And the increasingly acid ocean waters can actually eat away the carbon shells of corals and a myriad of other sea life.

The people I represent live on islands surrounded by coral reefs.

Coral reefs protect us from storms and provide habitat for fish and shelled animals that are a traditional source of food.

The existence of coral reefs attract hundreds of thousands of tourists to the Northern Mariana Islands each year.

Economists have valued our coral reefs at up to $70 million annually. Yet each year the oceans grow more acidic that economic value is being eroded.

I thank Mr. INSLEE for focusing on this issue.

I urge my colleagues to support House Resolution 989 and national and international policies to prevent ocean acidification.

Mr. FALEOMAVAEGA. Mr. Speaker, I rise in strong support of H. Res. 989, expressing the sense of the House of Representatives that the United States should adopt national policies and pursue international agreements to prevent ocean acidification, to study the impacts of ocean acidification, and to address the effects of ocean acidification on marine ecosystems and coastal economies.

We know ocean acidification occurs as a consequence of high levels of man-made carbon dioxide emissions. But we do not know the full ramifications of ocean acidification. As H. Res. 989 suggests, the United States should pursue national and international activities and agreements to develop a full body of scientific research in addition to the work that will be done by the National Oceanic and Atmospheric Administration as part of the Federal Ocean Acidification Research and Monitoring Act of 2009.

H. Res. 989 emphasizes that we must do more monitoring and research on ocean acidification in order to protect and preserve the ocean, which serves as a source of food, income and cultural identity for hundreds of millions people living in the United States and around the world.

As Chairman of the Foreign Affairs Subcommittee for Asia, the Pacific and the Global Environment, I know firsthand how important it is for the U.S. Congress to act as a primary supporter of efforts aimed at curbing climate change and its consequences, including ocean acidification. And in representing a district whose livelihood and heritage were shaped by the South Pacific, preserving the ocean environment will always be one of my paramount concerns. I urge my colleagues to join with the 53 Members who have already cosponsored H. Res. 989 and support its passage.

Mr. INSLEE. 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 Washington (Mr. INSLEE) that the House suspend the rules and agree to the resolution, H. Res. 989.

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. CHAFFETZ. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT

Mr. MARKEY of Massachusetts. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5026) to amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States from cybersecurity and other threats and vulnerabilities, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5026

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 ''Grid Reliability and Infrastructure Defense Act'' or the ''GRID Act''.

SEC. 2. AMENDMENT TO THE FEDERAL POWER ACT.

(a) CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.—Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding after section 215 the following new section:

''SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

''(a) DEFINITIONS.—For purposes of this section:

''(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms 'bulk-power system', 'Electric Reliability Organization', and 'regional entity' have the meanings given such terms in paragraphs (1), (2), and (7) of section 215(a), respectively.

''(2) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'defense critical electric infrastructure' means any infrastructure located in the United States (including the territories) used for the generation, transmission, or distribution of electric energy that—

''(A) is not part of the bulk-power system; and

''(B) serves a facility designated by the President pursuant to subsection (d)(1), but is not owned or operated by the owner or operator of such facility.

''(3) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITY.—The term 'defense critical electric infrastructure vulnerability' means a weakness in defense critical electric infrastructure that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of defense critical electric infrastructure.

''(4) ELECTROMAGNETIC PULSE.—The term 'electromagnetic pulse' means 1 or more pulses of electromagnetic energy emitted by a device capable of disabling, disrupting, or destroying electronic equipment by means of such a pulse.

''(5) GEOMAGNETIC STORM.—The term 'geomagnetic storm' means a temporary disturbance of the Earth's magnetic field resulting from solar activity.

''(6) GRID SECURITY THREAT.—The term 'grid security threat' means a substantial likelihood of—

''(A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system or of defense critical electric infrastructure; and

''(ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure, as a result of such act or event; or

''(B)(i) a direct physical attack on the bulk-power system or on defense critical electric infrastructure; and

''(ii) significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure as a result of such physical attack.

''(7) GRID SECURITY VULNERABILITY.—The term 'grid security vulnerability' means a weakness that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system.

''(8) LARGE TRANSFORMER.—The term 'large transformer' means an electric transformer that is part of the bulk-power system.

''(9) PROTECTED INFORMATION.—The term 'protected information' means information, other than classified national security information, designated as protected information by the Commission under subsection (e)(2)—

''(A) that was developed or submitted in connection with the implementation of this section;

''(B) that specifically discusses grid security threats, grid security vulnerabilities, defense critical electric infrastructure vulnerabilities, or plans, procedures, or measures to address such threats or vulnerabilities; and

''(C) the unauthorized disclosure of which could be used in a malicious manner to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

''(10) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

''(11) SECURITY.—The definition of 'security' in section 3(16) shall not apply to the provisions in this section.

''(b) EMERGENCY RESPONSE MEASURES.—

''(1) AUTHORITY TO ADDRESS GRID SECURITY THREATS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination identifying an imminent grid security threat, the Commission may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in its judgment to protect the reliability of the bulk-power system or of defense critical electric infrastructure against such threat. As soon as practicable but not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment, establish rules of procedure that ensure that such authority can be exercised expeditiously.

''(2) NOTIFICATION OF CONGRESS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination under paragraph (1), the President (or the Secretary, as the case may be) shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, such directive or determination.

''(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Commission shall, to the extent practicable in light of the nature of the grid security threat and the urgency of the need for such emergency measures, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Secretary, and other appropriate Federal agencies regarding implementation of such emergency measures.

