

Safety and Health, directed the preparation of this notice. The authority for this notice is the Paperwork Reduction Act of 1995 (44 U.S.C. 3506 *et seq.*) and Secretary of Labor's Order No. 5-2010 (75 FR 55355).

Signed at Washington, DC, on August 17, 2011.

David Michaels,

Assistant Secretary of Labor for Occupational Safety and Health

[FR Doc. 2011-21373 Filed 8-19-11; 8:45 am]

BILLING CODE 4510-26-P

DEPARTMENT OF LABOR

Office of Workers' Compensation Programs

Proposed Renewal of Existing Collection; Comment Request

ACTION: Notice.

SUMMARY: The Department of Labor, as part of its continuing effort to reduce paperwork and respondent burden, conducts a preclearance consultation program to provide the general public and Federal agencies with an opportunity to comment on proposed and/or continuing collections of information in accordance with the Paperwork Reduction Act of 1995 (PRA95) [44 U.S.C. 3506(c)(2)(A)]. This program helps to ensure that requested data can be provided in the desired format, reporting burden (time and financial resources) is minimized, collection instruments are clearly understood, and the impact of collection requirements on respondents can be properly assessed. Currently, the Office of Workers' Compensation Programs is soliciting comments concerning the proposed collection: Agreement and Undertaking (OWCP-1). A copy of the proposed information collection request can be obtained by contacting the office listed below in the addresses section of this Notice.

DATES: Written comments must be submitted to the office listed in the addresses section below on or before October 21, 2011.

ADDRESSES: Mr. Vincent Alvarez, U.S. Department of Labor, 200 Constitution Ave., NW., Room S-3201, Washington, DC 20210, telephone (202) 693-0372, fax (202) 693-2447, E-mail Alvarez.Vincent@dol.gov. Please use only one method of transmission for comments (mail, fax, or E-mail).

SUPPLEMENTARY INFORMATION

I. Background: Coal mine operators desiring to be self-insurers are required by law (30 U.S.C. 933 BL) to produce security by way of an indemnity bond,

security deposit, a letter of credit, or 501(c)(21) trust. Once a company's application to become self-insured is reviewed by the Division of Coal Mine Workers' Compensation (DCMWC) and it is determined the company is potentially eligible, an amount of security is determined to guarantee the payment of benefits required by the Act. The OWCP-1 form is executed by the self-insurer who agrees to abide by the Department's rules and authorizes the Secretary, in the event of default, to file suit to secure payment from a bond underwriter or in the case of a Federal Reserve account, to sell the securities for the same purpose. A company cannot be authorized to self-insure until this requirement is met. Regulations establishing this requirement are at 20 CFR 726.110 for Black Lung. This information collection is currently approved for use through October 31, 2011.

II. Review Focus: The Department of Labor is particularly interested in comments which:

- * Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

- * Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

- * Enhance the quality, utility and clarity of the information to be collected; and

- * Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

III. Current Actions: The Department of Labor seeks the approval of the extension of this currently approved information collection in order to determine if a coal mine company is potentially eligible to become self-insured. The information is reviewed to insure that the correct amounts of negotiable securities are deposited or indemnity bond is purchased and that in a case of default OWCP has the authority to utilize the securities or bond. If this Agreement and Undertaking were not required, OWCP would not be empowered to utilize the company's security deposit to meet its financial responsibilities for the payment of black lung benefits in case of default.

Type of Review: Extension.

Agency: Office of Workers' Compensation Programs.

Title: Agreement and Undertaking.

OMB Number: 1240-0039.

Agency Number: OWCP-1.

Affected Public: Businesses or other for-profit.

Total Respondents: 20.

Total Responses: 20.

Time per Response: 15 minutes.

Estimated Total Burden Hours: 5.

Total Burden Cost (capital/startup):

\$0.

Total Burden Cost (operating/maintenance): \$9.

Comments submitted in response to this notice will be summarized and/or included in the request for Office of Management and Budget approval of the information collection request; they will also become a matter of public record.

Dated: August 17, 2011.

Vincent Alvarez,

Agency Clearance Officer, Office of Workers' Compensation Programs, U.S. Department of Labor.

[FR Doc. 2011-21382 Filed 8-19-11; 8:45 am]

BILLING CODE 4510-CR-P

LEGAL SERVICES CORPORATION

Sunshine Act Meeting; Notice

DATE AND TIME: The Legal Services Corporation's Board of Directors will meet telephonically on August 25, 2011. The meeting will commence at 10:30 a.m., Eastern Standard Time, and will continue until the conclusion of the Board's agenda.

LOCATION: F. William McCalpin Conference Center, Legal Services Corporation, 3333 K Street, NW., Washington, DC 20007.

PUBLIC OBSERVATION: Members of the public who are unable to attend but wish to listen to the public proceeding may do so by following the telephone call-in directions provided below but are asked to keep their telephones muted to eliminate background noises. From time to time the Chairmana may solicit comments from the public.

CALL-IN DIRECTIONS FOR OPEN SESSIONS:

- Call toll-free number: 1-866-451-4981;

- When prompted, enter the following numeric pass code: 5907707348

- When connected to the call, please immediately "MUTE" your telephone.

STATUS OF MEETING: Open.

