of access. It also requires the Director of the Office of Management and Budget to designate a single website for accessing all agency guidance documents, except for those exempt from disclosure under the FOIA.

Democrats support a transparent Federal Government that is always accountable to the public, so we support this bill, as well. We don't buy into the incendiary rhetoric of some MAGA Republicans trying to paint agency guidance documents as some kind of sinister tool of the administrative state. They are the very opposite.

My Republican colleagues have said that this bill is important because it restores elements of President Trump's Executive Order No. 13891 that was revoked by President Biden.

To set the record straight, President Biden replaced that executive order—he didn't revoke it—because it sought to limit the Federal Government's ability to address the country's challenges and serve its people. Instead, President Biden launched an important effort to modernize the regulatory review process, including the process around guidance documents, which we are addressing today.

Let's be very clear: Republicans are dead set on rolling back the ability of Federal agencies to protect the public from corporate bad actors. In contrast, Democrats are putting people before profits, including through evidence-based regulations that protect Americans' freedoms and well-being.

Passage of this bill today is a good step in the right direction, as long as we all actually are interested in regulatory transparency and accountability.

Mr. Speaker, I urge my colleagues to support the bill, and I am happy to join them. I reserve the balance of my time.

Mr. COMER. Mr. Speaker, I yield 2 minutes to the gentleman from California (Mr. KILEY).

Mr. KILEY of California. Mr. Speaker, the basic premise of this bill, which I am happy to cosponsor, is that we should not have secret laws in the United States.

A major opportunity that we have right now is to modernize our government and to rein in the inexorable growth of the administrative state, restoring power to our elected representatives, States, local communities, and the American people themselves.

When we think about the administrative state, we think about all the regulations that are churned out, one after another, and compiled in the ever-growing Federal Register. The reality is, that is just the tip of the iceberg. Layered on top of all of that are these so-called guidance documents. These are memos, Dear Colleague letters, bulletins, all manner of what is referred to as ''regulatory dark matter.''

With respect to the ranking member, this is not a melodramatic term. It is actually quite appropriate. In physics, ''dark matter'' refers to the mysterious substance that makes up about 85 percent of the mass of the universe, but no one really knows what it is. Similarly, all of these guidance documents make up a great deal of the regulatory activity in our country, yet the agencies themselves can't even manage to track them down. How is an individual or a small business supposed to find out what this particular interpretation of the law is and how it will affect them, let alone how Congress is supposed to figure out how the laws that we have passed are ultimately being enforced and administered?

This is a commonsense measure that says that all of these guidance documents, which have real teeth when it comes to the enforcement of regulations, need to be compiled in one place that is searchable and accessible to every American citizen. It is a positive step for transparency and toward restoring government by the people.

Mr. CONNOLLY. Mr. Speaker, I have no further speakers. I urge passage of H.R. 1515, and I yield back the balance of my time.

Mr. COMER. Mr. Speaker, I urge my colleagues to support the Guidance Out Of Darkness Act, or GOOD Act, and to pass this legislation once again, like the House did in the last term. I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Kentucky (Mr. COMER) that the House suspend the rules and pass the bill, H.R. 1515.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

FEDERAL CONTRACTOR CYBERSECURITY VULNERABILITY REDUCTION ACT OF 2025

Mr. COMER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 872) to require covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 872

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025''.

SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLOSURE POLICY.

(a) RECOMMENDATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Director of the National Institute of Standards and Technology, and any other appropriate head of an Executive department, shall—

(A) review the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs; and

(B) recommend updates to such requirements and language to the Federal Acquisition Regulation Council.

(2) CONTENTS.—The recommendations required by paragraph (1) shall include updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

(b) PROCUREMENT REQUIREMENTS.—Not later than 180 days after the date on which the recommended contract language developed pursuant to subsection (a) is received, the Federal Acquisition Regulation Council shall review the recommended contract language and update the FAR as necessary to incorporate requirements for covered contractors to receive information about a potential security vulnerability relating to an information system owned or controlled by a contractor, in performance of the contract.

(c) ELEMENTS.—The update to the FAR pursuant to subsection (b) shall—

(1) to the maximum extent practicable, align with the security vulnerability disclosure process and coordinated disclosure requirements relating to Federal information systems under sections 5 and 6 of the IoT Cybersecurity Improvement Act of 2020 (Public Law 116–207; 15 U.S.C. 278g–3c and 278g–3d); and

(2) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely used standard.

