still worried about their R&D, can have access to the same kinds of protections.

This bill allows that kind of collaboration to take place, working through the clearinghouse in the Department of Homeland Security. That is why I think it is so important that we take this step forward. I urge all Members to join me in supporting this bill.

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

Mr. MCCAUL. Mr. Speaker, I rise today in support of H.R. 2952, the Critical Infrastructure Research and Development Advancement Act of 2013, sponsored by Chairman Meehan.

This legislation is vital in our nation's efforts to protect our critical infrastructure from attacks. The Department of Homeland Security has identified 16 sectors of the U.S. economy so vital, that disruption or destruction would result in catastrophic life-threatening or life-altering challenges. The CIRDA Act will assist the Department by encouraging the development and procurement of new technologies aimed at infrastructure protection.

I thank Chairman MEEHAN for his efforts in crafting thoughtful legislation that will enhance DHS' research and development tools, streamline its public-private coordination efforts, while ensuring that technological and product solutions are shared between the Department and its private sector partners.

This bill is a bipartisan effort that was passed out of both subcommittee and full committee by voice vote, and I thank the subcommittee Chairman and Ranking Member for their work.

I urge support for H.R. 2952.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise in strong support of H.R. 2952, the ''Critical Infrastructure Research and Development Advancement Act.''

H.R. 2952 requires the Department to have a well-developed Research and Development strategy to work in targeted ways to advance cybersecurity, particularly within the critical infrastructure sector.

Keeping pace with cybercriminals, hackers, and others who seek to exploit vulnerabilities in critical IT networks is a major challenge for the Federal government and its partners in the private sector.

Americans take for granted that when they flip a switch, their lights will come on, when they pick up a phone, there will be a ringtone and when they pick up their Smartphone, they will have a signal.

The reliability and functioning of these systems is dependent on computer systems, often Internet-based systems.

Recently, we have seen the damage that can be done when systems are breached. The database breach at Target, a major retailer, involved 70 million stolen records, which affected over a hundred million people.

The true cost of these kinds of breaches is almost unknowable because of the complexity of the crimes, and the sometimes-untraceable use of the stolen information.

What we do know is that hackers are breaching the networks of large corporate companies, gaining access to proprietary industry information, as well as consumer data.

The Department of Homeland Security is the lead Federal agency responsible for researching and developing more advanced and effective cybersecurity technologies to defend Americans from such attacks.

The legislation before us today creates a technology clearinghouse to help promote partnerships with laboratories and universities throughout the Nation for research on how to enhance not only the cyber but the physical of critical infrastructure.

I am pleased that it directs DHS to seek out new ways to better collaboration with its Centers of Excellence on this research.

I am confident that the teams at Jackson State University and Tougaloo College in Mississippi, which are part of the Centers of Excellence network, can make valuable contributions to this effort.

On a bipartisan basis, this Committee has developed a record for championing homeland security research and development while, at the same time, demanding accountability of DHS to ensure solid decision-making drives the expenditure of limited R&D dollars.

I urge my fellow colleagues to support H.R. 2952, the ''Critical Infrastructure Research and Development Advancement Act of 2013''.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 2952, a bill that will create a research and development strategy for critical infrastructure security technologies to protect critical American infrastructure from physical and cyber-attacks.

As a senior member of the Homeland Security Committee, I believe that the technology and protection of our critical infrastructure falls short in addressing the cyber-attacks we face on a daily basis.

We are in dire need of new security technologies to keep pace with rapidly evolving threats and the rapid advancement of the infrastructure itself.

This bill requires the Homeland Security Department to facilitate the development of a research and development (R&D) strategy for critical infrastructure security technologies.

The measure requires the Homeland Security Department, within 180 days of enactment and every two years thereafter, to submit to Congress a strategic plan for research and development efforts addressing the protection of critical infrastructure.

The plan must identify critical infrastructure security risks and any associated security technology gaps

The department also must submit a report to Congress, within 180 days of enactment and every two years thereafter, on departmental use of public-private consortiums to develop technology to protect such infrastructure.

The Congressional Budget Office (CBO) estimates that the bill would cost less than $500,000 annually in 2014 and 2015, assuming the availability of appropriated funds.