''(4) APPLICATION.—An order for emergency measures under this subsection may apply to—

''(A) the Electric Reliability Organization;

''(B) a regional entity; or

''(C) any owner, user, or operator of the bulk-power system or of defense critical electric infrastructure within the United States.

''(5) DISCONTINUANCE.—The Commission shall issue an order discontinuing any emergency measures ordered under this subsection, effective not later than 30 days after the earliest of the following:

''(A) The date upon which the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination that the grid security threat identified under paragraph (1) no longer exists.

''(B) The date upon which the Commission issues a written determination that the emergency measures are no longer needed to address the grid security threat identified under paragraph (1), including by means of Commission approval of a reliability standard under section 215 that the Commission determines adequately addresses such threat.

''(C) The date that is 1 year after the issuance of an order under paragraph (1).

''(6) COST RECOVERY.—If the Commission determines that owners, operators, or users of the bulk-power system or of defense critical electric infrastructure have incurred substantial costs to comply with an order under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission shall, after notice and an opportunity for comment, establish a mechanism that permits such owners, operators, or users to recover such costs.

''(c) MEASURES TO ADDRESS GRID SECURITY VULNERABILITIES.—

''(1) COMMISSION AUTHORITY.—If the Commission, in consultation with appropriate Federal agencies, identifies a grid security vulnerability that the Commission determines has not adequately been addressed through a reliability standard developed and approved under section 215, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring implementation, by any owner, operator, or user of the bulk-power system in the United States, of measures to protect the bulk-power system against such vulnerability. Before promulgating a rule or issuing an order under this paragraph, the Commission shall, to the extent practicable in light of the urgency of the need for action to address the grid security vulnerability, request and consider recommendations from the Electric Reliability Organization regarding such rule or order. The Commission may establish an appropriate deadline for the submission of such recommendations.

''(2) CERTAIN EXISTING CYBERSECURITY VULNERABILITIES.—Not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring the implementation, by any owner, user, or operator of the bulk-power system in the United States, of such measures as are necessary to protect the bulk-power system against the vulnerabilities identified in the June 21, 2007, communication to certain 'Electricity Sector Owners and Operators' from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information and Analysis Center.

''(3) RESCISSION.—The Commission shall approve a reliability standard developed under section 215 that addresses a grid security vulnerability that is the subject of a rule or order under paragraph (1) or (2), unless the Commission determines that such reliability standard does not adequately protect against such vulnerability or otherwise does not satisfy the requirements of section 215. Upon such approval, the Commission shall rescind the rule promulgated or order issued under paragraph (1) or (2) addressing such vulnerability, effective upon the effective date of the newly approved reliability standard.

''(4) GEOMAGNETIC STORMS.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards adequate to protect the bulk-power system from any reasonably foreseeable geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable events against which such standards must protect. Such standards shall appropriately balance the risks to the bulk-power system associated with such events, including any regional variation in such risks, and the costs of mitigating such risks.

''(5) LARGE TRANSFORMER AVAILABILITY.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards addressing availability of large transformers. Such standards shall require entities that own or operate large transformers to ensure, individually or jointly, adequate availability of large transformers to promptly restore the reliable operation of the bulk-power system in the event that any such transformer is destroyed or disabled as a result of a reasonably foreseeable physical or other attack or geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable attacks or events that shall provide the basis for such standards. Such standards shall—

''(A) provide entities subject to the standards with the option of meeting such standards individually or jointly; and

''(B) appropriately balance the risks associated with a reasonably foreseeable attack or event, including any regional variation in such risks, and the costs of ensuring adequate availability of spare transformers.

''(d) CRITICAL DEFENSE FACILITIES.—

''(1) DESIGNATION.—Not later than 180 days after the date of enactment of this section, the President shall designate, in a written directive or determination provided to the Commission, facilities located in the United States (including the territories) that are—

''(A) critical to the defense of the United States; and

''(B) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider.

The number of facilities designated by such directive or determination shall not exceed 100. The President may periodically revise the list of designated facilities through a subsequent written directive or determination provided to the Commission, provided that the total number of designated facilities at any time shall not exceed 100.

''(2) COMMISSION AUTHORITY.—If the Commission identifies a defense critical electric infrastructure vulnerability that the Commission, in consultation with owners and operators of any facility or facilities designated by the President pursuant to paragraph (1), determines has not adequately been addressed through measures undertaken by owners or operators of defense critical electric infrastructure, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, promulgate a rule or issue an order requiring implementation, by any owner or operator of defense critical electric infrastructure, of measures to protect the defense critical electric infrastructure against such vulnerability. The Commission shall exempt from any such rule or order any specific defense critical electric infrastructure that the Commission determines already has been adequately protected against the identified vulnerability. The Commission shall make any such determination in consultation with the owner or operator of the facility designated by the President pursuant to paragraph (1) that relies upon such defense critical electric infrastructure.

''(3) COST RECOVERY.—An owner or operator of defense critical electric infrastructure shall be required to take measures under paragraph (2) only to the extent that the owners or operators of a facility or facilities designated by the President pursuant to paragraph (1) that rely upon such infrastructure agree to bear the full incremental costs of compliance with a rule promulgated or order issued under paragraph (2).

''(e) PROTECTION OF INFORMATION.—

''(1) PROHIBITION OF PUBLIC DISCLOSURE OF PROTECTED INFORMATION.—Protected information—

''(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

''(B) shall not be made available pursuant to any State, local, or tribal law requiring disclosure of information or records.

''(2) INFORMATION SHARING.—

''(A) IN GENERAL.—Consistent with the Controlled Unclassified Information framework established by the President, the Commission shall promulgate such regulations and issue such orders as necessary to designate protected information and to prohibit the unauthorized disclosure of such protected information.

