be realigned under the Federal Acquisition Security Council (FASC).
- **Background for the Regulation Being Rescinded**: The FASC was established in the 2018 SECURE Technology Act for the purpose of bringing supply chain and cybersecurity experts throughout the government together to address supply chain risks posed

throughout the government acquisition process. The FASC is chaired by a designate from the U.S. Office of Management and Budget (OMB), and seven executive branch agencies are represented in its membership. The SECURE Technology Act also directs the FASC to work closely with industry in developing governmentwide supply chain risk management guidance. ITI recommends that the SECURE Technology Act supersede any other identified SCRM policy that seeks to exclude or remove a source from government networks (including Sec. 889 of the FY19 NDAA, Sec. 1656 of the FY18 NDAA, Sec. 851 of the FY22 NDAA, and Sec. 5949 of the FY23 NDAA) and that the FASC be the sole entity responsible for maintaining a list of problematic or banned ICT equipment for the purpose of government procurement. We lay out our SCRM policy arguments in dedicated white paper that is available here: https://www.itic.org/documents/public-sector/ITI_SupplyChain_Whitepaper_033021.pdf

- **Explain Reasons for the Rescission**: The FASC promotes a risk-based and collaborative approach to addressing supply chain risks in federal ICT systems. Accordingly, reorganizing all government-wide supply chain risk management policy under the FASC will ensure regulatory consistency while appropriately addressing national security risks.
- **Text of Relevant Statutory Authority**:https://www.federalregister.gov/documents/2021/08/26/2021-17532/federal-acquisition-security-council-rule
- **Name of Agency Head**: Russell Vought
- **Title of Agency Head**: Director, OMB

e. SEC "Security Controls" Authority

- **Agency:** Securities and Exchange Commission (SEC)
- **Title / CFR Section:** SEC "security controls" authority at 15 U.S.C. 78m(b)(2)(B)
- **Justification:** OMB should clarify that the Securities and Exchange Commission (SEC) authority to require adequate "internal accounting controls" does not extend to organizational cybersecurity safeguards. OMB should formally direct SEC to cease attempting to use this authority because it oversteps SEC's Congressionally authorized mandate.
- **Background:** Though the SEC has extracted financial settlements from several publicly traded companies under this theory, Congress never granted the SEC with this authority, and SEC Commissioners have dissented against its use. When the SEC's theory was tested at trial in *SEC vs. SolarWinds*, it was rejected by the U.S. District Court for the Southern District of New York. The court ruled that the SEC does not have authority to regulate an issuer's cybersecurity controls, and its "controls" authority is limited to financial accounting controls.

f. Cybersecurity Certification

We recommend the establishment of a unified cybersecurity certification scheme. Such a regime should be risk-based and outcomes-focused, leverage international standards, promote public-private collaboration, and embrace technological neutrality.

Currently, companies are required to navigate a complex landscape of overlapping and conflicting regulations. Simultaneously, regulatory authorities in the cybersecurity space are distributed across multiple regulatory jurisdictions. Accordingly, virtually all cybersecurity compliance schemes include overlapping controls.

A better approach would establish baseline requirements on a single standard that meet the security needs of the vast majority of existing regulations. Potential candidates are NIST SP 800-53 or the ISO/IEC 27000 series. Rather than eliminating existing compliance regimes within the U.S. government, basing all regulations on the same standard would create predictability and enable organizations to clearly meet expectations efficiently.

In some situations, critical sectors or agencies might require additional security measures. Instead of creating a whole new regime, regulators should be encouraged to start with the baseline regulatory requirements and add limited supplemental requirements through an annex. Basing all regimes off a universal baseline and controls catalogue has the added benefit of enabling control inheritance. If an organization has successfully implemented a control to comply with one set of regulations, other regulators can grant mutual recognition for that control and focus on the control delta between the baseline and the additional need.

By shifting the conversation in cybersecurity to baseline security standards, rather than simply eliminating regulation, OMB could vastly improve the ease of compliance with cybersecurity best practices while not getting bogged down in a regulatory mapping exercise.