The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local or tribal governments.

Mr. Speaker, the cost of this bill is a small price to pay for the increased security and safety it will provide once it has been successfully implemented.

In closing, I would like to state that I have always advocated for strengthening our Department of Homeland Security and giving the department the proper tools to protect our country.

It is important that we continue to help support the agencies that protect us.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Pennsylvania (Mr. MEEHAN) that the House suspend the rules and pass the bill, H.R. 2952, 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.

□ 1730

HOMELAND SECURITY CYBERSECURITY BOOTS-ON-THE-GROUND ACT

Mr. MEEHAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3107) to require the Secretary of Homeland Security to establish cybersecurity occupation classifications, assess the cybersecurity workforce, develop a strategy to address identified gaps in the cybersecurity workforce, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3107

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

SECTION 1. HOMELAND SECURITY CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

''SEC. 226. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

''(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Boots-on-the-Ground Act'.

''(b) CYBERSECURITY OCCUPATION CATEGORIES.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

''(2) APPLICABILITY.—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

''(c) CYBERSECURITY WORKFORCE ASSESSMENT.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

''(2) CONTENTS.—The assessment required under paragraph (1) shall, at a minimum, include the following:

''(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

''(B) Information on which cybersecurity positions are—

''(i) performed by—

''(I) permanent full time departmental employees, together with demographic information about such employees' race, ethnicity, gender, disability status, and veterans status;

''(II) individuals employed by independent contractors; and

''(III) individuals employed by other Federal agencies, including the National Security Agency; and

''(ii) vacant.

''(C) The number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions across the Department over a three year period, and information on what challenges, if any, were encountered with respect to the implementation of such authority.

''(D) Information on vacancies within the Department's cybersecurity supervisory workforce, from first line supervisory positions through senior departmental cybersecurity positions.

''(E) Information on the percentage of individuals within each cybersecurity occupation category who received essential training to perform their jobs, and in cases in which such training is not received, information on what challenges, if any, were encountered with respect to the provision of such training.

''(F) Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department in a manner that allows for tracking of overall recruiting and identifying areas for better coordination and leveraging of resources within the Department.

''(d) WORKFORCE STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department.

''(2) CONTENTS.—The comprehensive workforce strategy developed under paragraph (1) shall include—

''(A) a multiphased recruitment plan, including relating to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

''(B) a 5-year implementation plan;

''(C) a 10-year projection of the Department's cybersecurity workforce needs; and

''(D) obstacles impeding the hiring and development of a cybersecurity workforce at the Department.

''(e) INFORMATION SECURITY TRAINING.—Not later than 270 days after the date of the enactment of this section, the Secretary shall establish and maintain a process to verify on an ongoing basis that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate with assigned responsibilities. The Secretary shall maintain documentation to ensure that training provided to an individual under this subsection meets or exceeds requirements for such individual's job function.

''(f) UPDATES.—The Secretary shall submit to the appropriate congressional committees annual updates regarding the cybersecurity workforce assessment required under subsection (c), information on the progress of carrying out the comprehensive workforce strategy developed under subsection (d), and information on the status of the implementation of the information security training required under subsection (e).

''(g) GAO STUDY.—The Secretary shall provide the Comptroller General of the United States with information on the cybersecurity workforce assessment required under subsection (c) and progress on carrying out the comprehensive workforce strategy developed under subsection (d). The Comptroller General shall submit to the Secretary and the appropriate congressional committees a study on such assessment and strategy.

''(h) CYBERSECURITY FELLOWSHIP PROGRAM.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 225 the following new item:

''Sec. 226. Cybersecurity occupation categories, workforce assessment, and strategy.''.

SEC. 2. PERSONNEL AUTHORITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 1 of this Act, is further amended by adding at the end the following new section:

''SEC. 227. PERSONNEL AUTHORITIES.

''(a) IN GENERAL.—

''(1) PERSONNEL AUTHORITIES.—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title 10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a written explanation of such determination. Such authority shall be exercised—

''(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

''(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

''(2) CIVIL SERVICE PROTECTIONS.—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).

''(3) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a plan for the use of the authorities provided under this subsection.

