Notification of Anticipated Contract termination or Reduction; OMB Control Number 0704–0533.

Affected Public: Businesses or other for-profit and not-for-profit institutions.

Respondent's Obligation: Required to obtain or retain benefits.

Type of Request: Renewal of a currently approved collection.

Reporting Frequency: On occasion.

Number of Respondents: 42.

Responses per Respondent: 6.19, approximately.

Annual Responses: 260.

Average Burden per Response: .74 hours.

Annual Burden Hours: 193.

Needs and Uses: DFARS clause 252.249–7002, Notification of Anticipated Contract termination or Reduction, is used in all contracts under a major defense program. The purpose of this requirement is to help establish benefit eligibility under the Job Training Partnership Act (29 U.S.C. 1661 and 1662) for employees of DoD contractors and subcontractors adversely affected by contract termination or substantial reductions under major defense programs.

OMB Desk Officer: Ms. Jasmeet Seehra.

Comments and recommendations on the proposed information collection should be sent to Ms. Jasmeet Seehra, DoD Desk Officer, at *Oira_submission@omb.eop.gov.* Please identify the proposed information collection by DoD Desk Officer and the Docket ID number and title of the information collection.

You may also submit comments, identified by docket number and title, by the following method:

Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

DoD Clearance Officer: Mr. Frederick C. Licari.

Written requests for copies of the information collection proposal should be sent to Mr. Licari at: WHS/ESD Directives Division, 4800 Mark Center Drive, 2nd Floor, East Tower, Suite 03F09, Alexandria, VA 22350–3100.

Jennifer Lee Hawes,

Regulatory Control Officer, Defense Acquisition Regulations System.

[FR Doc. 2018–08552 Filed 4–23–18; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

[Docket DARS–2018–0023]

DoD Guidance for Reviewing System Security Plans and the NIST SP 800–171 Security Requirements Not Yet Implemented

AGENCY: Department of Defense (DoD).

ACTION: Notice and request for comment.

SUMMARY: DoD has drafted guidance for procurements requiring implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and is making the draft guidance available to the public.

DATES: Comments are due by May 31, 2018.

ADDRESSES: You may submit comments, identified by docket DARS–2018–0023, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Search for ''DARS–2018–0023.'' Select ''Comment Now'' and follow the instructions provided to submit a comment. Please include ''DARS–2018–0023'' on any attached documents.
- *Mail:* Defense Procurement and Acquisition Policy, Attn: Ms. Mary Thomas, OUSD(A&S) DPAP/PDI, Room 3C958, 3060 Defense Pentagon, Washington, DC 20301–3060.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Thomas, DPAP/PDI, at *mary.s.thomas.civ@mail.mil* or by mail at: Defense Procurement and Acquisition Policy, Attn: Ms. Mary Thomas, OUSD(A&S) DPAP/PDI, Room 3C958, 3060 Defense Pentagon, Washington, DC 20301–3060.

SUPPLEMENTARY INFORMATION:

The Defense Federal Acquisition Regulation Supplement clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to provide ''adequate security'' for ''covered defense information'' that is processed, stored, or transmitted on the contractor's internal information system or network. To provide adequate security, the contractor must, at a minimum, implement NIST SP 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.'' NIST SP 800–171 states that in order to demonstrate implementation or planned implementation of the security requirements in NIST SP 800–171, nonfederal organizations should describe in a System Security Plan how the specified security requirements are met, or how organizations plan to meet the requirements, and should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. NIST SP 800–171 further states that, when requested, the System Security Plan and any associated Plans of Action for any planned implementations or mitigations should be submitted to the responsible Federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements.

DoD developed the document ''DoD Guidance for Reviewing System Security Plans and the NIST SP 800–171 Security Requirements Not Yet Implemented'' to facilitate the consistent review and understanding of System Security Plans and Plans of Action, the impact that NIST SP 800–171 Security Requirements that are ''not yet implemented'' have on an information system, and to assist in prioritizing the implementation of security requirements not yet implemented. The document ''Assessing the State of a Contractor's Internal Information System in a Procurement Action'' illustrates how ''DoD Guidance for Reviewing System Security Plans and the NIST SP 800–171 Security Requirements Not Yet Implemented'' may be used during a procurement for which DoD must assess the state of a contractor's internal information system.