Finally, an effort to consolidate sprawling cybersecurity controls would support initiatives like the Unleashing Prosperity Through Deregulation Executive Order signed by President Trump in January 2025. Similarly, expanding the centralized regulatory review process is in line with EO 14215 and OMB Memorandum M-25-24. This is in line with a recommendation ITI made in 2023 where we recommended a strengthening the standardized clearing process within OIRA for all new regulatory activity to prevent the future fragmentation of regulation.[1]

2. ***Pre-Merger Notification Rule under the Hart-Scott-Rodino (HSR) Antitrust Improvements Act Filing Requirements***

- **Agency:** Federal Trade Commission (FTC)
- **Title/Section of CFR to be rescinded:** 16 CFR Parts 801 and 803
- **Rule Type:** Final Rule
- **Name of Regulation being rescinded:** Pre-Merger Notification Rule under the Hart-Scott-Rodino (HSR) Antitrust Improvements Act Filing Requirements.
- **Justification:** Over-reporting imposes a compliance burden without proportional enforcement benefits. Clarifying thresholds and reducing reporting for low-risk transactions would preserve agency resources and reduce burdens on innovation ecosystems.
- **Agency Contact Information:** Robert Jones, Assistant Director, Premerger Notification Office, Bureau of Competition, Federal Trade Commission, 400 7th Street SW,

[1] https://www.itic.org/public-policy/ITIResponsetoONCDRegulatoryHarmonizationRFI.pdf

Washington, DC 20024; (202) 326-3100.

- **Background for the regulation being rescinded:** The HSR pre-merger notification process imposes expansive and outdated reporting burdens on technology companies, particularly those involved in cross-border and venture transactions that do not present competition concerns. Recent FTC and DOJ proposals to broaden filing requirements would significantly increase compliance costs for mergers unlikely to raise antitrust issues.
- **Explain Reasons for the rescission:** We urge the FTC and relevant agencies to consider narrowing the scope of reportable transactions under the HSR Act, streamlining requirements for transactions involving non-controlling minority interests or startups with limited revenue, and incorporating clear, predictable thresholds for global technology firms.
- **Text of Relevant CFR:** 16 CFR Part 801: Antitrust; 16 CFR Part 803: Antitrust; Fees; Reporting and recordkeeping requirements.
- **Name of Agency Head**: Andrew N. Ferguson
- **Title of Agency Head:** Chairman, FTC

3. FTC Negative Option Rule

- **Agency:** Federal Trade Commission (FTC)
- **Title/Section of CFR to be rescinded:** 16 CFR Part 425
- **Rule Type:** Final Rule
- **Name of Regulation being rescinded:** Rule Concerning Recurring Subscriptions and Other Negative Option Programs.
- **Justification:** ITI opposes the FTC's amended Negative Option Rule because it imposes broad, unnecessary, and counterproductive regulatory burdens that undermine consumer benefits, stifle innovation, and harm market competition.
- **Agency Contact Information:** Katherine Johnson, Attorney, (202) 326-2185, *kjohnson3@ftc.gov*, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.
- **Background for the regulation being rescinded:** The FTC originally issued the Negative Option Rule in 1973 to regulate subscription-based marketing models such as book-of-the-month clubs. In response to evolving e-commerce practices, Congress subsequently enacted additional protections through the Restore Online Shoppers' Confidence Act (ROSCA) and the Telemarketing Sales Rule (TSR). In 2019, the FTC initiated a targeted review focused narrowly on improving disclosures, billing consent, and cancellation practices related to negative options. However, the 2024 amendments dramatically expanded the Rule's scope, creating sweeping civil penalty exposure for any material misrepresentation linked to a negative option product, prompting significant legal, economic, and procedural concerns.
- **Explain Reasons for the rescission:** The amended Negative Option Rule should be rescinded because it is overly broad, economically harmful, and unnecessary. It penalizes any material misrepresentation tied to a negative option product, even if unrelated to the subscription itself, creating significant uncertainty for lawful businesses. This chilling effect will discourage consumer-friendly subscription models, raise costs for consumers, and stifle innovation, especially harming small businesses.

