May 11, 2026

ELECTRONIC SUBMISSION

Attn: EPA-HQ-OLEM-2025-0313

Kristina Guarino
Office of Land and Emergency Management
U.S. Environmental Protection Agency
1200 Pennsylvania Ave NW
Washington, DC 20460

Re: Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Common Sense Approach to Chemical Accident Prevention

Dear Ms. Guarino,

On February 24th, 2026, the U.S. Environmental Protection Agency (EPA) published the Proposed Rule, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Common Sense Approach to Chemical Accident Prevention."[1] EPA subsequently published an extension for the comment period of this Notice, extending the deadline to May 11th, 2026.[2] In this Notice, EPA proposes to amend its Risk Management Program[3] (RMP) by making significant revisions to the 2024 Safer Communities by Chemical Accident Prevention (SCCAP) Rule.[4]

EPA's stated goal of transparency,[5] when promulgating the SCCAP Rule, was laudable to some extent. However, too much transparency can undermine our country's security, when the transparency leads to public dissemination of sensitive information that, in the wrong hands, can help terrorists, criminals, hostile States, and bad actors generally make strategic determinations over which critical infrastructure to target. The SCCAP Rule led to an unbalanced approach, in

[1] U.S. Environmental Protection Agency, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Common Sense Approach to Chemical Accident Prevention," *Federal Register*, Vol. 91, No. 36 (February 24, 2026), p. 8,970.
[2] U.S. Environmental Protection Agency, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Common Sense Approach to Chemical Accident Prevention; Extension of Comment Period," *Federal Register*, Vol. 91, No. 63 (April 2, 2026), p. 16,621.
[3] 40 CFR Part 68.
[4] U.S. Environmental Protection Agency, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Safer Communities by Chemical Accident Prevention," *Federal Register*, Vol. 89, No. 48 (March 11, 2024), p. 17,622.
[5] *See, e.g.*, 89 Fed. Reg. at 17,634.

which transparency interests were allowed to overwhelm security concerns, to an extent that made our country and communities less secure, and less safe. Therefore, we are encouraged to see that EPA is now revisiting the decisions made in the 2024 SCCAP Rule, and respectfully submit these comments for your consideration.

Both of us were career officials at the U.S. Department of Homeland Security, in the Cybersecurity and Infrastructure Security Agency (CISA), when EPA issued the SCCAP Rule. CISA leads the national effort and works with law enforcement, local government, and infrastructure owners and operators to understand, manage, and reduce the threats to our nation's cyber and physical infrastructure.[6]

When EPA issued the SCCAP Rule in March of 2024, one of us, Bridget Bean, was Assistant Director for CISA's Integrated Operations Division, in which capacity she oversaw CISA's field operations, which included oversight of 150 Chemical Security Inspectors deployed nationwide to help ensure that chemical facilities were properly protected against bad actors. Not long after the SCCAP Rule was published, in August of 2024 Ms. Bean became Executive Director of CISA, the highest ranked career official, with management responsibilities over the entire agency. In January of 2025, Ms. Bean became the Acting Director of CISA, a position that she held until May of 2025.

At the time when EPA issued the SCCAP Rule, the other signatory to this comment letter, Trevar Kolodny, worked as a Senior Policy Analyst in CISA's Infrastructure Security Division, in the Office of Chemical Security. In this capacity, he delivered strategic policy recommendations to senior leadership to help build CISA's voluntary ChemLock program,[7] and to help inform the Office of Chemical Security's transition after the lapse of the Chemical Facility Antiterrorism Standards.[8]

In these capacities, we witnessed firsthand the concern, and in many cases, alarm among the community of chemical facilities, law enforcement organizations, and many elements of the U.S. Department of Homeland Security, as EPA required the public disclosure by high-risk chemical facilities of information that many of them had previously regarded as protected Chemical-terrorism Vulnerability Information (CVI).[9] Now that we are both out of Government and freer to speak, we are grateful for this opportunity to reinforce those concerns in this comment, particularly with regard to the public availability of information, as enforced in the 2024 SCCAP Rule and as modified in this Notice.

---

[6] U.S. Cybersecurity and Infrastructure Security Agency. *About CISA*. https://www.cisa.gov/about
[7] U.S. Cybersecurity and Infrastructure Security Agency. *ChemLock*. https://www.cisa.gov/resources-tools/programs/chemlock
[8] U.S. Cybersecurity and Infrastructure Security Agency. *Chemical Facility Anti-Terrorism Standards (CFATS)*. https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats
[9] 6 CFR 27.400.

Discussion

1) EPA's Proposal Represents an Improvement Over the Existing Rule, with Regard to Public Availability of Information.

    a. *Shifting the Disclosure Responsibility from Owners and Operators to EPA is a More Faithful, and Normatively Superior, Understanding of Agency Responsibilities under the Freedom of Information Act.*

We support EPA's proposal to remove the burden of public information availability from the regulated facilities. This is a commendable development, on both normative and legal grounds.

When proposing the SCCAP Rule, EPA cited its obligations under the Freedom of Information Act[10] (FOIA) as requiring disclosure of the covered chemical facility information, despite security-based objections that had been expressed.[11] Yet the requirements that EPA placed on industry went far beyond anything that was required, or even within the spirit, of FOIA's provisions.

Specifically, FOIA requires the Federal Government to provide requested information to the public. FOIA's mandate is that "[e]ach agency shall make available to the public information as follows."[12] In the SCCAP Notice, EPA claimed that FOIA tied its hands, given FOIA's requirement that information requested via FOIA three or more times must be made available for public inspection in an electronic format.[13] Yet, quite importantly, EPA left the opening words of the paragraph out of its citation, namely, "Each *agency*, in accordance with published rules, shall make available for public inspection in an electronic format"[14] the subsequently listed documents.