Matters To Be Considered

1. Approval of Agenda.

2. Consider and act on the Finance Committee's recommendation regarding LSC's FY 2013 appropriation request.

3. Public comment.

4. Consider and act on other business.

5. Consider and act on adjournment of meeting.

CONTACT PERSON FOR INFORMATION:

Katherine Ward, Executive Assistant to the Vice President & General Counsel, at (202) 295-1500. Questions may be sent by electronic mail to FR_NOTICE_QUESTIONS@lsc.gov.

ACCESSIBILITY: LSC complies with the American's with Disabilities Act and Section 504 of the 1973 Rehabilitation Act. Upon request, meeting notices and materials will be made available in alternative formats to accommodate individuals with disabilities.

Individuals who need other accommodations due to disability in order to attend the meeting in person or telephonically should contact Katherine Ward, at (202) 295-1500 or FR_NOTICE_QUESTIONS@lsc.gov, at least 2 business days in advance of the meeting. If a request is made without advance notice, LSC will make every effort to accommodate the request but cannot guarantee that all requests can be fulfilled.

Dated: August 18, 2011.

Victor M. Fortuno,

Vice President & General Counsel.

[FR Doc. 2011-21551 Filed 8-19-11; 4:15 pm]

BILLING CODE 7050-01-P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: "Current Implementations of Cloud Computing Indicate a New Approach to Security"

AGENCY: The National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) Program, National Science Foundation.

ACTION: Call for participation.

FOR FURTHER INFORMATION CONTACT:
assumptionbusters@nitrd.gov.

DATES: Workshop: October 21, 2011; Deadline: September 21, 2011. Apply via e-mail to assumptionbusters@nitrd.gov. Travel expenses will be paid for selected participants who live more than 50 miles from Washington, DC, up to the limits established by Federal Government travel regulations and restrictions.

SUMMARY: The NCO, on behalf of the Special Cyber Operations Research and

Engineering (SCORE) Committee, an interagency working group that coordinates cyber security research activities in support of national security systems, is seeking expert participants in a day-long workshop on the pros and cons of the Security of Distributed Data Schemes. The workshop will be held October 21, 2011 in Gaithersburg, MD. Applications will be accepted until 5 p.m. EST September 21, 2011. Accepted participants will be notified by October 1, 2011.

SUPPLEMENTARY INFORMATION:

Overview: This notice is issued by the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) Program on behalf of the SCORE Committee.

Background: There is a strong and often repeated call for research to provide novel cyber security solutions. The rhetoric of this call is to elicit new solutions that are radically different from existing solutions. Continuing research that achieves only incremental improvements is a losing proposition.

We are lagging behind and need technological leaps to get, and keep, ahead of adversaries who are themselves rapidly improving attack technology. To answer this call, we must examine the key assumptions that underlie current security architectures. Challenging those assumptions both opens up the possibilities for novel solutions and provides an even stronger basis for moving forward on those assumptions that are well-founded. The SCORE Committee is conducting a series of four workshops to begin the assumption buster process. The assumptions that underlie this series are as follows: Cyber space is an adversarial domain; the adversary is tenacious, clever, and capable; and re-examining cyber security solutions in the context of these assumptions will result in key insights that will lead to the novel solutions we desperately need. To ensure that our discussion has the requisite adversarial flavor, we are inviting researchers who develop solutions of the type under discussion, and researchers who exploit these solutions. The goal is to engage in robust debate of topics generally believed to be true to determine to what extent that claim is warranted. The adversarial nature of these debates is meant to ensure the threat environment is reflected in the discussion in order to elicit innovative research concepts that will have a greater chance of having a sustained positive impact on our cyber security posture.

The fourth topic to be explored in this series is cloud computing. The

workshop on this topic will be held in Gaithersburg, MD on October 21, 2011.

Assertion: "Current implementations of cloud computing indicate a new approach to security"

Implementations of cloud computing have provided new ways of thinking about how to secure data and computation. Cloud is a platform upon which we leverage various opportunities to improve the way in which we think about and implement the practices and technology needed to secure the things that matter most to us. Current implementations of cloud computing security take advantage of the unique capabilities and architectures of cloud computing (e.g. scale).

Working from this assertion, we want researchers and cloud implementers to submit, as part of your application to participate in the October 21st Assumption Buster Workshop, a one-page paper stating your opinion of the assertion and outlining your key thoughts on the topic. Below are some additional areas to explore stated specifically in strong language supportive of the assertion.

- Controls on provider side, controls on the subscribe-side, and controls of the shared space in cloud implementations can be defined in ways that allow for a comprehensive view of the cloud security landscape to be displayed and managed.
- A common security risk model can be leveraged when assessing cloud computing services and products, and use of this model provides a consistent baseline for Cloud based technologies.
- Cloud computing security is a natural fit when examined against the Federal cybersecurity research themes focused on designed-in-security, tailored trustworthy spaces, moving target, and cyber economic incentives. These themes will be best demonstrated using Cloud Computing.
- Opportunities exist to create existence proofs for specific security improvements such as minimal kernels that can be formally verified which could provide a stronger basis for virtual machines.
- We can establish a trust boundary remote-control that allows a cloud customer to directly control system boundaries.
- Credible explications of security priorities are possible thus enabling customers to obtain a complete picture and insight into the security offered by their cloud implementation.
- Cloud customers are able to measure the strength of the logical separation