Existing laws such as the Restore Online Shoppers' Confidence Act (ROSCA) and the Telemarketing Sales Rule (TSR) already provide effective mechanisms to combat deceptive practices. Instead of targeted enforcement, the Rule imposes sweeping, duplicative requirements without sufficient evidence that such broad regulation is warranted.

- **Text of Relevant CFR:** Text available here: https://www.federalregister.gov/documents/2024/11/15/2024-25534/negative-option-rule
- **Name of Agency Head**: Andrew N. Ferguson
- **Title of Agency Head:** Chairman, FTC

4. Semiconductors related regulations

a. *CHIPS Act Notices of Funding Opportunity (NOFO) Requirements*

- **Agency**: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.
- **Title/Section of CFR to be replaced**: N/A (non-regulatory NOFO but aligned with 15 U.S.C. § 4652 under the CHIPS Act).
- **Rule Type**: Notice of Funding Opportunity (NOFO).
- **Name of Regulation/Program Being Replaced**: CHIPS Incentives Program – Commercial Fabrication Facilities (NOFO Amendment to 2023-NIST-CHIPS-CFF-01)
- **Justification**: While the CHIPS Incentives Program promotes domestic semiconductor manufacturing, its stringent eligibility requirements, extensive compliance burdens, and prescriptive planning mandates risk discouraging innovation and excluding smaller firms, especially in rapidly evolving sub-sectors such as advanced packaging and materials R&D. The program's complexity may reinforce incumbent advantages and diminish the pace of supply chain diversification.
- **Agency Contact Information**: CHIPS Program Office (CPO); CHIPSInquiries@chips.gov Phone: (202) 307-5800 Website: https://www.chips.gov.
- **Background for the Regulation Being Replaced**: The CHIPS Incentives Program under the CHIPS Act of 2022 was designed to catalyze investments in semiconductor manufacturing, particularly through the construction, expansion, or modernization of fabrication facilities. However, its implementation has emphasized detailed requirements for social programs, financial and workforce development commitments, and extraordinarily burdensome reporting obligations, along with a multistage application process involving complex due diligence and milestone tracking. To better align with the diverse needs of the semiconductor ecosystem and enhance national resilience, a dedicated stream should be established within the program to support modular, lower-risk, or R&D-intensive facilities, which often contribute critically to innovation and supply chain robustness.
- **Explain Reasons for the Replacement:** ITI encourages OMB and NIST to recalibrate the CHIPS Incentives Program to reduce compliance barriers. The changes recommended below align to Congressional intent to ensure that CHIPS incentives help make the U.S. a more competitive player in the race to build semiconductor fabrication capacity across

all segments of the semiconductor market. We recommend significantly amending the current NOFO (Commercial Fabrication Facilities) to:

- Expedite and streamline/simplify the multi-phase application process, including the government's negotiation of in-process applications.
- Minimize criteria promoting diversity, equity, inclusion and childcare requirements.
- Eliminate requirements regarding criteria on upside sharing, stock buybacks, inclusive opportunities for business, project labor agreements, climate and environment impact plans, and community investments to promote equity.

- **Text of Relevant Statutory Authority:** 15 U.S.C. § 4652 (CHIPS Act implementation); CHIPS Act of 2022, Division A of Pub. L. 117-167; NOFO Reference: 2023-NIST-CHIPS-CFF-01.
- **Name of Agency Head**: Craig Burkhardt
- **Title of Agency Head**: Acting Under Secretary of Commerce for Standards and Technology and Acting Director, NIST.