(d) WAIVER.—The head of an agency may waive the security vulnerability disclosure policy requirement under subsection (b) if—

(1) the agency Chief Information Officer determines that the waiver is necessary in the interest of national security or research purposes; and

(2) if, not later than 30 days after granting a waiver, such head submits a notification and justification (including information about the duration of the waiver) to the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(e) DEPARTMENT OF DEFENSE SUPPLEMENT TO THE FEDERAL ACQUISITION REGULATION.—

(1) REVIEW.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall review the Department of Defense Supplement to the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs and develop updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

(2) REVISIONS.—Not later than 180 days after the date on which the review required under subsection (a) is completed, the Secretary shall revise the DFARS as necessary to incorporate requirements for covered contractors to receive information about a potential security vulnerability relating to an information system owned or controlled by a contractor, in performance of the contract.

(3) ELEMENTS.—The Secretary shall ensure that the revision to the DFARS described in this subsection is carried out in accordance

with the requirements of paragraphs (1) and (2) of subsection (c).

(4) WAIVER.—The Chief Information Officer of the Department of Defense, in consultation with the National Manager for National Security Systems, may waive the security vulnerability disclosure policy requirements under paragraph (2) if the Chief Information Officer—

(A) determines that the waiver is necessary in the interest of national security or research purposes; and

(B) not later than 30 days after granting a waiver, submits a notification and justification (including information about the duration of the waiver) to the Committees on Armed Services of the House of Representatives and the Senate.

(f) DEFINITIONS.—In this section:

(1) The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) The term ''covered contractor'' means a contractor (as defined in section 7101 of title 41, United States Code)—

(A) whose contract is in an amount the same as or greater than the simplified acquisition threshold; or

(B) that uses, operates, manages, or maintains a Federal information system (as defined by section 11331 of title 40, United Stated Code) on behalf of an agency.

(3) The term ''DFARS'' means the Department of Defense Supplement to the Federal Acquisition Regulation.

(4) The term ''Executive department'' has the meaning given that term in section 101 of title 5, United States Code.

(5) The term ''FAR'' means the Federal Acquisition Regulation.

(6) The term ''NIST'' means the National Institute of Standards and Technology.

(7) The term ''OMB'' means the Office of Management and Budget.

(8) The term ''security vulnerability'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(9) The term ''simplified acquisition threshold'' has the meaning given that term in section 134 of title 41, United States Code.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kentucky (Mr. COMER) and the gentleman from Virginia (Mr. CONNOLLY) each will control 20 minutes.

The Chair recognizes the gentleman from Kentucky.

GENERAL LEAVE

Mr. COMER. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kentucky?

There was no objection.

Mr. COMER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I am happy to support H.R. 872, the Federal Contractor Cybersecurity Vulnerability Reduction Act.

Mr. Speaker, this bill will require Federal contractors to have a vulnerability disclosure policy, or VDP. This would help contractors more quickly alert Federal agencies about vulnerabilities, which could avoid a future cybersecurity breach.

Federal agencies must act quickly when dealing with a cyberattack. The sooner a Federal agency knows that it may have a problem, the sooner it can take steps to protect its systems and data, including the personal data of millions of Americans.

It is reasonable to require Federal contractors to play a proactive role in addressing vulnerabilities in Federal information systems. This bill complements the committee's ongoing work aimed at helping Federal agencies protect their data and information systems.

Mr. Speaker, I thank our great Cybersecurity, Information Technology, and Government Innovation Subcommittee chairwoman, the gentlewoman from South Carolina (Ms. MACE), for introducing this important legislation, which the House Oversight and Government Reform Committee unanimously passed last year and the House later passed as part of the fiscal year 2025 National Defense Authorization Act.

I also thank the Cybersecurity, Information Technology, and Government Innovation Subcommittee ranking member, the gentlewoman from Ohio (Ms. BROWN), for cosponsoring this legislation, building on the bipartisan support from last year.

Mr. Speaker, I encourage my colleagues to support H.R. 872 once again, and I reserve the balance of my time.

Mr. CONNOLLY. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I appreciate today's consideration of the Federal Contractor Cybersecurity Vulnerability Reduction Act, as well as the work of Chairwoman MACE and Ranking Member BROWN in leading this legislation for us today.

The bill would ensure that Federal contractors implement vulnerability disclosure policies consistent with the guidance and guidelines of the National Institute of Standards and Technology, industry best practices, and international standards.