''(b) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

''(c) DEFINITION OF QUALIFIED EMPLOYEE.—In this section, the term 'qualified employee' means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastructure information systems, or networks of either of such systems.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 226 (as added by section 1 of this Act) the following new item:

''Sec. 227. Personnel authorities.''.

SEC. 3. CLARIFICATION REGARDING AUTHORIZATION OF APPROPRIATIONS.

No additional amounts are authorized to be appropriated by reason of this Act or the amendments made by this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Pennsylvania (Mr. MEEHAN) and the gentlewoman from New York (Ms. CLARKE) each will control 20 minutes.

The Chair recognizes the gentleman from Pennsylvania.

GENERAL LEAVE

Mr. MEEHAN. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include any extraneous material on the bill under consideration.

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

There was no objection.

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

I rise today in support of H.R. 3107, which is the Homeland Security Cybersecurity Boots-on-the-Ground Act, and it is sponsored by the ranking member of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, Ms. YVETTE CLARKE of New York. This critical piece of legislation is necessary to ensure that the Department of Homeland Security can address gaps in the Department's cybersecurity workforce.

I am proud to cosponsor this legislation, as it will direct the Department to assess its cyber workforce, create occupational classifications, and develop a cybersecurity workforce strategy.

Throughout the past year, our subcommittee has worked in a bipartisan fashion to identify the cyber threat to our Nation's critical infrastructure, as well as to assess the Department's ability to prevent major cyber attacks. Through our oversight capacity, we have identified areas where Congress can act to neutralize this evolving threat. I am particularly proud of the work we did to tweak this legislation and to incorporate it into the larger committee cyber bill.

I believe that today's markup will go a long way in supporting this mission, and I urge support for this crucial piece of legislation.

Mr. Speaker, I reserve the balance of my time.

Ms. CLARKE of New York. Mr. Speaker, I yield myself such time as I may consume.

I rise in strong support of H.R. 3107, the Homeland Security Cybersecurity

Boots-on-the-Ground Act. This is a bill I introduced to address fundamental challenges in the cyber workforce at the Department of Homeland Security. It has gained bipartisan support, as acknowledged by the gentleman from Pennsylvania (Mr. MEEHAN), our chairman.

Since the attacks of September 11, the urgent need to fill critical national security positions at times has led to actions that may have inadvertently heightened our vulnerability and fostered an over-reliance on private contractors. From a recruitment and retention standpoint, it is critical that the Department of Homeland Security clearly identifies job classifications for the cyber positions it seeks to fill. That was one of the major conclusions of the Cyber Skills Task Force that the Homeland Security Advisory Committee assembled at the request of then-DHS Secretary Janet Napolitano in 2012.

I introduced the Homeland Security Cybersecurity Boots-on-the-Ground Act to implement a number of the task force's key recommendations.

First, the bill directs DHS to develop and issue comprehensive occupation classifications for persons performing activities in furtherance of the Department's cybersecurity missions.

Secondly, the bill requires the Secretary to assess the readiness and capacity of the Department to meet its cybersecurity mission. As part of the assessment, the Department has to identify where positions are located, whether these positions are vacant, and whether they are held by full-time employees or contractors.

Thirdly, the bill requires the Secretary to develop a comprehensive workforce strategy. This strategy will be implemented to enhance the readiness, capacity, training, recruitment, and retention of the Department's cybersecurity workforce.

Finally, the bill requires the Secretary to establish and maintain a process to verify that individuals employed by private contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training.

H.R. 3107 takes a holistic approach to the challenge of recruiting, training, and retraining the cybersecurity workforce that DHS needs.

I thank Ranking Member MEEHAN for all of his support and for all of the work that we have done together in a bipartisan way to bring this legislation to the floor, as well as the suite of cybersecurity legislation that we brought forth to the floor today.

I want to also thank the staff of both the committee and my office for the work and the diligence that they have put into bringing forth what I call real 21st century legislation. It is very important legislation. And our very way of life depends on its success.

Since 2008, the Department of Homeland Security has been the lead Federal civilian agency for cybersecurity. It has been responsible for working with Federal agencies to secure their IT networks, and the private sector, particularly critical infrastructure owners and operators, to raise the level of cyber hygiene and address threats in a timely manner.