b. *Prohibition on Certain Semiconductor Products and Services*

- **Agency**: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).
- **Title/Section of CFR to be rescinded**: 48 CFR Parts 40, and 52 [FAR Case 2023-008; Docket No. FAR-2023-0008, Sequence No. 1] RIN 9000-AO56.
- **Rule Type**: Advanced Notice of Proposed Rule.
- **Name of Regulation/Program Being Rescinded**: Prohibition on Certain Semiconductor Products and Services.
- **Justification**: The FAR Case significantly exceeds regulatory authority granted by Congress. Specifically, the FAR Case goes beyond the authorizing statue's definitions of "critical systems" and "use," and in so doing, would not be proportionate to the risk of using commercial semiconductors. The FAR Case also contradicts the statute by proposing to require more than a "reasonable inquiry" as to the origin of semiconductors. Details can be found here:https://www.itic.org/documents/public-sector/ITICommentstoDoDonSec.5949FY23NDAA.pdf.
- **Agency Contact Information**: Email *Farpolicy@gsa.gov* or call 202-969-4075.
- **Background for the Regulation Being Rescinded**: This Case was issued to develop regulations to implement Section 5949 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2023. While the statute contains requirements to secure the nation's supply chain, the Advanced Notice of Proposed Rulemaking (ANPR) omits flexibility provided in the statute, especially for commercially-available-off-the-shelf (COTS) items, in a manner that is concerning to industry. Problematic measures include expanding the scope of the restriction to all information systems, rather than limiting it to "critical systems," the applicability to commercial and COTS products, requirement flow down, a requirement to exceed the "reasonable inquiry" standard for supply chain due diligence, and the broad definitions. We summarize our specific

concerns and recommendations here: https://www.itic.org/documents/public-sector/ITICommentstoDoDonSec.5949FY23NDAA.pdf.

- **Explain Reasons for the Rescission**: The FAR Case significantly exceeds regulatory authority granted by Congress, which contradicts the holding of *Loper Bright*. The FAR Case would:
    - Go beyond the authorizing statue's definitions of "critical systems" and "use," and in so doing, would not be proportionate to the risk of using commercial semiconductors.
    - Contradict the statute by proposing to require more than a "reasonable inquiry" as to the origin of semiconductors.

- **Text of Relevant Statutory Authority**: https://uscode.house.gov/statviewer.htm?volume=136&page=3485.
- **Name of Agency Head**: Stephen Ehikian
- **Title of Agency Head**: Acting Administrator

c. *Unpredictable Trade Environment*

While not a discrete regulation, the imposition of complex, broadly scoped, and rapidly changing tariff and trade actions has similar effects to regulatory barriers that hinder investment and innovation across the U.S. technology value chain. The recent country-based and sectoral tariff announcements and proposals create administrative burdens that can reduce confidence in making large-scale investments in the United States (including projects to strengthen U.S. competitiveness in technologies such as semiconductors and AI), reduce flexibility in supply chain operations, and hurt the competitiveness of U.S. goods and services in the global marketplace.

5. *Telecom Regulations*

a. *Data Breach Reporting Requirements*

- **Agency**: Federal Communications Commission (FCC)
- **Title/Section of CFR to be rescinded**: **Rule Type**: Data Breach Reporting Requirements, WC Docket No. 22-21, Report & Order, FCC 22-111
- **Name of Regulation/Program Being Rescinded**: FCC 2023 Data Breach Order
- **Justification**: Order likely runs afoul of the Congressional Review Act, as it relies on the same legal authorities—Sections 201(b) and 222—as the disapproved 2016 Broadband Privacy Order.
- **Agency Contact Information**: Mason Shefa, Competition Policy Division, Wireline Competition Bureau, at (202) 418-2494, *mason.shefa@fcc.gov*.
- **Explain Reasons for the Rescission**: The Federal Communications Commission should reverse rules from the 2023 Data Breach Order that expand the definition of covered data and eliminate Subparts U and EE. Expanding the definition of "covered data" to include

personally identifiable information beyond customer proprietary network information (CPNI) creates a risk of over-notification and consumer fatigue, without materially improving data security or privacy outcomes. ITI further warns that the Order may run afoul of the Congressional Review Act, as it relies on the same legal authorities—Sections 201(b) and 222—as the disapproved 2016 Broadband Privacy Order. Moreover, the outdated safeguard provisions, including rigid authentication protocols, can impede the adoption of modern security best practices. Consistent with ITI's recommendations, the Commission should adopt a harm-based notification standard and align any breach reporting obligations with existing federal frameworks like CIRCIA to ensure clarity, efficiency, and legal durability.