''(B) SHARING OF PROTECTED INFORMATION.—The regulations promulgated and orders issued pursuant to subparagraph (A) shall provide standards for and facilitate the appropriate sharing of protected information with, between, and by Federal, State, local, and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators, and users of the bulk-

power system in the United States and of defense critical electric infrastructure. In promulgating such regulations and issuing such orders, the Commission shall take account of the role of State commissions in reviewing the prudence and cost of investments within their respective jurisdictions. The Commission shall consult with appropriate Canadian and Mexican authorities to develop protocols for the sharing of protected information with, between, and by appropriate Canadian and Mexican authorities and owners, operators, and users of the bulk-power system outside the United States.

''(3) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall permit or authorize the withholding of information from Congress, any committee or subcommittee thereof, or the Comptroller General.

''(4) DISCLOSURE OF NON-PROTECTED INFORMATION.—In implementing this section, the Commission shall protect from disclosure only the minimum amount of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure. The Commission shall segregate protected information within documents and electronic communications, wherever feasible, to facilitate disclosure of information that is not designated as protected information.

''(5) DURATION OF DESIGNATION.—Information may not be designated as protected information for longer than 5 years, unless specifically redesignated by the Commission.

''(6) REMOVAL OF DESIGNATION.—The Commission may remove the designation of protected information, in whole or in part, from a document or electronic communication if the unauthorized disclosure of such information could no longer be used to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

''(7) JUDICIAL REVIEW OF DESIGNATIONS.—Notwithstanding subsection (f) of this section or section 313, a person or entity may seek judicial review of a determination by the Commission concerning the designation of protected information under this subsection exclusively in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in the District of Columbia. In such a case the court shall determine the matter de novo, and may examine the contents of documents or electronic communications designated as protected information in camera to determine whether such documents or any part thereof were improperly designated as protected information. The burden is on the Commission to sustain its designation.

''(f) JUDICIAL REVIEW.—The Commission shall act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section that are filed under section 313(a). Any party seeking judicial review pursuant to section 313 of an order issued under this section may obtain such review only in the United States Court of Appeals for the District of Columbia Circuit.

''(g) PROVISION OF ASSISTANCE TO INDUSTRY IN MEETING GRID SECURITY PROTECTION NEEDS.—

''(1) EXPERTISE AND RESOURCES.—The Secretary shall establish a program, in consultation with other appropriate Federal agencies, to develop technical expertise in the protection of systems for the generation, transmission, and distribution of electric energy against geomagnetic storms or malicious acts using electronic communications or electromagnetic pulse that would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of such systems. Such program shall include the identification and development of appropriate technical and electronic resources, including hardware, software, and system equipment.

''(2) SHARING EXPERTISE.—As appropriate, the Secretary shall offer to share technical expertise developed under the program under paragraph (1), through consultation and assistance, with owners, operators, or users of systems for the generation, transmission, or distribution of electric energy located in the United States and with State commissions. In offering such support, the Secretary shall assign higher priority to systems serving facilities designated by the President pursuant to subsection (d)(1) and other critical-infrastructure facilities, which the Secretary shall identify in consultation with the Commission and other appropriate Federal agencies.

''(3) SECURITY CLEARANCES AND COMMUNICATION.—The Secretary shall facilitate and, to the extent practicable, expedite the acquisition of adequate security clearances by key personnel of any entity subject to the requirements of this section to enable optimum communication with Federal agencies regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities. The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with their obligations to protect classified and protected information, share timely actionable information regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities with appropriate key personnel of owners, operators, and users of the bulk-power system and of defense critical electric infrastructure.

''(h) CERTAIN FEDERAL ENTITIES.—For the 11-year period commencing on the date of enactment of this section, the Tennessee Valley Authority and the Bonneville Power Administration shall be exempt from any requirement under subsection (b) or (c) (except for any requirement addressing a malicious act using electronic communication).''.

(b) CONFORMING AMENDMENTS.—

(1) JURISDICTION.—Section 201(b)(2) of the Federal Power Act (16 U.S.C. 824(b)(2)) is amended by inserting ''215A,'' after ''215,'' each place it appears.

(2) PUBLIC UTILITY.—Section 201(e) of the Federal Power Act (16 U.S.C. 824(e)) is amended by inserting ''215A,'' after ''215,''.

SEC. 3. BUDGETARY COMPLIANCE.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the House Budget Committee, provided that such statement has been submitted prior to the vote on passage.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Massachusetts (Mr. MARKEY) and the gentleman from Michigan (Mr. UPTON) each will control 20 minutes.

The Chair recognizes the gentleman from Massachusetts.

GENERAL LEAVE

Mr. MARKEY of Massachusetts. 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 in the RECORD.

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

There was no objection.

Mr. MARKEY of Massachusetts. Mr. Speaker, I yield myself such time as I may consume.

Right now, Mr. Speaker, America's electric grid is vulnerable to cyber or other attacks by terrorists or hostile countries. Our adversaries are actively probing these weaknesses and already have the capacity to exploit them. The consequences of such an attack could be devastating. The commercially operated grid provides 99 percent of the power used by our defense facilities. Every one of our Nation's critical civilian systems—water, communications, health care, transportation, law enforcement, and financial services—depends on that grid. Classified Member briefings have underscored the urgency of this threat.