In other words, FOIA, by its structure and language, places the responsibility on the Federal Government to disclose the information in its own possession. FOIA was never intended to place the burden and onus of public disclosure on the owners and operators of critical infrastructure. To the extent that EPA relied on FOIA to require infrastructure operators and owners to disclose their own information directly to the public, EPA not only misapplied FOIA,

[10] Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552).
[11] U.S. Environmental Protection Agency, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Safer Communities by Chemical Accident Prevention," *Federal Register*, Vol. 87, No. 168 (August 31, 2022), p. 53,556 at 53,602.
[12] 5 U.S.C. § 552(a).
[13] 87 Fed. Reg. at 53,602 (*citing* 5 U.S.C. § 552(a)(2)(D)(ii)(II)).
[14] 5 U.S.C. § 552(a)(2) (emphasis added).

but improperly used its legal responsibilities under FOIA as an excuse to place the burden of public disclosure directly on the infrastructure owners and operators themselves.

Moreover, the burden on infrastructure owners and operators is not trivial. As EPA has noted in its regulatory analysis in this proposal, the information availability provisions of the SCCAP Rule were the most expensive aspects of the rule, other than the provisions relating to Safer Technology Alternatives Analysis (STAA).[15] Indeed, EPA has concluded that the information availability requirements alone cost industry burden of $127 million over a 10-year period. Given that industry was forced to bear this cost in order to satisfy a statutory obligation that Congress expressly imposed on the Federal Government, rather than on infrastructure owners and operators, the SCCAP Rule arguably violated the Unfunded Mandates Reform Act.[16]

There are additional benefits for EPA to take responsibility for meeting any FOIA disclosure requirements, besides relieving the burden from industry. In particular, as EPA has recognized,[17] EPA's retention of control over disclosure would give the Federal Government greater control over the exact content of the information disclosed, and promote uniformity in the information provided, which would have security benefits, both because only Federally vetted information would actually be disclosed, and the Federal Government would retain full knowledge over the information disclosed to the public. In addition, when the Government retains control over the information disclosure, the Government also potentially contains more information about who is actually requesting the information, which can be helpful for law enforcement, although it appears that EPA is proposing to relinquish that benefit by making the data available in a publicly accessible, on-demand, online tool.

b. *Removing the Language Provisions Removes an Onerous Burden from Chemical Facilities, as well as from EPA*

In addition, shifting the disclosure responsibilities from the chemical facilities to the Government will protect chemical facilities from bearing the burden of translating the documents disclosed into certain foreign languages, upon request. As EPA recognized in the Notice,[18] removing the requirement to make the disclosure documents available in languages other than English is the most appropriate implementation of Executive Order (EO) 14224, Designating English as the Official Language of the United States.[19] This Executive Order did confirmed the

[15] 91 Fed. Reg. at 8,973.
[16] Unfunded Mandates Reform Act of 1995, Pub. L. No. 104-4, 109 Stat. 48 (codified as amended at 2 U.S.C. §§ 1501-71).
[17] 91 Fed. Reg. at 8,984.
[18] *Id.*
[19] Exec. Order No. 14224, *Federal Register*, Vol. 90, No. 43 (March 1, 2025), p. 11,363.

status of English as the official language of the United States, and rescinded EO 13166, Improving Access to Services for Persons With Limited English Proficiency.[20]

Yet even under the preexisting EO 13166, EPA exceeded its remit in requiring chemical facilities to provide disclosures in languages other than English. Under its terms, EO 13166, as with FOIA, placed any performance obligations on the Federal Government itself, not on regulated stakeholders. Specifically, the EO provided that "each Federal agency shall examine the services it provides and develop and implement a system by which [Limited English Proficiency] persons can meaningfully access those services consistent with, and without unduly burdening, the fundamental mission of the agency."[21]

In other words, the Federal policy was that *agencies* would provide services to people with limited English proficiency, not that the agencies would, with no statutory justification, require the provision of such multilingual services by regulated stakeholders. Creating such a burden on stakeholders, not only to know the two languages in the neighborhood most often spoken other than English, but to provide materials in these languages upon request, is both a burden and an expense, which distracts from the core missions of these companies.

More than 350 languages are spoken in the United States.[22] In addition, whilst it is tempting to think of chemical facilities as large corporations, which some are, many are also very small, with five or fewer employees. It is extraordinary to require such facilities, not only to provide the information, but to have the knowledge of which two non-English languages are most widely spoken in the surrounding community (however that is defined), and to be able to translate disclosure documents into such languages as Spanish, Farsi, Russian, or Mandarin, depending on where the facility is located. The burden to require these companies to provide their chemical information in multiple languages is real, and probably violates the Paperwork Reduction Act,[23] which requires Federal agencies to minimize paperwork burdens on regulated stakeholders, and obtain approval from the Office of Management and Budget for any information collections. Such a burdensome requirement on the regulated stakeholders also violates the spirit of the cost-benefit analyses required by EO 12866,[24] and the Regulatory Flexibility Act, which requires EPA to consider the impacts of its regulations on small businesses.[25]

---

[20] Exec. Order No. 13166, *Federal Register*, Vol. 65, No. 59 (August 16, 2000), p. 50,121.
[21] *Id.*
[22] American Academy of Arts and Sciences. *Main Languages Spoken at Home by U.S. Residents Aged Five Years and Older, 2008 – 2010*. https://www.amacad.org/publication/state-languages-us-statistical-portrait/section/3
[23] Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501-21).
[24] Exec. Order No. 12866, *Federal Register*, Vol. 58, No. 190 (October 4, 1993), p. 51,735.
[25] Regulatory Flexibility Act, Pub. L. No. 96-354,94 Stat. 1164 (1980) (codified as amended at 5 U.S.C. §§ 601-12).