Mr. Speaker, each year, software developers, security researchers, and others discover tens of thousands of security vulnerabilities in computer software and systems. For example, in 2023 alone, more than 29,000 common vulnerabilities and exposures were logged in this widely used National Vulnerability Database.

If companies established a process for accepting, assessing, and managing reports of such vulnerabilities, otherwise known as vulnerability disclosure policies, they can make use of such discoveries to fix problems before they are exploited by malign actors.

Vulnerability disclosure policies are an extremely effective tool. Most Federal agencies already have such policies, as do Federal contractors and subcontractors providing information systems and Internet of Things devices to Federal agencies.

By requiring all Federal contractors to follow suit, this bill shores up another front in the never-ending battle to protect the Federal Government's information systems and data and, thereby, the American public.

Mr. Speaker, I urge passage of the bill, and I reserve the balance of my time.

Mr. COMER. Mr. Speaker, I yield 10 minutes to the gentlewoman from South Carolina (Ms. MACE), the chairman of the Cybersecurity, Information Technology, and Government Innovation Subcommittee.

Ms. MACE. Mr. Speaker, I thank my friend and the distinguished chairman of the Committee on Oversight and Government Reform, the gentleman from Kentucky (Mr. COMER), for yielding. I thank both the chairman and the ranking member, Mr. CONNOLLY, for their leadership on this critical issue, not only in this congressional session but the last one, as well.

Mr. Speaker, I rise today in strong support of my bill, H.R. 872, the Federal Contractor Cybersecurity Vulnerability Reduction Act.

In 2020, the Office of Management and Budget directed Federal agencies to implement cybersecurity vulnerability disclosure policies. These policies enable third-party researchers and white hat hackers to work with the Federal Government to proactively identify and patch vulnerabilities in information systems before a cyberattack takes place.

Mr. Speaker, we all know how critically important it is, particularly with systems that are older than some of us in this room, that these vulnerability disclosure policies require these third parties to notify the Federal agency of any sensitive data they encounter, like personally identifiable information, financial information, proprietary information, or trade secrets.

This allows cybersecurity vulnerability to be addressed and data to be secured before it is exploited by malign actors, including our adversaries. My colleagues know that malign actors affiliated with China, Russia, Iran, and others are after us all day, every day, 365 days a year.

These vulnerability disclosure policies are critical to preventing cyberattacks on Federal systems.

This is an important step in Federal cybersecurity, but the work of Federal agencies is supplemented by millions of contractors working on behalf of Federal departments and agencies. The Federal Government awards over 11 million contracts annually, with many of those contractors having access to Federal systems and vast amounts of sensitive information, including personally identifiable information of American citizens.

My bill, the Federal Contractor Cybersecurity Vulnerability Reduction Act, will require the Office of Management and Budget, or OMB, to oversee updates to the Federal Acquisition Regulation to ensure that Federal contractors with access to Federal systems or who work with Federal data adopt these vulnerability disclosure policies, as well.

My bill also requires the Secretary of Defense to update the Defense Federal Acquisition Regulation Supplement to require the same cybersecurity vulnerability disclosure policies, safeguarding the personal information of our servicemembers and the information vital to our national security.

These updates shall be done consistent with the guidelines and best practices developed by the National Institute of Standards and Technology and simply require contractors to abide by the same cybersecurity standards as Federal agencies.

Federal contractors with access to government systems and data should have the same safeguards in place as the government itself, ensuring that Federal systems and data are protected and that security vulnerabilities are addressed.

Adoption of vulnerability disclosure policies by government contractors will help protect the sensitive data of American citizens and our national security.

My bill would close a crucial vulnerability and protect our Nation from malicious actors who seek to steal our data and harm our citizens.

Mr. Speaker, I am very pleased to see this bill passed out of the Oversight and Government Reform Committee unanimously last year by a vote of 42–0. It is long past time we get this done. Until these vulnerability disclosure policies are adopted across the entire Federal digital ecosystem, our Nation's data and security are at risk.

Mr. Speaker, before I urge my colleagues to support this bill, I will say I walked into the Chamber this afternoon moments ago, and I saw a tweet or a post on X from South Carolina Attorney General Alan Wilson, who said his protecting South Carolinians from sexual predators is a top priority. Protecting citizens of this country has been my top priority since the day I was ever sworn into office, particularly my constituents whom I represent.