My legislation will help ensure that DHS has the workforce it needs to execute these critical responsibilities. For that reason, I urge all of my colleagues to support H.R. 3107.

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

Mr. MEEHAN. Mr. Speaker, I am very grateful for the gentlewoman's presentation of this issue, and I yield myself such time as I may consume.

I just want to conclude my remarks on this bill by pointing to the preparation that went into this bill. I would also recognize the importance of not just this issue and the challenges that we face with the complexity of this issue but to recognize that in order for the Department to fulfill its mission, they have to have the kind of workforce that is capable of doing it. And in areas like this, that requires a skilled workforce and, some would say, a uniquely skilled workforce.

I think the gentlewoman's wisdom in recognizing that once you develop that skilled workforce, when 90 percent of the assets are out in the private sector, it does not take too long before that private sector comes knocking on the door and starts to say, we want your people out here. And so wisely, the gentlewoman has pointed to allowing us to have a plan in place that looks at the three Rs: readiness, recruitment, and retention. And that is the essence of what we want to try to do with this very, very important legislation. We want to give some flexibility and control to the Department to not only train and make sure we have got the best next generation of those who will commit themselves to our Nation by service through the Department and protecting our homeland but, once they have developed those skills, that we are able, as much as possible, to retain them within here by virtue of allowing them the capacity and flexibility to do the work that they do best. There will still be plenty of opportunity to find bright people in the private sector as well. But we have got to make sure the mission of homeland security is not affected.

For those reasons, I urge all Members to join me in supporting this bill, and I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise today to express my support for H.R. 3107, the "Homeland Security Cybersecurity Boots-on-the-Ground Act".

I would like to commend Subcommittee Ranking Member CLARKE for her commitment to addressing a critical issue for the Department of Homeland Security—how to recruit and retain a robust cybersecurity workforce.

There is an urgent need for greater protection of our cyber infrastructure, with the rate and intensity of system breaches at an all-time high and the mounting source of cyber threats.

The Department of Homeland Security is the lead Federal agency for protecting the government's Internet platform ".gov" and for partnering with the private sector on cybersecurity.

Attracting the best and brightest in the cybersecurity field has been a chronic challenge for the Department. In an effort to come up with some effective strategies to overcome that challenge, in July 2012, then-Secretary Janet Napolitano directed the Homeland Security Advisory Committee to assemble a "Task Force on CyberSkills".

The Task Force issued a series of recommendations that included the adoption of a list of mission-critical cybersecurity tasks and a model for assessing the competency and progress of the existing and future DHS mission-critical cybersecurity workforce.

H.R. 3107 adopts many of the Task Force's key recommendations.

For instance, in order to recruit the Department with the cyber workforce it needs, H.R. 3107 requires DHS to have comprehensive occupation classifications to categorize what types of work will be done in each position.

Today, DHS does not utilize a uniform classification system and, as a result, positions get posted that offer little clarity on what knowledge, skills, and experience is sought.

Sophisticated cyber mission-critical skills are not a dime-a-dozen, and Federal agencies have to compete among themselves, and especially private sector employers for talent.

This bill seeks to ensure that DHS has an effective approach to attracting, hiring, and retaining a mission-critical cybersecurity workforce.

I urge my colleagues to support this bipartisan legislation.

Mr. MCCAUL. Mr. Speaker, I rise today in support of H.R. 3107, the Homeland Security Cybersecurity Boots-on-the-Ground Act, sponsored by Ranking Member CLARKE.

H.R. 3107 includes important provisions to bolster the cybersecurity workforce at the Department of Homeland Security. Across our nation, businesses, colleges and universities are transforming their organizations to include strong and robust cybersecurity practices. It is essential that DHS is hiring the best and the brightest that this emerging field has to offer. The Department's efforts to protect the homeland from an attack depend on it.

The legislation offered by Ms. CLARKE was introduced and passed out of the committee with bipartisan support and we were pleased to have worked with her to adjust the language to mirror the workforce provisions in the full committee's cyber bill. It will require the Department to take inventory of its cyber workforce, including those of other Federal agencies. Subsequently, the Secretary will be required to present to Congress a workforce strategy, focused on how to attract and maintain top cybersecurity experts.