In this respect, it is particularly worth noting that EPA placed on regulated stakeholders a burden that very few agencies, including EPA, would be prepared to meet in their own right. Even within the Federal Government, the expense of using translation services from the U.S. Department of State means that such translation services are used sparingly, and by many agencies not at all. Virtually no Federal agency has the ability to maintain information, not only in English, but in two other languages that are commonly spoken in the vicinity of any relevant premise. It is perhaps unsurprising that EPA is dropping the multilingual requirement, now that EPA is proposing to handle disclosure itself. However, it was inappropriate, even before the promulgation of EO 14224, to ask regulated stakeholders to bear the cost of translation services that Federal agencies themselves find too onerous to bear, and it is encouraging to see EPA recognize and correct this.

2) EPA's Proposal Would be Further Improved by Restoring, to the Fullest Extent Possible, the Chemical RMP as it Existed Before the Enactment of the SCCAP Rule

a. *The Security Threat to Chemical Facilities Remains Potent*

Although the Notice represents a significant improvement over the existing 2024 SCCAP Rule, the approach would be further improved by reverting as closely as possible to the pre-2024 *status quo*. If EPA concludes that some form of disclosure is required by FOIA, then EPA should make sure that the resulting disclosure is as limited as possible, informed by recognition of how the chemical sector represents a uniquely attractive target to bad actors.

During the SCCAP rulemaking process, it was dismaying to see how EPA cited to a 2021 study, in which researchers concluded that there were no terrorist events in the chemical process industries in North America, after the 1970's.[26] This cited report[27] analyzed a dataset which, by definition, only included incidents that had actually occurred. As EPA would know from its interactions with law enforcement and with CISA through the EO 13650 working group,[28] access to data showing the full picture of the chemical security threat is carefully restricted, and not publicly available, meaning that studies relying solely on public information, restricted to incidents that have actually occurred, should be treated with caution.

There have been publicly known attacks on critical infrastructure with chemical capabilities, even if this chemical infrastructure does not necessarily fall under EPA's jurisdiction, and even if these particular attacks did not result in chemical releases. As perhaps

[26] 87 Fed. Reg. at 53,603.
[27] Valeria Casson Moreno, Genserik Reniers, Ernesto Salzano, and Valerio Cozzani, *Analysis of physical and cyber security-related events in the chemical and process industry*, Process Safety and Environmental Protection, Volume 116, 2018, Pages 621-631, ISSN 0957-5820.
https://www.sciencedirect.com/science/article/abs/pii/S095758201830079X?via%3Dihub
[28] *See* Exec. Order No. 13,650, 78 Fed. Reg. 48,029 (August 1, 2013).

the most famous example, in 2021 the Colonial Pipeline Company halted all of its pipeline operations for six days after a ransomware attack.[29] Less dramatically, but more recently, Iran successfully hacked and defaced Israeli-made controls at multiple water plants in Pennsylvania,[30] even before the recent conflict with Iran, and CISA has issued a recent advisory[31] warning that Iranian hackers are targeting U.S. energy and water suppliers. Although the hacks against water infrastructure have so far proven relatively minor, it is worth noting that these water plants typically contain large amounts of chlorine, which would be toxic if released. In addition, before the Chemical Facility Antiterrorism Standards lapsed, CISA ran a Personnel Surety Program (PSP),[32] which screened facility personnel and unescorted visitors to high-risk chemical facilities, and which with regularity identified people with terrorist ties who sought access to restricted areas and critical assets at high-risk chemical facilities.[33]

The Aggregation Problem: Why a Centralized Database Is More Dangerous Than Facility-Level Disclosure

The proposal's central mechanism — consolidating RMP data into a single, publicly accessible, searchable federal database — does not merely replicate the security vulnerabilities created by the 2024 SCCAP Rule. It compounds them in a manner that intelligence and security professionals will immediately recognize as the aggregation problem: the phenomenon by which individually innocuous data points, when consolidated into a single repository, produce an intelligence product of substantially greater value to adversaries than the sum of its parts.

Under the SCCAP Rule, a determined adversary seeking to identify high-value chemical targets would have been required to visit thousands of individual facility disclosures, correlating information manually across disparate sources. This friction was not incidental — it was a meaningful, if imperfect, security feature. The proposed centralized, searchable database eliminates that friction entirely. A single query can now return facility location, regulated substance inventory, off-site consequence analysis, and accident history across thousands of facilities simultaneously, effectively generating the kind of target-selection product that a

---

[29] Easterly, J. & Fanning, T. *The Attack on Colonial Pipeline: What We've Learned and What We've Done Over the Past Two Years*. CISA Blog, May 7, 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[30] *E.g.*, Nickel, D. & Miller, M. (2026, April 7). *Iranian hackers are targeting US energy and water sectors, federal agencies warn*. POLITICO. https://www.politico.com/news/2026/04/07/iranian-hackers-energy-water-cybersecurity-00862018.

[31] Cybersecurity and Infrastructure Security Agency. (2026, April 7). *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[32] U.S. Cybersecurity and Infrastructure Security Agency, "Chemical Facility Anti-Terrorism Standards; Personnel Surety Program Implementation Notice," *Federal Register*, Vol. 84, No. 131 (July 9, 2019), p. 32,768.

[33] *See* U.S. Cybersecurity and Infrastructure Security Agency. *Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program*. https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/personnel-surety-program.

sophisticated adversary's reconnaissance phase would otherwise require significant time, resources, and potential exposure to produce.