The GRID Act, which has been produced out of the Energy and Environment Subcommittee of the Energy and Commerce Committee, working with Mr. UPTON, the ranking member of the subcommittee, passed by a unanimous 47–0 vote. It is the product of months of bipartisan work led by Chairman WAXMAN and Ranking Members Barton and Upton. It reflects important work by Mr. BARROW and other members of the Energy and Commerce Committee and by Chairman THOMPSON, Representative CLARKE—Chairwoman Clarke—and others on the Homeland Security Committee. And it shows that when it comes to the nexus between national security and energy, all Americans agree that we must chart a more secure path.

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

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

Mr. Speaker, I, too, want to compliment the members on our committee, both Republican and Democrat, not only in our subcommittee that Mr. MARKEY chairs and I'm the ranking member, but also Chairman WAXMAN and Ranking Member BARTON.

This has been a multiyear effort; it really has. This bill is a product of that work. We've had a number of classified hearings and discussions and briefings over the last couple of years with Members attending for hours at a time. We've had some public hearings as well; and this bill is a product of that, which is exactly why the bill passed out of full committee 47–0 on a roll call vote.

The security of our Nation's energy infrastructure from attack is one of the most important issues that this Congress might address this year, and it's not an issue that we can take lightly. Energy, as we know, electricity literally powers our economy in everything that we do. Even small price spikes and supply disruptions can wreak havoc on our economy for perhaps who knows how long, and it is imperative that the security of our Nation's energy infrastructure gets all of the attention that it deserves. This legislation is a step in the right direction

to protect our critical energy and defense infrastructure.

Let me tell you a couple of things that this bill does. As it relates to cyber- and electromagnetic weapons, it gives FERC the authority to establish standards to protect the bulk power system against vulnerabilities to malicious acts using electronic communications or electromagnetic weapons.

Geomagnetic storms: The bill requires FERC to direct NERC to submit for approval a reliability standard under section 215 to protect the bulk power infrastructure. And for large transformers, the bill requires FERC again to direct NERC to submit for approval a reliability standard under section 215 to require adequate availability of large transformers to ensure the reliability of the bulk power infrastructure in the event of a physical or other attack with a geomagnetic storm.

□ 1100

I would like to cite just a few words in a letter that was signed by some real national security experts—James Woolsey, Stephen Hadley, John Hamre, Rudy de Leon, James Schlesinger, William Perry, and Willy Schneider, Jr. It's an official-use only letter, so I cannot submit this letter for the RECORD or read more than just a few words.

They say together: We strongly endorse the timely passage of this legislation in recognition that the electricity grid is a critical national security asset, the backbone of defense capability in modern civilization and also in recognition that the grid is vulnerable.

The letter goes on: We don't want a vulnerable grid. We, as a society, cannot live with a vulnerable grid. This bill corrects many of the flaws in what could otherwise be standard operating procedure.

Again, I applaud and thank Chairmen WAXMAN and MARKEY, Ranking Member BARTON, and all of the members of our committee who have spent many hours to address this situation with this legislation.

I reserve the balance of my time.

Mr. MARKEY of Massachusetts. Mr. Speaker, I yield such time as he may consume to the chairman of the full Energy and Commerce Committee, the gentleman from the State of California (Mr. WAXMAN).

Mr. WAXMAN. Mr. Speaker, I rise in support of the Grid Reliability and Infrastructure Defense Act.

When it is signed by the President, this will be a bipartisan law, and it will be vital in protecting the Nation's electric grid from cyberattacks, from direct physical attacks, from electromagnetic pulses, and from solar storms.

Beginning in the last Congress, on a bipartisan basis, a group of Members worked on this legislation—ED MARKEY, JOE BARTON, FRED UPTON, and I. JOHN DINGELL and RICK BOUCHER have also played significant roles in developing the proposal. JOHN BARROW had a very important part in this legislation as well. I commend all of them for working together with me in preparing for this legislation that we are presenting to our colleagues today.

The staffs of both the majority and minority had extensive discussions with interested stakeholders and agencies. We worked with many Members to answer their questions, to address their concerns, and to consider their constructive suggestions. Their input has strengthened this bill. It has been a cooperative process that has produced strong bipartisan legislation. In fact, the Energy and Commerce Committee favorably reported the bill by a unanimous vote of 47–0.

Today, our electric grid simply isn't adequately protected from a range of potential threats in an emergency situation. Where the grid faces an imminent threat, the Federal Energy Regulatory Commission currently lacks the authority to require the necessary protective measures. There is also an ever-growing number of grid security vulnerabilities. These are weaknesses in the grid that could be exploited by criminals, by terrorists, or by other countries to damage our electric grid. There are weaknesses that even make the grid vulnerable to naturally occurring geomagnetic storms.

This bipartisan legislation will provide the Federal Energy Regulatory Commission with the authorities it needs to address these threats. It also directs the Commission to look at the long-term threats, not just at the imminent threats, with standards written or approved by the Commission. In addition, the bill includes provisions that focus specifically on the portions of the grid that serve facilities critical to the defense of the United States.

These are important national security and grid reliability issues. We have heard from the Defense Department, from former Defense Secretaries, from national security advisers, and from CIA Directors. They have told us that the changes made by this bill are critical to our national security, and the Congressional Budget Office confirms that the final bill is budget neutral.

Today's legislation is an opportunity for all of us to work together, and I urge my colleagues to seize this opportunity and to support this important bipartisan legislation.

Mr. UPTON. Mr. Speaker, I know that we have one other Member who wishes to speak, but I do not see him on the floor; so I continue to reserve the balance of my time.