These new provisions will help ensure the Department has a coherent plan to address their need to hire cyber professionals and fill those much needed positions.

I would like to thank Ranking Member CLARKE for all of her work on this important subject, I urge support for the bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Pennsylvania (Mr. MEEHAN) that the House suspend the rules and pass the bill, H.R. 3107, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. MEEHAN. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this question will be postponed.

The point of no quorum is considered withdrawn.

SUNSCREEN INNOVATION ACT

Mr. WHITFIELD. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4250) to amend the Federal Food, Drug, and Cosmetic Act to provide an alternative process for review of safety and effectiveness of nonprescription sunscreen active ingredients and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4250

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 ''Sunscreen Innovation Act''.

SEC. 2. REGULATION OF NONPRESCRIPTION SUNSCREEN ACTIVE INGREDIENTS.

Chapter V of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351 et seq.) is amended by adding at the end the following:

''Subchapter I—Nonprescription Sunscreen Active Ingredients

''SEC. 586. DEFINITIONS.

''In this subchapter:

''(1) The term 'Advisory Committee' means the Nonprescription Drug Advisory Committee or any successor to such Committee.

''(2) The terms 'generally recognized as safe and effective' and 'GRASE' mean generally recognized, among experts qualified by scientific training and experience to evaluate the safety and effectiveness of drugs, as safe and effective for use under the conditions prescribed, recommended, or suggested in the product's labeling, as described in section 201(p).

''(3) The term 'GRASE determination' means, with respect to a nonprescription sunscreen active ingredient or a combination of nonprescription sunscreen active ingredients, a determination of whether such ingredients or combination of ingredients is generally recognized as safe and effective and not misbranded for use under the conditions prescribed, recommended, or suggested in the product's labeling, as described in section 201(p).

''(4) The term 'nonprescription' means not subject to section 503(b)(1).

''(5) The term 'pending request' means each request submitted to the Secretary—

''(A) for consideration for inclusion in the over-the-counter drug monograph system;

''(B) that was deemed eligible for such review by publication of a notice of eligibility in the Federal Register prior to the date of enactment of the Sunscreen Innovation Act; and

''(C) for which safety and effectiveness data has been submitted to the Secretary prior to such date of enactment.

''(6) The term 'sponsor' means the person submitting the request under section 586A(a), including a time and extent application under section 586B, or the person that submitted the pending request.

''(7) The term 'sunscreen active ingredient' means an active ingredient that is intended for application to the skin of humans for purposes of absorbing, reflecting, or scattering radiation.

''(8) The term 'sunscreen' means a product containing one or more sunscreen active ingredients.

''SEC. 586A. GENERAL PROVISIONS.

''(a) REQUESTS.—Any person may submit a request to the Secretary for a determination of whether a nonprescription sunscreen active ingredient or a combination of nonprescription sunscreen active ingredients, for use under specified conditions, to be prescribed, recommended, or suggested in the labeling thereof (including dosage form, dosage strength, and route of administration) is generally recognized as safe and effective and not misbranded.

''(b) RULES OF CONSTRUCTION.—

''(1) CURRENTLY MARKETED SUNSCREENS.—Nothing in this subchapter shall be construed to affect the marketing of sunscreens that are lawfully marketed in the United States on or before the date of enactment of this subchapter.

''(2) ENSURING SAFETY AND EFFECTIVENESS.—Nothing in this subchapter shall be construed to alter the Secretary's authority to prohibit the marketing of a sunscreen that is not safe and effective or to impose restrictions on the marketing of a sunscreen to ensure safety and effectiveness.

''(3) OTHER PRODUCTS.—Nothing in this subchapter shall be construed to affect the Secretary's regulation of products other than sunscreens.

''(c) SUNSET.—This subchapter shall cease to be effective at the end of the 5-year period beginning on the date of enactment of this subchapter.

''SEC. 586B. ELIGIBILITY DETERMINATION.

''(a) IN GENERAL.—Upon receipt of a request under section 586A(a), not later than 60 days after the date of receipt of such request, the Secretary shall—

''(1) determine whether the request is eligible for further review under sections 586C and 586D, as described in subsection (b);

''(2) notify the sponsor of the Secretary's determination; and

''(3) make such determination publicly available in accordance with subsection (c).