The U.S. Department of Justice recognized this precise threat in its 2000 assessment, warning that internet consolidation of OCA data posed the greatest risk of exploitation precisely because it allowed relevant information to be aggregated in a single, anonymously accessible location. That warning was issued before the era of large language models, automated data harvesting, and AI-assisted target analysis — tools that dramatically lower the technical barrier to extracting actionable intelligence from consolidated public databases. EPA should confront directly the question of whether a centralized, searchable database of hazardous chemical facilities, accessible without authentication or identity verification, is consistent with the agency's statutory obligation to minimize, rather than facilitate, the consequences of potential chemical releases. On that question, the 2000 DOJ assessment provides a clear answer, and the intervening twenty-five years have done nothing to weaken it.

Cyber-Physical Convergence: How Public RMP Data Enables the Modern Threat

The threat to chemical facilities is no longer primarily physical. The convergence of cyber and physical attack vectors has fundamentally altered the risk calculus that EPA must apply when evaluating the security implications of public information availability. When EPA last issued a rule protective of RMP information, in 2019, the cyber-physical threat to critical infrastructure — while recognized — had not yet manifested in the dramatic and public ways it subsequently has. The threat environment has materially deteriorated since then, and EPA's analysis must account for this deterioration.

The modern attack sequence against critical infrastructure frequently does not begin at the fence line or the control room. It begins with open-source intelligence collection. Sophisticated threat actors — whether nation-state, criminal, or terrorist — conduct extensive reconnaissance before committing resources to an operation. They seek to identify facilities handling the most hazardous substances in the largest quantities, located in proximity to dense population centers, with histories of prior incidents suggesting existing vulnerabilities, and with emergency response profiles that suggest limited capacity to contain a release. The proposed EPA database, as structured, provides each of these data points in a single, queryable, unauthenticated interface.

This is not a theoretical concern. As CISA has documented, the People's Republic of China's Volt Typhoon campaign has been specifically focused on pre-positioning within U.S. critical infrastructure — not for immediate disruption, but to develop the targeting intelligence and persistent access that would enable rapid, coordinated infrastructure attacks in the event of a future conflict. The selection of which infrastructure to target is itself an intelligence function,

and EPA should understand that a publicly searchable database of high-consequence chemical facilities, cross-referenced against population exposure data, is precisely the kind of open-source resource that supports that function — at no cost and no risk to the adversary conducting the reconnaissance.

For facilities covered by the RMP that also operate industrial control systems — which include the majority of larger and higher-consequence facilities — the combination of publicly available substance and quantity data with operational technology that is increasingly networked and frequently inadequately secured represents a convergent vulnerability that EPA is not equipped to assess independently. EPA should therefore defer to CISA's expertise on this question, and should not promulgate public disclosure requirements over CISA's objection. The interagency record from the 2024 SCCAP rulemaking makes clear that the U.S. Department of Homeland Security and Department of Justice (DOJ) raised precisely these concerns and were substantially overridden. That outcome was a mistake then; repeating it now, with a threat environment that has only grown more acute, would be a serious analytical and institutional failure.

Fortunately, none of these latent or exploited vulnerabilities have so far resulted in a chemical release. However, U.S. critical infrastructure, including chemical infrastructure, remains actively targeted both by State and by non-State actors. Indeed, in this context it is critical to note that the U.S. Government Accountability Office has identified high-risk chemical facilities as a potentially rich cybersecurity target for terrorists, criminals, and foreign States.[34] Further, DOJ did provide, in the months leading up to 9/11, a comprehensive analysis on the dangers inherent in posting off-site consequence analysis (OCA) information for chemical facilities on the internet.[35]

This DOJ report, commissioned just months before 9/11, noted that "in the last two years alone there have been two incidents involving domestic terrorist groups planning to cause industrial chemical releases for terroristic purposes."[36] This is interesting as a publicly available acknowledgement of exactly the kind of foiled threat would not be included in the public database on which the 2021 study that EPA cited relied. DOJ also noted the attractiveness of chemical facilities as a terrorist target, given that causing a chemical release would be a "relatively simple" way to cause an attack with the power of a Weapon of Mass Destruction, and DOJ also noted that "[o]f the nearly 15,000 facilities that have submitted OCA data, almost half

[34] U.S. Government Accountability Office. (2020, May 14). *Critical Infrastructure: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities* (GAO-20-453). https://www.gao.gov/assets/gao-20-453.pdf.
[35] U.S. Department of Justice, April 18, 2000. Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the internet.
[36] *Id.* at p.3.

report that over 1,000 people live in zones that could be affected by the release of toxic chemicals from those facilities."[37]

Although the DOJ report was limited, by the terms of the RMP statute, to OCA information, the insights apply more broadly. Information on weaponizing chemicals has long been publicly available. It is true, as many commenters have stated, that comprehensive information on how to weaponize chemicals can readily be found online. However, "Internet access poses the greatest risk that OCA data will be used in relation to an attempted industrial chemical release."[38] This is true, not merely because the internet makes information readily discoverable, but potentially does so in a way that allows relevant information to be consolidated in a single database, which can effectively provide bad actors a signal as to where to concentrate their efforts. Moreover, the internet allows such bad actors to access and search this information anonymously.

In the 2024 SCCAP Rule, EPA did not meaningfully justify its departure from its reasoned conclusion in its 2019 Final Rule,[39] issued during the previous Trump administration, that requiring heightened RMP disclosure to the general public would increase security risks.[40] During the rulemaking process leading up to the 2024 SCCAP Rule, EPA largely dismissed critical interagency comments from the U.S. Department of Homeland Security and the U.S. Department of Justice, along with other agencies, which identified security risks in the information made available, as was seen in the OMB Redline that was included on the docket leading up to the 2024 SCCAP Rule. As the Redline edits made clear, the security agencies were deeply concerned by the information being made available, and the risk profile has not measurably improved since 2024; if anything, threats to U.S. security interests are as concerning as ever.