Mr. MARKEY of Massachusetts. Mr. Speaker, I yield 2 minutes to the gentleman from Georgia (Mr. BARROW), to whom Chairman WAXMAN has already made reference. Mr. BARROW is probably the longest-standing Member who has been working on this issue.

Mr. BARROW. I thank the gentleman for yielding. I thank him for his work on this important subject.

Mr. Speaker, the grid that generates and distributes electricity across our country is one of the engineering wonders of the world, but it took generations to build, and it grew up in peacetime, safely removed from any threat of physical attack by our enemies, and it was long before the Internet. Today, we use the Internet to run this vast infrastructure, and that leaves us vulnerable to a potentially devastating cyberattack.

The GRID Act takes the first steps toward protecting our electric grid from those who want to do us harm. The necessary costs are modest compared to the cost of doing nothing. We cannot count on our enemies to wait for us. The threat is real, and the solution is in our hands, so I encourage my colleagues to support the bill.

Mr. UPTON. In seeing that the Member is not here, I would ask again for a strong ''yea'' vote, and I would hope that our Senate colleagues are listening so that they will be able to move this legislation as quickly as possible.

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

Mr. MARKEY of Massachusetts. Mr. Speaker, I yield 2 minutes to the gentleman from Rhode Island (Mr. LANGEVIN), who, in the last Congress, was the chair of what is now the Emerging Threats Subcommittee on the Homeland Security Committee. I have worked with him under his leadership on these issues for years.

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

Mr. LANGEVIN. I thank the gentleman for yielding.

Mr. Speaker, I rise today in strong support of H.R. 5026, legislation to protect our national electric grid system. I would particularly like to thank Chairman MARKEY for his outstanding leadership and dedication to this important national security issue. I know he has given great time and effort and thought to this, and I thank him for that.

I would also like to thank Chairman WAXMAN for his attention to this issue.

I would also like to recognize and to thank my good friend Mr. THOMPSON, chairman of the full Homeland Security Committee, for working with me in 2008 to hold hearings and to closely examine what actions our country must absolutely take to prevent attacks on our national security electric grid.

Two years ago, I testified before Chairman MARKEY's subcommittee about the threats to our bulk power system from cyberattack. In the 110th Congress, as chairman of the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I conducted a detailed and thorough examination of cyberthreats to our critical infrastructure, and I want to reiterate what I made clear in my testimony.

I believe that America is still vulnerable to a cyberattack against the electric grid, which would cause severe damage, not only to our critical infrastructure, but also to our economy and

to the welfare of our citizens. The vast majority of our critical assets is in private hands. In many sectors, private entities are largely self-regulated and are responsible for developing and for implementing their own standards according to their own priorities.

This bill will ensure that serious threats to our electric grid are addressed by giving the Federal Government the ability to require strong safety measures in our electric power system. It has the foresight to not only specifically focus on cyberthreats but also to focus on other potentially devastating issues, such as electromagnetic interference. These measures will help to ensure that we prepare for the worst case scenarios and that we protect our citizens in the case of a devastating attack or accident.

So, again, I really want to thank Chairman MARKEY for his attention to this important issue, and I look forward to working with the Energy and Commerce Committee in continuing to raise awareness about securing our critical infrastructure and in protecting our citizens from cyberattack.

Mr. Speaker, I rise today in support of H.R. 5026, legislation to protect our national electric grid system. I would like to thank Chairman MARKEY for his leadership on this important national security issue. I would also like to recognize my good friend and Chairman of the Homeland Security Committee, Mr. THOMPSON, for working with me in 2008 to hold hearings and closely examine what actions our country must take to prevent attacks on our national grid.

Two years ago, on September 11, 2008, I testified before Chairman MARKEY's Subcommittee about the threats to our bulk power system from cyber attack. In the 110th Congress, as Chairman of the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I conducted a detailed and thorough examination of cyber threats to our critical infrastructure, and I want to reiterate what I made clear in my testimony. I believe America remains vulnerable to a cyber attack against the electric grid that would cause severe damage to not only our critical infrastructure, but also our economy and the welfare of our citizens.

The vast majority of our critical assets are in private hands. In many sectors, private entities are largely self-regulated and are responsible for developing and implementing their own standards according to their own priorities. This bill will ensure that serious threats to our grid are addressed by giving relevant government agencies, such as the Department of Homeland Security, the ability to require strong safety measures in our electric power system. The bill also has the foresight to not only specifically focus on cyber threats but also on other potentially devastating issues such as electromagnetic interference. The scope of the bill includes the bulk power system, which should also protect critical distribution systems in major cities, like New York and Washington, DC from a cyber attack. Additionally, by empowering the Federal Energy Regulatory Commission, FERC, this legislation goes a long way to enabling a faster response by both government and industry in case of an imminent threat. These measures will help ensure that we prepare for worst-case scenarios and protect our citizens in the case of a devastating attack or catastrophe.

I applaud the attention being focused on this issue by the Congress, and I want to once again thank Chairman MARKEY for his attention to this important issue. I look forward to working with the Energy and Commerce Committee and to securing our critical infrastructure and protecting our citizens from cyber attack.

Mr. UPTON. Mr. Speaker, I ask unanimous consent to reclaim the balance of my time.

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

There was no objection.

Mr. UPTON. I yield 2 minutes to the distinguished gentleman from Maryland (Mr. BARTLETT), who is in support of the bill.

Mr. BARTLETT. Mr. Speaker, I rise in strong support of the bipartisan bill, H.R. 5026, which has been approved unanimously by a vote of 47–0 by the Energy and Commerce Committee. That doesn't happen very often in today's Congress.