''DoD Guidance for Reviewing System Security Plans and the NIST SP 800–171 Security Requirements Not Yet Implemented'' provides a ''DoD Value'' to assess the risk that a security requirement left unimplemented has on an information system, to assess the risk of a security requirement with an identified deficiency, and to address the priority for which an unimplemented requirement should be implemented. The guidance also addresses the method(s) to implement the security requirements, and, when applicable, provides clarifying information for security requirements that are frequently misunderstood.

The matrix ''Assessing the State of a Contractor's Internal Information System in a Procurement Action'' is provided to illustrate how DoD may choose to assess submitted System Security Plans and Plans of Action in procurement actions that require the implementation of NIST SP 800–171.

To access the documents entitled ''DoD Guidance for Reviewing System Security Plans and the NIST SP 800–171 Security Requirements Not Yet Implemented'' and ''Assessing the State of a Contractor's Internal Information System in a Procurement Action,'' go to the Federal eRulemaking Portal at *www.regulations.gov,* search for the docket ''DARS–2018–0023'' click ''Open Docket,'' and view ''Supporting Documents.''

Jennifer Lee Hawes,

Regulatory Control Officer, Defense Acquisition Regulations System.

[FR Doc. 2018–08554 Filed 4–23–18; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2018–OS–0021]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, Department of Defense.

ACTION: Notice of a modified system of records.

SUMMARY: The Office of the Secretary of Defense (OSD) proposes to modify a system of records notice entitled GlobalNET Outreach and Collaboration Platform, DSCA 02. This system is a web based technology solution that provides the Regional Center for Security Studies and Defense Security Cooperation Agency (DSCA) with a procedure to improve international outreach efforts as well as foster collaboration among their faculty, current and former students, OSD, and other designated Department of Defense (DoD) educational institutions and communities. The GlobalNET platform provides a collaborative social networking environment/capability for students, alumni, faculty, partners, and other community members.

DATES: Comments will be accepted on or before May 24, 2018. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* *Federal Rulemaking Portal: http://www.regulations.gov.*

Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, DC 20301–1155, or by phone at (571) 372–0478.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. The GlobalNET Outreach and Collaboration Platform (DSCA 02) is a web based information technology platform to improve international partner outreach and collaboration efforts in a federated environment. The system collects information on students in order to allow them to share information with peers, faculty, and regional center personnel. GlobalNET is the official DSCA system for performing alumni outreach, facilitating alumnus/professor communication and peer-to-peer communications (or social networking).

As a result of reviewing this system of records notice, the DSCA proposes to modify this system by updating the following sections: Categories of individuals, categories of records, authorities, routine uses, retention and disposal, notification procedure, record access procedures, and record source categories. This notice also reflects changes to ensure compliance with Office of Management and Budget Circular A–108.

The OSD notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy and Civil Liberties Division website at *https://defense.gov/privacy.*

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on February 27, 2018 to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB).

Dated: April 18, 2018.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER

GlobalNET Outreach and Collaboration Platform, DSCA 02.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Amazon Web Services, LLC, 13461 Sunrise Valley Drive, Herndon, VA 20171–3283.

GlobalNET Program Manager, Defense Security Cooperation Agency, ATTN: PGM/CMO, 201 12th Street S, Suite 203, Arlington, VA 22202–5408.

SYSTEM MANAGER(S):

GlobalNET Program Manager, Defense Security Cooperation Agency, ATTN: PGM/CMO, 201 12th Street S, Suite 203, Arlington, VA 22202–5408.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 134, Under Secretary of Defense for Policy; Department of Defense (DoD) Directive (DoDD) 5101.1, DoD Executive Agent; DoDD 5105.65, Defense Security Cooperation Agency (DSCA); DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; and DoDD 5200.41, DoD Regional Centers for Security Studies.

PURPOSE(S) OF THE SYSTEM:

This system is a technology solution that provides the Regional Center for Security Studies and Defense Security Cooperation Agency (DSCA) with a methodology to improve international outreach efforts as well as foster collaboration among their faculty, current and former students, OSD, and other designated Department of Defense (DoD) educational institutions and communities as required. The primary purpose of GlobalNET platform is to provide a collaborative social networking environment/capability for students, alumni, faculty, partners, and other community members.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

DoD Military and civilian employees, military students, alumni, contractors, systems integrators, and subject matter experts who interact with DoD educational institutions.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, country of residence, nationality, rank, email addresses,