At a time when critical infrastructure, including chemical infrastructure, is growing more rather than less vulnerable to disruption, as cyber threats expand the risk landscape dramatically and as the risks from nation state actors appear to be on the rise, even as the threat from terrorists and criminals remain at least as strong as ever, it is deeply concerning that EPA would cite the lack of domestic chemical terrorist incidents since the 1970's as a reason not to be concerned. Chemical plants remain deeply vulnerable to threats from terrorists and bad actors,[41] and EPA

---

[37] *Id.* at p.2.
[38] *Id.* at p.4.
[39] U.S. Environmental Protection Agency, Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act," *Federal Register*, Vol. 84, No. 244 (December 19, 2019), p. 69,834.
[40] 84 Fed. Reg. at 69,844.
[41] Lippin TM, McQuiston TH, Bradley-Bull K, Burns-Johnson T, Cook L, Gill ML, Howard D, Seymour TA, Stephens D, Williams BK. Chemical plants remain vulnerable to terrorists: a call to action. Environ Health Perspect. 2006 Sep; 114(9):1307-11. doi: 10.1289/ehp.8762. PMID: 16966080; PMCID: PMC1570090. https://pmc.ncbi.nlm.nih.gov/articles/PMC1570090/

should account deeply with this reality before requiring the public disclosure of sensitive information related to chemical facilities.

b. *FOIA does Not Require Disclosure at the Scale that EPA Contemplates*

When balancing transparency against the security interests inherent in the chemical sector, it is critical to bear in mind that FOIA does not require, or even call for, proactive public disclosure in an electronic format. Rather, FOIA requires that agencies make available for inspection in a public format copies of records that previously *have* been requested pursuant to FOIA,[42] *and* which have been requested three or more times.[43] Thus, the requirement for public availability under this statutory provision does not require EPA proactively to provide all the RMP information in a publicly searchable database, particularly not information that has yet to be requested for the requisite number of times.

To give a sense of the size of the chemical sector, during the lifetime of CFATS, CISA received top-screen submissions from more than 45,000 unique chemical facilities, and at the time of lapse regulated 3,242 such facilities as high-risk.[44] According to EPA, the number of facilities covered by the RMP falls between these numbers, at approximately 12,000 facilities as of the end of 2019.[45] Understanding that the overlap between these facilities and those regulated by EPA may be imperfect, this would essentially mean that nearly 10,000 FOIA requests would have to be received before every former CFATS high-risk facility could possibly be required to be made proactively available; and the number would rise to 36,000 separate FOIA requests to include the broader universe of facilities covered by the EPA RMP generally. These numbers, as high as they are, do not take into account the statistical certainty that any FOIA requests would not be equally distributed; there would naturally be more interest in some facilities than in others, so the total number of FOIA requests that would be required, before FOIA could be argued to require proactive disclosure across the entire chemical sector, would in fact be significantly higher.

In other words, FOIA would not require the proactive disclosure of this information in the kind of public directory that EPA envisions. At most, FOIA would be an excuse. A public directory that provided limited information regarding facilities that had reached the statutorily

---

[42] 552 U.S.C. § 552(a)(2)(D)(i) (emphasis added).
[43] 552 U.S.C. § 552(a)(2)(D)(ii)(II).
[44] U.S. Cybersecurity and Infrastructure Security Agency. *Chemical Facility Anti-Terrorism Standards (CFATS) Monthly Statistics.* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/monthly-statistics#:~:text=Current%20Statistics,more%20about%20the%20CFATS%20Process.
[45] U.S. Environmental Protection Agency. (2020, April). *Clean Air Act Section 112(r): Accidental Release Prevention/Risk Management Plan Rule.* [Fact Sheet]. https://www.epa.gov/sites/default/files/2020-03/documents/caa112_rmp_factsheet_march_2020_final.pdf

prescribed number of requests in the past would be less of a security risk, and would fully comply with FOIA's provisions regarding electronic public disclosure.

c. *Federal Custodianship of the Proposed Database Does Not Cure Its Security Deficiencies*

A recurring premise of EPA's proposal is that federal retention of RMP data, and federal control over its disclosure, is inherently more secure than facility-level disclosure. This premise is not self-evident, and the recent record of intrusions into federal information infrastructure should cause EPA to examine it carefully before embedding it as a foundational assumption of a national chemical security policy.

The compromise of U.S. telecommunications infrastructure by the People's Republic of China, in the operation publicly attributed to Salt Typhoon, demonstrated that sophisticated nation-state actors have achieved persistent, broad access to networks that undergird federal government communications. Salt Typhoon's intrusion extended to systems used by law enforcement and national security agencies — precisely the entities whose communications one would expect to be most robustly protected. If those systems proved vulnerable, the assumption that an EPA-managed public database of 12,000 chemical facilities will be securely administered and access-controlled requires explicit justification, not mere assertion.

This concern is amplified by the proposal's contemplation of a publicly accessible, on-demand online tool for RMP data. A database that is, by design, publicly accessible cannot rely on access controls as a security mechanism. Once the data is made publicly available, federal custodianship provides no meaningful security benefit — the information is as available to a hostile foreign intelligence service as it is to a community resident. EPA should be candid about this limitation rather than using federal custodianship as a rhetorical substitute for genuine security analysis. The question is not who holds the database, but what information the database contains and who can access it — and on both counts, the proposal as structured does not provide adequate protection.