''(b) CRITERIA FOR ELIGIBILITY.—

''(1) IN GENERAL.—To be eligible for review under sections 586C and 586D, a request shall be for a nonprescription sunscreen active ingredient or combination of nonprescription sunscreen active ingredients, for use under specified conditions, to be prescribed, recommended, or suggested in the labeling thereof, that—

''(A) is not included in the stayed sunscreen monograph in part 352 of title 21, Code of Federal Regulations; and

''(B) has been used to a material extent and for a material time, as described in section 201(p)(2).

''(2) TIME AND EXTENT APPLICATION.—A sponsor shall include in a request under section 586A(a) a time and extent application including all the information required to meet the standard described in paragraph (1)(B).

''(c) PUBLIC AVAILABILITY.—

''(1) REDACTIONS FOR CONFIDENTIAL INFORMATION.—If a nonprescription sunscreen active ingredient or combination of nonprescription sunscreen active ingredients is determined to be eligible for further review under subsection (a)(1), the Secretary shall make the request publicly available, with redactions for information that is treated as confidential under section 552(b) of title 5, United States Code, section 1905 of title 18, United States Code, or section 301(j) of this Act.

''(2) IDENTIFICATION OF CONFIDENTIAL INFORMATION BY SPONSOR.—Sponsors shall identify any information which the sponsor considers to be confidential information described in paragraph (1).

''(3) CONFIDENTIALITY DURING ELIGIBILITY REVIEW.—The information contained in a request under section 586A(a) shall remain confidential during the Secretary's consideration under this section of whether the request is eligible for further review.

''SEC. 586C. DATA SUBMISSION; FILING DETERMINATION.

''(a) IN GENERAL.—In the case of a request under section 586A(a) that is determined to be eligible under section 586B for further review under this section and section 586D—

''(1) the Secretary shall, in notifying the public under section 586B(a)(3) of such eligibility determination, invite the sponsor of the request and any other interested party to submit, in support of or otherwise relating to a GRASE determination—

''(A) published and unpublished data and other information related to the safety and effectiveness of the nonprescription sunscreen active ingredient or combination of nonprescription sunscreen active ingredients for its intended nonprescription uses; or

''(B) any other comments; and

''(2) not later than 60 days after the submission of such data and other information by the sponsor, including any revised submission of such data and other information following a refusal to file under subparagraph (B), the Secretary shall—

''(A)(i) issue a written notification to the sponsor determining that the request under section 586A(a), together with such data and other information, is sufficiently complete to conduct a substantive review and make such notification publicly available; and

''(ii) file such request; or

''(B) issue a written notification to the sponsor refusing to file the request and stating the reasons for the refusal and why the data and other information submitted is not sufficiently complete to conduct a substantive review and make such notification publicly available;

''(3) the Secretary shall, in filing a request under paragraph (2)—

''(A) invite the public to submit further comments with respect to such filing; and

''(B) limit such public comment, and the comment period under paragraph (1), to the period ending on the date that is 60 days after such filing;

''(4) if the Secretary refuses to file the request—

''(A) the sponsor may, within 30 days of receipt of written notification of such refusal, seek a meeting with the Secretary regarding whether the Secretary should file the request; and

''(B) the Secretary shall convene the meeting; and

''(5) following any such meeting—

''(A) if the sponsor asks that the Secretary file the request (with or without amendments to correct any purported deficiencies to the request) the Secretary shall file the request over protest, issue a written notification of the filing to the sponsor, and make such notification publicly available; and

''(B) if the request is so filed over protest, the Secretary shall not require the sponsor to resubmit a copy of the request for purposes of such filing.

''(b) REASONS FOR REFUSAL TO FILE REQUEST.—The Secretary may refuse to file a request submitted under section 586A(a) if the Secretary determines the data or other information submitted by the sponsor under this section are not sufficiently complete to conduct a substantive review with respect to such request.

''(c) PUBLIC AVAILABILITY.—

''(1) REDACTIONS FOR CONFIDENTIAL INFORMATION.—The Secretary shall make data and other information submitted in connection with a request under section 586A(a) publicly available, with redactions for information that is treated as confidential under section 552(b) of title 5,