According to the National Academy of Sciences, this bill is necessary because there is one event that we will not avoid, and that is solar geomagnetic interference—a solar storm. If—really, when—we have a big one like the Carrington event that occurred in 1859, this will shut down our whole grid. It would cost us only about $100 million to protect the grid from EMP. This investment won't be made without H.R. 5026. The consequences of inaction are dire. If our grid is destroyed by EMP or by a Carrington event, which is an electromagnetic storm, the National Academies warn it will cost us between $1 trillion and $2 trillion in damages, and it will take 4 to 10 years to recover.

With the grid's being down, more or less, for 4 to 10 years, one can only imagine the consequences to our society. This is a really important bipartisan bill, and I rise in very strong support.

Mr. MARKEY of Massachusetts. Mr. Speaker, I yield myself such time as I may consume.

The GRID Act has three basic components.

First, it establishes Federal authority to address emergency situations. If the President identifies an imminent threat to the bulk power system or to other parts of the grid that serve critical defense facilities, the Federal Energy Regulatory Commission can issue an emergency order requiring measures to protect against this threat. This authority covers threats from cyberattacks, from electromagnetic weapons, from direct physical attacks, or from solar storms.

However, in many cases, we will not know about a cyberattack or other threat to the grid until it's too late. Accordingly, the GRID Act establishes measures to protect the grid against key vulnerabilities so that, if and when an emergency does happen, we are already prepared.

Most importantly, if FERC identifies a vulnerability to a cyber or to an electromagnetic attack that has not adequately been addressed, it has the authority to require intramеasures to protect the bulk power system.

The legislation also requires FERC, within 6 months of enactment, to establish measures to protect against the Aurora vulnerability to cyberattack. That vulnerability was identified nearly 3 years ago, but the current standard-setting process has not addressed it. That is unacceptable. It must be fixed.

Ranking Member UPTON and other members of our committee sat through a top secret briefing last October with regard to the threat that this Aurora vulnerability and that other vulnerabilities pose as potential threats to our country and which could be exploited by other countries or by subnational groups or by domestic terrorists. This is something that we must close. I think every Member in that top secret briefing left, having experienced a sobering moment in their lives, realizing the great responsibility we have to pass legislation that can deal with this problem.

The GRID Act also deals with other critical vulnerabilities. Solar flares cause geomagnetic currents that can destroy large electric transformers. Experts agree that it is only a matter of time before we experience a solar storm large enough to bring down a large portion of the grid, potentially causing trillions of dollars in damage. In addition, the grid is highly vulnerable to attack because the large transformers upon which it relies are built overseas and can take years to replace. The GRID Act addresses these issues by requiring the development of reliability standards to protect against geomagnetic storms and to ensure the availability of adequate backup supplies of large transformers.

Finally, the GRID Act gives FERC the authority to protect portions of the grid that serve the top 100 critical defense facilities against a cyber or an electromagnetic weapons attack.

The amended version of the bill now before the House makes one change to the version reported out of committee. In order to make the bill deficit neutral, the amended bill exempts the Bonneville Power Administration and the Tennessee Valley Authority from requirements other than cyberprotections during the first 11 years after enactment. With this change, the Congressional Budget Office has determined that the bill will not affect direct Federal spending. The amended bill does not score.

Colleagues, the electric grid's vulnerability to cyber and to other attacks is one of the single greatest threats to our national security. This bipartisan legislation is critical to empowering the Federal Government and the private sector with the capacities they

will need to protect us against that threat.

□ 1115

There are people plotting right now that, if they could, would exploit this vulnerability.

I urge all Members to vote ''yes'' on the GRID Act. It is a moment that we must all come together in order to protect our country.

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

Mr. UPTON. Mr. Speaker, I yield 2 minutes to the distinguished ranking member of the full committee, the gentleman from Texas (Mr. BARTON), in support of the bill.

Mr. BARTON of Texas. Mr. Speaker, I want to compliment Chairman MARKEY for referring to Mr. UPTON as ''Chairman UPTON.'' That may be a foreteller of things to come, and we appreciate his prescience in acknowledging that possibility.

Mr. Speaker, I do rise in support of H.R. 5026, the Grid Reliability and Infrastructure Defense Act, better known as the GRID Act.

This is an example of legislation that has come to the floor after a 47–0 bipartisan vote in the Energy and Commerce Committee that shows what the Congress can do when Republicans are allowed into the room to help draft and put into place legislation. While it is a rare occasion in this Congress, it certainly is something that both sides of the aisle can be proud of.

I want to especially commend Subcommittee Chairman MARKEY, Full Committee Chairman WAXMAN, Ranking Member UPTON, and others on both sides of the aisle to make this day possible.

Our electric grid is increasingly vulnerable to cyber attack, and if a nation-state or a terrorist group were successful in crippling our electric grid, it would have devastating consequences for our economy and our national defense. We've read news stories reporting allegations that spies may have penetrated the mechanisms that control our power supplies.

Cybersecurity experts report that the ''smart grid'' we are counting on to improve reliability and enhance consumer choices could also increase our exposure to hackers in places like China and Russia. Our defense community is concerned about possible electromagnetic attacks from terrorist or hostile countries. We must take substantive action to address the susceptibility of our electric systems to such attacks. The stakes are just too high for us to do nothing.

The GRID Act, Mr. Speaker, takes care of all these problems.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. UPTON. I yield the gentleman 1 additional minute.

Mr. BARTON of Texas. I appreciate the ranking member's yielding additional time.

The GRID Act would shield both our bulk power system and the infrastructure serving critical defense facilities. The legislation authorizes the President to address imminent grid security threats through the Federal Energy Regulatory Commission, better known as FERC. It would give FERC the authority to issue notice-and-comment rule to address grid security vulnerabilities.