Equally important, and less frequently discussed in public regulatory proceedings, is the insider threat: the risk that individuals with authorized access to sensitive federal databases will misuse that access, whether through malicious intent, susceptibility to foreign recruitment, or compromise through social engineering or coercive means. The Chemical Facility Anti-Terrorism Standards Personnel Surety Program, administered by CISA prior to the statute's lapse, screened facility personnel and unescorted visitors to high-risk chemical facilities and with regularity identified individuals with terrorist ties seeking access to restricted areas. That program addressed the insider threat at the facility level. No analogous screening mechanism

exists for personnel with access to a federal database containing the consolidated vulnerability profiles of thousands of high-risk chemical facilities.

Foreign intelligence services, including those of the PRC, Iran, and Russia, actively recruit or coerce individuals with access to sensitive U.S. government databases. A database consolidating the location, substance inventory, OCA data, and accident history of 12,000 chemical facilities would represent a high-value collection target for any of these services. The value of that collection target increases precisely as the database becomes more comprehensive and more easily queryable — both features that the proposal promotes. EPA should address directly how it intends to manage insider threat risk to the proposed database, and should seek input from CISA and the Office of the Director of National Intelligence before finalizing any centralized disclosure mechanism.

d. *Public Disclosure Requirements Undermine the Voluntary Information-Sharing Architecture That National Infrastructure Security Depends Upon*

Congress recognized, in enacting the Critical Infrastructure Information Act of 2002 as part of the Homeland Security Act, that owners and operators of critical infrastructure would not voluntarily share sensitive vulnerability information with the federal government unless that information was specifically protected from public disclosure. This recognition produced the Protected Critical Infrastructure Information (PCII) program, administered by CISA, which provides robust protection against FOIA disclosure and other compelled release for voluntarily submitted critical infrastructure information. The explicit legislative premise of the PCII program is that voluntary information sharing — which is essential to effective national infrastructure security — will not occur if the act of sharing exposes sensitive information to public availability.

The 2024 SCCAP Rule, and to a lesser extent the current proposal, undermines this premise in the chemical sector. Although RMP submissions are themselves compelled rather than voluntary, EPA's posture toward disclosing compelled submissions signals to industry that the federal government's commitments to protect voluntarily submitted information in related contexts are not reliable. When EPA compels chemical facilities to submit detailed vulnerability-relevant information and then makes that information publicly available, it sends an unambiguous message to the broader critical infrastructure community: information shared with the federal government in a regulatory context will be used against the submitter's security interests. The corrosive effect of this message extends well beyond EPA's regulatory authority. CISA's entire voluntary information-sharing architecture — including the chemical sector's participation in sector-specific information-sharing programs — depends on the credibility of the federal government's commitment to protecting sensitive infrastructure information. EPA's approach directly undermines that credibility.

Moreover, there is a practical consequence that EPA has not addressed: facilities that anticipate public disclosure of their RMP submissions have strong incentives to minimize the specificity and accuracy of what they submit. A regulatory framework that creates incentives for underreporting does not advance safety or security — it degrades the quality of the information available to emergency responders, regulators, and the intelligence community alike. EPA should recognize that the voluntary information-sharing model that CISA, FBI, and partner agencies depend on is a national security asset, and that its erosion in the chemical sector, driven by EPA's disclosure approach, imposes costs that extend far beyond EPA's regulatory mission.

e. *Congress did Not Legislate the RMP as a Public Disclosure or Right-to-Know Program*

Two other statutory points are worth reinforcing in this regard. First, the EPA RMP is not a public disclosure or right to know program. The EPA RMP, as set forth in Section 112(r) of the Clean Air Act,[46] simply requires the owners and operators of stationary[47] chemical facilities to identify potential hazards that may be caused by release of their chemicals, design and maintain safe facilities to prevent such releases, and to minimize the consequences of accidental releases that do occur.[48] In order to do so, the statute requires facilities that contain a threshold amount[49] of certain listed, hazardous substances[50] to prepare and implement risk management plans under EPA's auspices.[51] The risk management plan[52] must include a hazard assessment,[53] prevention program,[54] and emergency response program in case that an accidental release occurs.[55]

The statute is quite detailed as to what each aspect of the program should include. The hazard assessment includes an estimate of potential release quantities and downwind effects, including potential exposures to affected populations, with a variety of specific items to be included.[56] The prevention program requires safety precautions and maintenance, monitoring, and employee training measures to be used at the source,[57] and the emergency response program

[46] Clean Air Act Amendments of 1990, Pub. L. No. 101-549, § 112(r), 104 Stat. 2399 (codified at 42 U.S.C. § 7412(r)).
[47] 42 U.S.C. § 7412(r)(2)(C).
[48] 42 U.S.C. § 7412(r)(1).
[49] 42 U.S.C. § 7412(r)(5).
[50] 42 U.S.C. § 7412(r)(3).
[51] 42 U.S.C. § 7412(r)(7).
[52] 42 U.S.C. § 7412(r)(7)(B)(ii).
[53] 42 U.S.C. § 7412(r)(7)(B)(ii)(I).
[54] 42 U.S.C. § 7412(r)(7)(B)(ii)(II).
[55] 42 U.S.C. § 7412(r)(7)(B)(ii)(III).
[56] 42 U.S.C. § 7412(r)(7)(B)(ii)(I).
[57] 42 U.S.C. § 7412(r)(7)(B)(ii)(II).

must include procedures for informing the public and local agencies responsible for responding to accidental releases, emergency healthcare, and employee training measures.[58]