I recently gave a speech on this floor where I was very detailed about horrific abuses I have experienced. When you talk about vulnerabilities, I know about being vulnerable.

When you talk about cybersecurity, I sit awake in my bed every single night wondering if anyone has ever seen those videos of me or any of the other women in the tapes that I outlined in my speech.

In the last 3 weeks since I came forward and gave that speech on the floor, my attorney general, Alan Wilson—and I am going to make sure every South Carolinian knows your name forever, not just for what you did but for what you have not done, your inaction on vulnerabilities of my own constituents in my district in South Carolina. You have done nothing in the last 3 weeks except attack me, a Member of Congress, who, in my duty, did my duty to protect her constituents.

□ 1600

I will keep fighting for every American citizen whether it is in this bill about vulnerability disclosure policy and Federal Government. I will do it for rape victims not just in my district, but in my State and in my country. I will do it because I care. I swore an oath to the Constitution to serve my constituents, to serve my State, and to serve my Nation every possible way that I can.

Mr. Speaker, I urge my colleagues to take cyber threats by malign actors seriously. I urge my colleagues to protect the security of Americans' data. I urge my colleagues to do whatever we can in this Chamber to protect people who are vulnerable, whether we are talking about data or we are talking about rape victims, sex trafficking, all those things.

Victims should not be attacked ever, and I am one of those victims. I am tired of being attacked by the attorney general. I am tired of being blamed for being a rape victim and being a victim of Peeping Toms and voyeurism, same with these other victims. I am tired of it. I will not stand for it, not in this Chamber, not in my State, and not back home.

Attorney General Alan Wilson, I hope you have your No. 2 pencil out, and I hope you are taking notes. I hope that pencil is sharpened because, once I get my teeth stuck in you, I am not letting go. I will fight for every woman and girl across this country all day every day always.

The SPEAKER pro tempore. Members are reminded to address their remarks to the Chair.

Mr. CONNOLLY. Mr. Speaker, I support H.R. 872 and urge its adoption.

Mr. Speaker, I yield back the balance of my time.

Mr. COMER. Mr. Speaker, I urge my colleagues to support this important legislation, which will streamline cybersecurity vulnerability disclosure to protect Federal IT systems.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Kentucky (Mr. COMER) that the House suspend the rules and pass the bill, H.R. 872, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

SAFE AND SMART FEDERAL PURCHASING ACT

Mr. COMER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 856) to require the Director of the Office of Management and Budget conduct a review to determine the impact of the lowest price technically acceptable source selection process on national security, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 856

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Safe and Smart Federal Purchasing Act''.

SEC. 2. REVIEW TO DETERMINE THE IMPACT OF THE LOWEST PRICE TECHNICALLY ACCEPTABLE SOURCE SELECTION PROCESS ON NATIONAL SECURITY.

(a) REVIEW.—The Director shall review the procurement management practices of Defense and Civilian agencies to determine whether the provisions of section 15.101–2 of the Federal Acquisition Regulation have created any national security risk.

(b) REPORT.—Not later than 180 days after the enactment of this Act, the Director shall submit a report on the results of the review under subsection (a) to—

(1) the Committee on Oversight and Government Reform of the House of Representatives; and

(2) the Committee on Homeland Security and Governmental Affairs of the Senate.

(c) DEFINITIONS.—In this section:

(1) DEFENSE AND CIVILIAN AGENCY.—The term ''Defense and Civilian agency'' has the meaning given the term ''agency'' in section 133 of title 41, United States Code.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kentucky (Mr. COMER) and the gentleman from Virginia (Mr. CONNOLLY) each will control 20 minutes.

The Chair recognizes the gentleman from Kentucky.

GENERAL LEAVE

Mr. COMER. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kentucky?

There was no objection.

Mr. COMER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, the lowest price technically acceptable, LPTA, is a source selection method outlined in the Federal Acquisition Regulation.

This process uses price as a determining factor for a contract rather than other technical or operational factors.

Following legislative work done by the House Oversight Committee during the 115th Congress, constraints were placed on agency use of the LPTA in the fiscal year 2019 National Defense Authorization Act.

These constraints recognize that the LPTA criteria are not always appropriate for agencies seeking complex or technically innovative services.

For instance, this can result in agencies sacrificing long-term value for short-term savings. We also do not want the LPTA to be used in a manner that jeopardizes national security.

This bill requires the Director of the Office of Management and Budget to evaluate this source selection process to determine whether agencies are