As Mr. MARKEY pointed out, this bill is revenue-neutral. It does not increase the Federal deficit in any shape, form, or fashion. It is worthy of support.

I want to repeat again, it came out the Energy and Commerce Committee 47–0. I hope the House will unanimously vote for this and send it to the other body.

Mr. MARKEY of Massachusetts. I thank the gentleman from Michigan for working with the majority in such a cooperative fashion. National defense is an area where we should be trying to cooperate, and this bill is a preeminent example of that happening in this Congress. And I want to thank him and the gentleman from Texas (Mr. BARTON) for creating that atmosphere which made it possible.

I think that this is a historic piece of legislation. Mr. WAXMAN and I and all of the Members on our side really do believe that this is the way Congress should work. I congratulate the gentleman for his work on it.

I have no further requests for time, and I reserve the balance of my time.

Mr. UPTON. Mr. Speaker, I yield myself the balance of my time.

I just want to say, this is an issue that we sat down together for the last, actually, couple of years examining the facts. Many of us that particularly live in areas—for me, the Midwest, coming from Michigan, we had a devastating tornado come through this weekend, and for many of us, myself included, our electricity went out for a number of hours. And then a number of times, particularly during the winter and even in the summer where these electric storms that come through, sometimes the electricity may be out for a couple of days.

We look to our friends down in Haiti who, many of them still may not have electricity after the devastating earthquake that hit there a number of months ago. Can you imagine if that happened here in this country, where, because of our grid vulnerabilities, you could be perhaps out of electricity for a year or 2, trying to get gasoline to get out of there, trying to get refrigeration for your food, trying to have a job, take care of your family?

Some of us read the book ''The Road.'' Lots of different scenarios that are out there. We need to be prepared. This bill moves us down that road.

And I again want to compliment my friend, Mr. MARKEY, to make sure that this legislation did move through. We had a lot of bipartisan support, a lot of eyes opened and ears too, particularly as we sat through some of those classified briefings. Let's hope that the Senate moves quickly, the President signs it swiftly, and, in fact, we can see legislation move to make sure that those scenarios remain that way and don't become realities.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise today in support of H.R. 5026, the Grid Reliability and Infrastructure Defense—or GRID—Act.

As Chairman of the House Committee on Homeland Security, I am well aware of the need to protect our Nation's critical infrastructure.

Our Committee has held numerous classified briefings and public hearings on threats to the electric grid. Again and again, we received testimony from expert witnesses that our Nation's electric grid has inadequate protections against cyber attacks and against significant disruptions from electromagnetic threats, EMP, such as solar storms and radio frequency devices.

Further, the Federal Government does not have the authority to ensure its security, nor has it partnered effectively with the private sector to do so.

Protecting our electric grid from EMP will require the best efforts from both government and industry. To date, the electric sector has had a difficult time protecting their assets from EMP threats because although the potential impacts are huge, the frequency of their occurrence is very low.

This is one of those cases where government intervention seems necessary to protect our most important national critical infrastructure.

Last year, I, along with my ranking member PETER KING and many other bipartisan members of our Committee introduced H.R. 2195 to give the Federal Energy Regulatory Commission authority to require protections to be put in place for high impact, low frequency events.

H.R. 5026 is the product of collaborative work between this Committee and our colleagues on the Energy and Commerce Committee, most notably Chairman WAXMAN and Representatives MARKEY and BARROW.

Our electric grid is currently strained to capacity.

We saw during the Northeast Blackout of 2003 what can happen when the strained system finally breaks. That blackout interrupted electricity delivery to 55 million people in the U.S. and Canada. Luckily, major outages only lasted a day or so.

But just imagine what would happen if the power did not come back on for a week, or a month, or several months. What would happen?

An elecromagnetic pulse could make such an incredible scenario a reality.

The one that most people have heard about is from a high altitude burst of a nuclear weapon.

Also of concern are smaller radio or microwave devices, usually termed ''Intentional Electromagnetic Interference'' or ''IEMI''.

Of particular concern are ''geomagnetically induced currents'', GIC, caused by solar activity.

A 2008 National Academy of Sciences report warned that our Sun will inevitably inflict a severe geomagnetic storm with the largest geographic footprint of any natural disaster. The damage caused by this event could be $1 trillion to $2 trillion, and recovery could take 4 to 10 years.

The next period of maximum solar activity is only two years away.

From a homeland security perspective, it is important that we take an ''all hazards'' approach to the risk and increase preparedness for both intentional and naturally occurring events.

While some may argue that the threat of a high-altitude nuclear weapon burst perpetrated by a rogue state or a terrorist group is remote, I do not discount it. Given the high-consequence nature of such an attack, I take it very seriously.

On the other hand, scientists tell us that the likelihood of a severe naturally occurring geomagnetic event capable of crippling our electric grid is 100 percent. It will happen; it is just a question of when.

GIC is a natural occurrence just like earthquakes, wildfires, tornadoes or hurricanes.

Similarly, geomagnetic storms occur from time to time as part of the natural activity of the Sun. One such storm, in 1989, disrupted power throughout most of Quebec, and resulted in auroras as far south as Texas.

With the significant investments we are making in ''Green Energy'' and the ''Smart Grid'', we find ourselves at an opportune moment to protect our grid from an EMP and cyber attacks.

As we expand and improve our grid, we must also build in physical and cyber protections from the start, and we must retrofit key elements of the existing grid in order to protect it.