None of these provisions even mention the public availability or disclosure of any information provided under the program. In fact, the only disclosure requirements here are to EPA itself, with the owner or operator of the chemical facility in question required to register the risk management plan with EPA.[59] There is an old canon of statutory interpretation: *expressio unius est exclusio alterius* – to express one thing is to exclude the others.[60] Mentioning one thing implies exclusion of another.[61] This principle has been endorsed by the Supreme Court as well, broadly enough that the Court typically doesn't see the need to belabor the point.[62]

Congress could easily have included a disclosure to the general public as well here, yet there are no such requirements to be found in the RMP statute. Given that the RMP statute merely requires disclosure to EPA, without even mentioning disclosure to the general public, it seems like a straightforward instance of regulatory overreach for EPA to use the RMP statute to justify a public disclosure requirement, particularly given how public availability of this information undercuts the very safety and security goals that the RMP statute is meant to promote. To the extent that EPA would argue that FOIA requires any disclosure not specifically envisioned in the RMP statute, EPA should administer such requirements in its FOIA regulations,[63] rather than shoehorn them into an RMP regulatory program where such requirements do not belong.

f. *Requiring Public Disclosure Distorts EPA's Obligations Under EPCRA*

The fact that the RMP statute is not a public disclosure statute is further underlined by the fact that there actually does exist a separate right-to-know statute governing chemical facilities, namely the Emergency Planning and Community Right-to-Know Act (EPCRA).[64] Many of the reporting requirements that EPA has promulgated for the RMP appear to be duplicated from the EPCRA requirements rather than the RMP statute[65]--yet crucially, EPCRA requires that facilities share this information to their local emergency planning committees (LEPCs) upon request, not to the general public.[66] Any information disclosed to the general

[58] 42 U.S.C. 7412(r)(7)(B)(ii)(III).
[59] 42 U.S.C. 7412(r)(7)(B)(iii).
[60] *Burgin v. Forbes*, 169 S.W.2d 321, 325; Newblock v. Bowles, 170 Okl. 487, 40 P.2d 1097, 1100.
[61] Black's Law Dictionary, 6th ed., p. 581.
[62] *E.g.*, *TRW Inc. v. Andrews*, 534 U.S. 19, 28 (2001) (*citing Leatherman v. Tarranty Cty. Narcotics Intelligence & Coordination Unit*, 507 U.S. 163, 168 (1993)).
[63] Title 40, Chapter I, Subchapter A, Part II.
[64] Emergency Planning and Community Right-to-Know Act of 1986, Pub. L. No. 99-499, 100 Stat. 728 (codified as amended at 42 U.S.C. §§ 11001-50).
[65] 42 U.S.C. §§ 11021-22.
[66] 42 U.S.C. §§ 11021(a), 11022(a).

public is meant, under EPCRA, to be mediated through the LEPCs,[67] and in certain instances requires that the requester explain their need for the information requested.[68]

Congress enacted EPCRA in 1986, nearly 20 years after first enacting FOIA in 1967. Yet rather than simply allow this information to be covered by FOIA procedures, Congress created a distinct scheme, under which any collected information would be shared at the first instance with LEPCs, which are directly charged with planning responses to accidental chemical releases, and to receiving and processing requests from the public for the information provided in EPCRA.[69] Given that Congress only authorized this information to be provided through the specific, limited procedures established in EPCRA, EPA would effectively undermine that Congressional intent by first replicating the required EPCRA information in the separate, unrelated RMP statute, and secondly by requiring public disclosure of that information, even when the RMP statute contains no provisions requiring, or even contemplating, public disclosure.

This is particularly true given that much of the information required by the RMP proposal here appears to be replicated from EPCRA, without any specific statutory authorization requiring this disclosure. This is especially the case for the required disclosure of the Safety Data Sheets[70] and hazardous chemical inventory.[71] EPA's interpretation of the RMP statute would effectively render EPCRA redundant, if the information shared to LEPCs under that act is required to be disclosed in a publicly available database anyway.

As the Supreme Court has held, "It is a basic principle of statutory construction that a statute dealing with a narrow, precise, and specific subject is not submerged by a later enacted statute covering a more generalized spectrum."[72] Likewise, "Where there is no clear intention otherwise, a statute will not be controlled or nullified by a general one, regardless of the priority of enactment."[73]

Here, EPCRA is the statute that governs the public disclosure of chemical hazard information. Section 112(r) of the Clean Air Act is simply a general accident prevention provision that does not even mention public disclosure. EPA cannot and should not use section 112(r) of the Clean Air Act to override EPCRA's preexisting, carefully calibrated disclosure framework, absent some concrete, affirmative showing that Congress meant to alter the preexisting EPCRA framework. For EPA to do so first by replicating EPCRA's requirements in the RMP, which makes no specific reference to the information that EPCRA requires, and then

[67] 42 U.S.C. §§ 11021(c)(2), 11022(e)(3).
[68] 42 U.S.C. § 11022(e)(3)(C).
[69] 42 U.S.C. § 11001(c).
[70] 42 U.S.C. §11021.
[71] 42 U.S.C. § 11022.
[72] *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 153 (1976).
[73] *Id.* (citing *Morton v. Mancari*, 417 U.S. 535, 550-51 (1974)).

by requiring public availability of that information where nothing in Section 112(r) of the Clean Air Act requires it, does not implement the scheme for chemical hazard disclosure that Congress created, but rather distorts it. By the same token, EPCRA is more specific, to the chemical industry, than the FOIA statute at large that EPA would use to largely make the EPCRA disclosure channel redundant.