- **Name of Agency Head**: Brendan Carr
- **Title of Agency Head**: Chairman

6. *Permitting Reforms*

a. Establish U.S. Army Corps of Engineers Nationwide Permit (NWP) for data center construction.

- **Agency:** U.S. Army Corps of Engineers
- **Rule Type:** Final Rule
- **Name of Regulation/Program:** Nationwide Permit Program, 33 C.F.R. Part 330.
- **Justification:** This pathway has many precedents as NWPs have been successfully deployed for other infrastructure sectors, demonstrating that narrowly tailored, low-impact permits are a viable regulatory tool. Establishing an NWP for data center construction would reliably eliminate 6 months or more from the typical Individual Permit process managed by the Corps. Alternatively, data centers could be expressly included within an existing NWP that achieves the same efficiencies (e.g., NWP 39, which covers commercial and institutional developments). More details about the importance of streamlining the permitting process for critical energy infrastructure projects can be found in our response to the Department of Energy's Request for Information on AI Infrastructure on DOE Lands here: https://www.itic.org/documents/artificial-intelligence/ITIResponse_DOE_FR2025-05936.pdf.
- **Background:** Under Section 404 of the Clean Water Act, the U.S. Army Corps of Engineers regulates the discharge of dredged or fill material into waters of the United States. 33 U.S.C. § 1344(e). For activities with minor impacts, the Corps can issue NWPs—a type of general permit intended to streamline the permitting process for projects with minimal individual and cumulative environmental effects. NWPs are valid for 5 years and cover a wide range of activities.
- **Reasons for Rescission:** Currently, data center construction—despite often having low-impact footprints—is typically required to undergo the more burdensome Individual Permit process under Section 404. This process requires site-specific environmental reviews, public notice periods, and consultation with resource agencies. The result is a permitting timeline that can extend 6 months or longer, delaying critical infrastructure that supports the digital economy and broader energy goals. Establishing a dedicated

NWP for data center construction would provide a predictable, expedited pathway for compliance. Many data centers are sited to avoid or minimize wetland impacts and could conform to reasonable NWP thresholds and mitigation requirements. By removing these projects from the lengthy individual permit queue, the Corps can focus its resources on higher-impact proposals, improving efficiency across the board. The urgency is underscored by the rapid expansion of cloud computing, AI, and advanced manufacturing—all of which require robust and resilient data infrastructure.

- **Statutory Authority:** 33 U.S.C. § 1344(a): "The Secretary may issue permits, after notice and opportunity for public hearings for the discharge of dredged or fill material into the navigable waters at specified disposal sites. Not later than the fifteenth day after the date an applicant submits all the information required to complete an application for a permit under this subsection, the Secretary shall publish the notice required by this subsection." 33 U.S.C. § 1344(e): "In carrying out his functions relating to the discharge of dredged or fill material under this section, the Secretary may, after notice and opportunity for public hearing, issue general permits on a State, regional, or nationwide basis for any category of activities involving discharges of dredged or fill material if the Secretary determines that the activities in such category are similar in nature, will cause only minimal adverse environmental effects when performed separately, and will have only minimal cumulative adverse effect on the environment."

b. Require agencies and provide necessary funds to leverage digital technologies to streamline and accelerate environmental permitting.