Federal authority and funding are needed if this effort is to succeed. H.R. 5026 represents a critical step forward in our efforts to meet these homeland security challenges and deserves support from this House.

Therefore, I urge Members to join me and support H.R. 5026.

Ms. CLARKE. Mr. Speaker, I rise today in strong support of H.R. 5026, the Grid Reliability and Infrastructure Defense Act, and urge my colleagues to support it. I thank my colleague Chairman MARKEY for bringing this important legislation to the floor.

The GRID Act empowers the Federal Energy Regulatory Commission, in the event of a Presidential emergency declaration, to take actions needed to protect our grid.

I have said this before but it bears repeating: A modern society is characterized by the presence of three things: clean available water, properly functioning sewage and sanitation services, and electricity.

I would further assert that the way our present systems function, electricity is needed to power those other critical systems. So at a minimum, we rely on electricity to function as a modern society.

It is our very reliance on this infrastructure that makes it an obvious target for attack. We know that many of our adversaries—from terrorist groups to nation states—have and continue to develop capabilities that would allow them to attack and destroy our grid at a time of their choosing.

There are two significant threats to the electric grid. One is the threat of cyber attack. Many nation states, like Russia, China, North Korea, and Iran, have offensive cyber attack capabilities, while terrorist groups like Hezbollah and al Qaeda continue to work to develop capabilities to attack and destroy critical infrastructure like the electric grid through cyber means.

If you believe intelligence sources, our grid is already compromised. An April 2009 article in the Wall Street Journal cited intelligence sources who claim that the grid has already been penetrated by cyber intruders from Russia and China who are positioned to activate malicious code that could destroy portions of the grid at their command.

The other significant threat to the grid is the threat of a physical event that could come in the form of a natural or manmade Electromagnetic Pulse, known as EMP. The potentially devastating effects of an EMP to the grid are well documented.

During the Cold War, the U.S. government simulated the effects of EMP on our infrastructure, because of the threat of nuclear weapons, which emit an EMP after detonation. Though we may no longer fear a nuclear attack from Soviet Russia, rogue adversaries (including North Korea and Iran) possess and test high altitude missiles that could potentially cause a catastrophic pulse across the grid.

These are but two of the significant emerging threats we face in the 21st century. Our adversaries openly discuss using these capabilities against the United States. According to its ''Cyber Warfare Doctrine,'' China's military strategy is designed to achieve global ''electronic dominance'' by 2050, to include the capability to disrupt financial markets, military and civilian comunications capabilities, and the electric grid prior to the initiation of traditional military operations.

Cyber and physical attacks against the grid could both be catastrophic and incredibly destructive events, but they are not inevitable. Protections can—and must—be put in place ahead of time to mitigate the impact of these attacks.

The time for action is now, support the GRID Act and help ensure America's future.

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

Mr. MARKEY of Massachusetts. I yield back the balance of my time with the urging of an ''aye'' vote by the Members.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Massachusetts (Mr. MARKEY) that the House suspend the rules and pass the bill, H.R. 5026, as amended.

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

The title was amended so as to read: ''A bill to amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities.''

A motion to reconsider was laid on the table.

WORLD OCEAN DAY

Ms. CHU. Mr. Speaker, I move to suspend the rules and agree to the resolution (H. Res. 1330) recognizing June 8, 2010, as World Ocean Day, as amended.

The Clerk read the title of the resolution.

The text of the resolution is as follows:

H. RES. 1330

Whereas in 2008, the United Nations General Assembly decided that, as of 2009, June 8 would be designated by the United Nations as ''World Ocean Day'';

Whereas many countries have celebrated World Ocean Day following the United Nations Conference on Environment and Development, which was held in Rio de Janeiro, Brazil, in 1992;

Whereas World Ocean Day allows us the yearly opportunity to pay tribute to the ocean for what it provides;

Whereas we have an individual and collective duty, both nationally and internationally, to protect, conserve, maintain, and rebuild our ocean and its resources;

Whereas our present ocean stewardship is necessary to provide for current and future generations;

Whereas the world depends on the health of our ocean for a full range of ecological, economic, educational, scientific, social, cultural, nutritional, and recreational benefits;

Whereas the ocean is linked to adaptation to climate and other environmental change, foreign policy, and national and homeland security;

Whereas we must ensure accountability for our actions, and serve as a model country promoting balanced, productive, efficient, sustainable, and informed ocean, coastal, and Great Lakes use, management, and conservation within the global community; and

Whereas our ocean is in need of strong policies that support ecosystem-based management, coastal and marine spatial planning, informed science-based decision making and improved understanding, government coordination, regional ecosystem protection and restoration, enhanced water quality and sustainable practices on land, changing conditions in the Arctic as well as ocean, coastal, and Great Lakes observations and infrastructure: Now, therefore, be it

Resolved, That the House of Representatives recognizes World Ocean Day.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from California (Ms. CHU) and the gentleman from Ohio (Mr. TURNER) each will control 20 minutes.

The Chair recognizes the gentlewoman from California.

GENERAL LEAVE

Ms. CHU. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from California?

There was no objection.

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

Mr. Speaker, on behalf of the Committee on Oversight and Government Reform, I'm happy to rise in support of House Resolution 1330. This measure recognizes June 8, 2010, as World Ocean Day.

World Ocean Day offers the opportunity to celebrate the wonders of the underwater world and look carefully at our interactions with the sea.

The timing of this measure is critical. Today we find ourselves in the midst of the worst ocean oil disaster in our Nation's history. With our addiction to oil jeopardizing the vibrant and economically vital marine life of America's seas, we are being reminded daily of the often-forgotten value of