EPA administers both the RMP statute and EPCRA, and should read both statutes together. The best reading of the statutes, in conjunction, is that EPCRA information is limited to LEPCs, and to members of the public who request information from the LEPCs pursuant to that statute. Any other information should not be provided to the general public through the RMP, which after all is not a disclosure statute, unless EPA can articulate specific reasons why the availability of that information, in a publicly available and searchable format, is germane to the RMP statutory aims. The fact that much of this information is already available through EPCRA undermines the policy case for public disclosure through the RMP. To the extent that EPA considers EPCRA's procedures to be insufficient, the correct response by EPA would be to flesh out the EPCRA regulations, not the creation of a novel public disclosure program through the RMP statute.

Finally, it is worth noting that the duplicating EPCRA reporting requirements in the RMP arguably violates the Paperwork Reduction Act's[74] provisions requiring the Government to limit information burdens on the public created through unnecessary duplication.[75] Moreover, to the extent that members of the public try to obtain chemical hazard information not already covered by EPCRA, chemical facilities would have a strong argument to invoke Exemption 4 of FOIA, which provides an exemption from FOIA for privileged and confidential commercial information obtained from regulated stakeholders.[76] Given that chemical facilities treated similar information as CVI under CFATS, a strong argument based on the sensitivity of the information is viable. At a minimum, given the security concerns at issue, EPA should not cite FOIA as a requirement to proactively divulge this information, given that chemical hazard information is more directly governed by EPCRA, and that it is not even clear that FOIA would apply to any chemical hazard information obtained by EPA that falls outside EPCRA's scope.

Suggested Changes to Proposal

Any information that EPA provides about chemical facilities, pursuant to the RMP, should be grounded in the specific provisions, or at least the accident prevention and mitigation goals, of the RMP statute. The actual information that communities need is what to do in case of

[74] Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501-21).
[75] 44 U.S.C.§ 3506(c)(3)(B).
[76] 5 U.S.C. § 552(b)(4).

an accident (or security breach). Members of the general public really do not need to know the specific technical data of the hazardous chemicals, or information about specific vulnerabilities, which can be exploited. To the extent that activists might use access to this information to pressure companies, or in EPA's words, add to "community pressure and oversight,"[77] this is not an appropriate use of the RMP statute.

As such, EPA's RMP regulations should not provide to the general public any information beyond: (i) the names of regulated substances above the threshold amounts; and (ii) the contact information for relevant local authorities, which would include officials on the LEPCs that serve as intermediaries under EPCRA.

The Safety Data Sheets (SDS) should not be included on the list of information to be made publicly available. Congress specifically provided for SDS disclosure to LEPCs, rather than to the general public, in Section 311 of the EPCRA.[78] These are highly technical, complex documents, which most members of the public could not even readily comprehend. Congress's decision to provide a mechanism to relay this information to LEPCs, which are best situated to respond to emergencies, does not apply to the general public. As such, EPA's proposal to include this information is duplicative of EPCRA's requirements, and distorts the framework that Congress created when they provided for disclosure of this information to LEPCs and local governments. Thus, this information should not be part of any public availability requirement through the RMP.

Similarly, the hazardous chemical inventory should not be included in any information to be made publicly available. Congress specifically provided for the disclosure of the amount, location, and potential hazards of any hazardous chemical inventory to LEPCs, rather than to the general public, in Section 312 of the EPCRA.[79] Once again, it distorts the framework for disclosure to LEPCs, and for using the LEPCs as intermediaries for any further public disclosure, as created in EPCRA, simply to duplicate this requirement for the general public through the RMP. As such, this information should be dropped from any public availability requirement through the RMP.

Similarly, EPA should not include the accident history in any requirement for the availability of public information. Providing a list of hazardous substances (the disclosure of which Congress has provided for LEPCs rather than the general public), along with a five-year accident history, gives bad actors an effective roadmap to vulnerabilities that exist, not only within the chemical facility in question, but to others that may be similarly situated.

[77] 87 Fed Reg. at 53,574.
[78] 42 U.S.C. § 11021.
[79] 42 U.S.C. § 11022.

Finally, the list of scheduled exercises should be excluded as well. Unless EPA can articulate how the inclusion of this information in a public disclosure plan would improve the safety of chemical plants, or mitigate the effects of an accidental release, it makes little sense to include public disclosure of this information as part of the RMP.

Conclusion

EPA's decision to remove the disclosure burden from the owners and operators of chemical facilities represents a welcome development that will reduce their regulatory burden promote uniformity in disclosure. However, the 2024 SCCAP Rule created vulnerabilities in expanding the amount of information about hazardous chemical facilities made available to the general public. By instead consolidating the required disclosures into a publicly available and searchable database, the proposal does not go far enough in undoing the risk that the 2024 SCCAP Rule created to the general public. In fact, by using a publicly accessible, central repository, the proposal would arguably worsen the security vulnerabilities created by the 2024 SCCAP Rule, in exactly the way that the 2000 DOJ Report warned against.

To the extent that EPA is able to reconcile greater security of the information regarding hazardous chemical facilities with its responsibilities under the RMP, EPCRA, and FOIA statutes, we would encourage EPA to do so. For the reasons above, we are confident that a full analysis of EPA's responsibilities under its various authorizing statutes, along with recognition of the security risks inherent in the overly broad dissemination of this information, would lead EPA to conclude that they should in fact limit the public availability of this information as discussed.

We are grateful for the opportunity to comment on this proposal.

Respectfully yours,

Bridget Bean
Visiting Fellow, The Heritage Foundation
Fmr. Executive Director, Cybersecurity and Infrastructure Security Agency[80]

Trevar D. Kolodny
Visiting Fellow, The Heritage Foundation
Fmr. Senior Policy Analyst, Office of Chemical Security, Cybersecurity and Infrastructure Security Agency[81]

[80] Institutional affiliations provided for identification purposes only. This comment reflects the individual views of the author, and not the institutional position of either The Heritage Foundation or CISA.
[81] *Id*