- **Agency:** U.S. Environmental Protection Agency; U.S. Army Corps of Engineers; Nuclear Regulatory Commission; Federal Energy Regulatory Commission; Bureau of Land Management; U.S. Fish and Wildlife Service; National Oceanic and Atmospheric Administration; National Marine Fisheries Service; Bureau of Ocean Energy Management; Council on Environmental Quality
- **Rule Type:** Final Rule; New Proposal
- **Name of Regulation/Program:** Cross-Media Electronic Reporting Rule (CROMERR), 40 C.F.R. Part 3. National Pollutant Discharge Elimination System (NPDES) Electronic Reporting Rule, 40 C.F.R. §127.23(4). U.S. Army Corps of Engineers Regulatory Request System.
- **Justification:** Establishing a centralized electronic environmental permitting system would remove tedious and costly obstacles to American businesses seeking to deploy projects, provide greater certainty and transparency throughout the permitting process, and modernize federal agency permitting programs.
- **Background:** Many federal agencies tasked with issuing environmental permits do not have regulations requiring electronic permitting. EPA implements its CROMERR system and NPDES e-reporting rules, and the Corps recently released a Regulatory Request System for Clean Water Act Section 404 permits. However, these environmental permitting regimes neither communicate with one another nor conform to modern interoperability protocols, thereby compelling regulated entities to re-enter the same

data through multiple, agency-specific portals and prompting agency staff to perform duplicative, paper-based, time-intensive manual reviews.

- **Reasons for Rescission:** This antiquated architecture conflicts with the Administration's directive to leverage information technology for efficient environmental permitting. Federal agencies should be directed to overhaul their systems and implement a centralized and modern electronic database and permitting system that is standardized across the federal government. The net social costs of maintaining obsolete, disparate systems materially exceed their benefits: duplicative data entry, delayed permit issuance, and inconsistent data validation collectively impose hundreds of millions of dollars in compliance costs on small and mid-sized businesses each year, while yielding no commensurate environmental gain. Conversely, rescission and replacement with a single, government-wide, cloud-based, platform would unlock immediate efficiencies, shorten average permit processing times, and improve data quality for enforcement and public-disclosure purposes. Uniform electronic reporting standards, harmonized user-credentialing, and real-time data sharing across agencies would restore transparency, reduce the risk of inadvertent non-compliance, and reallocate scarce intra-agency resources from clerical verification toward substantive environmental review, thereby advancing statutory objectives more effectively and relieving American innovators of unnecessary procedural hurdles. OMB should therefore issue a rule that establishes a flexible, open-source data-exchange framework readily adaptable to future technological advances.
- **Statutory Authority:** 44 U.S.C. § 3504(a)(1)(A) (Paperwork Reduction Act): OMB shall "develop, coordinate and oversee the implementation of Federal information resources management policies, principles, standards, and guidelines." 44 U.S.C. § 3516: "The Director shall promulgate rules, regulations, or procedures necessary to exercise the authority provided by this subchapter." 44 U.S.C. § 3604(a) (E-Government Fund): "The Fund shall be administered by the Administrator of the General Services Administration to support projects approved by the Director, assisted by the Administrator of the Office of Electronic Government, that enable the Federal Government to expand its ability, through the development and implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically. Projects under this subsection may include efforts to . . . enable Federal agencies to take advantage of information technology in sharing information and conducting transactions with each other and with State and local governments." 42 U.S.C. § 4336d: "The Council on Environmental Quality shall conduct a study and submit a report to Congress within 1 year of the enactment of this Act on the potential for online and digital technologies to address delays in reviews and improve public accessibility and transparency under section 4332(2)(C) of this title including, but not limited to, a unified permitting portal . . .."

c. *Allocate funding to provide federal agencies with the resources necessary to administer permitting programs in a timely manner*

- **Agency:** Office of Management and Budget
- **Rule Type**: N/A
- **Name of Regulation/Program**: N/A
- **Justification**: Permit applicants continue to experience extreme delays in permit review, with agencies citing lack of funding and resources. Reallocating the disbursement of federal funding to accelerate permitting decisions will more effectively carry out statutory functions, reduce unproductive delays and costs on project applicants, and foster American innovation in furtherance of the administration's goals.
- **Background**: While Congress determines the total appropriations for each federal agency, the agencies themselves retain discretion over how those appropriated dollars are distributed among internal programs and priorities. Within the bounds of the relevant appropriations statutes and governing fiscal law, an agency such as EPA may shift unobligated or otherwise discretionary funds toward the personnel, technical resources, and process-improvement initiatives necessary to expedite environmental permitting. Consequently, even when overall congressional funding levels are constrained—whether because of policy disagreements, attempts to curtail perceived regulatory overreach, or broader budgetary pressures—agencies possess lawful flexibility to realign available resources so that critical permit reviews proceed without undue delay.
- **Reasons for Reform**: Chronic underfunding has lengthened processing times for Section 404, NPDES, and Title V permits by weeks to months, delaying billions of dollars in construction, manufacturing, and energy projects. Targeted reinvestment would yield immediate, measurable gains in job creation and GDP without altering the overall fiscal stance of the federal budget. Directing environmental agencies to exercise this allocation authority towards essential core functions such as permitting not only supports statutory mandates for efficient permitting but also mitigates the risk that budget limitations will hamper economic development or undermine environmental compliance goals. By judiciously channeling discretionary dollars into staffing, data management, and interagency coordination efforts keyed to permit timeliness, agencies can sustain predictable review schedules and uphold their administrative responsibilities.
- **Statutory Authority**: N/A

7. Tax related rules

a. Section 199 – Domestic Production Activities Deduction (IRC)

When Section 199 was originally enacted in 2004, any software was explicitly included as domestic production in black letter law. The IRS inappropriately narrowed the scope of "any computer software" that should have been eligible for the domestic production incentive. Subsequently in 2017 Congress repealed the Section 199 domestic production activities deduction as part of the

effort to lower the rate and broaden the base. Treasury and the IRS should remove the prior Section 199 regulations that inappropriately narrowed the scope of Section 199's reference to "any computer software":

- Treas Reg 199-3(i)(6)(ii) which effectively treats all online software as a "service," which does not qualify for Section 199.
- Treas. Reg. 199-3(i)(6)(iii) which provides exceptions for online software that meets certain criteria, i.e., self-comparable exception and third-party comparable exception. If the online software meets either of these exceptions, then the gross receipts from such online software is treated as being derived from the lease, rental, license, sale, exchange or other disposition of computer software. Conversely, if it doesn't meet the criteria, then the online software is not qualified under Section 199.
- Treas Reg 199-3(i)(6)(v) contains examples of application of Treas Reg 199-3(i)(6).

b. Corporate Alternative Minimum Tax Adjusted Financial Statement Income Allocation

The IRS and Treasury should reconsider the application of Section 482 principles to create adjusted financial statement income ("AFSI"), rather than reallocate AFSI, in a manner that seems inconsistent with the purpose of the corporate alternative minimum tax (CAMT).

Treasury and the IRS should make a technical Correction to modify the rule in Prop. Reg. Section 1.56A-26(d)(1) on the application of the principles of IRC Section 482 and its regulations (IRC Section 482 Principles) in accounting for a controlled transaction or controlled transfer (as defined in Treas. Reg. Section 1.482-1(i)(8)) for CAMT purposes. Before the modification, Prop. Reg. Section 1.56A-26(d)(1) indicated that a CAMT entity must make appropriate adjustments to CAMT basis (not AFSI) to apply IRC Section 482 Principles to controlled transactions or controlled transfers that were not accounted for in FSI in a manner consistent with the IRC Section 482 Principles. The Technical Correction would clarify that the CAMT entity must adjust its AFSI to apply the IRC Section 482 Principles to the controlled transactions or controlled transfers.

We appreciate OMB's leadership in soliciting stakeholder feedback to enhance the effectiveness of the federal regulatory framework. ITI and our member companies stand ready to serve as resource as the Administration considers opportunities for reform. We welcome continued dialogue and collaboration to ensure that regulatory policies support innovation, economic competitiveness, and national security.

***