SUPPORTING STATEMENT - PART A

National Industrial Security System (NISS) – 0704-0571

Summary of Changes from Previously Approved Collection

- Increase in wage estimates for Respondents and Processing Workers, but a decrease in Operational and Maintenance costs. This causes an increase in Total Labor Burden, but a net decrease in Total Cost to the Federal Government.

1. Need for the Information Collection

Executive Order 12829, "National Industrial Security Program" (NISP) Section 201-202 directs that "the Secretary of Defense serve as the Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees." The National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M) prescribes specific requirements to protect classified information released by U.S. Government agencies to contractors. The Secretary of Defense, as Executive Agent, has the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the NISP. Contractors participating in the NISP are subject to a Facility Security Clearance (FCL) Orientation Meeting to determine their eligibility to participate in the NISP. Additionally, contractors are subject to periodic Security Vulnerability Assessments (SVAs) to ensure that safeguards employed are adequate for the protection of classified information.

Department of Defense Directive 5104.42, "Subject: Defense Security Service" outlines the mission, organization and management, responsibilities and functions, relationships, authorities, and administration of DCSA. DCSA is a Defense Agency under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)). As it pertains to this request for authority to collect information, DCSA is responsible for the following:

- Managing, administering, and implementing the DoD portion of the NISP for DoD components, and 31 non-DoD agencies pursuant to E.O. 12829

- Exercising authority delegated to the Secretary of Defense for the issuance of security clearances to contractor employees, pursuant to E.O. 12829.

2. Use of the Information

DCSA performs its Mission to enable contractor performance on classified contracts, provide proactive oversight, and incident response to ensure compliance in accordance with the NISPOM. The National Industrial Security System (NISS) is the repository of records related to the collection and maintenance of information pertaining to contractor facility security clearances (FCL) and contractor capabilities to protect classified information in its possession. The information is utilized to determine if a company and its key management personnel are eligible for issuance of a facility clearance in accordance with NISPOM requirements. In addition, information is utilized to inform Government Contracting Activities (GCAs) of contractor's ability to maintain facility clearance status and/or storage capability as well as to analyze vulnerabilities identified within security programs and ensure proper mitigation actions are taken to preclude unauthorized disclosure of classified information.

The National Industrial Security System (NISS) deployed in September 2018. Industry and Government personnel have access to the system through a multifactor authentication requirement and establish accounts to maintain the accuracy of business records, standard forms, key management personnel, as well as provide reports to DCSA on events that may have an impact on their FCL. The system includes automated workflows to facilitate ease of information submission (as opposed to the previous manual process) as well as DCSA oversight of contractor security posture, authorization and accreditation of information systems, ensure accuracy of contract, technology, program, and overall facility data.

Users access the NISS through a web browser and fill out information through webforms, providing content in free text, check box, pick lists, drop-down, and file upload content. Information provided is digitally stored in the DCSA data center in Quantico, Virginia. Correspondence from the system to users also includes system-generated email notifications to inform the users of progress along workflows or that new information is available for them within the system.

To access NISS, users sign-in through the National Industrial Security Program (NISP) Central Access Information Security System (NCAISS), with a landing page that displays all appropriate disclosures associated with the Privacy Act Statement through a "Notice" prior to users logging in the system. NCAISS is a web portal that provides identity and access management services to authenticate users and provide access to different DCSA applications. To register, from the NCAISS login page (https://ncaiss-ps3.dss.mil/) users click on the "Register for an account" button to navigate to the self-enrollment form. Once the Self Enrollment form opens, users fill out the required information and associate their Common Access Card (CAC) or Personal Key Infrastructure from an External Certificate Authority (PKI/ECA) and click "Next." They are then given the opportunity to review their information and continue. Once they have submitted their form, NCAISS creates their account and notifies the user via email that their account is ready for use. After creating their NCAISS user account, users can then request NISS specific system access indicating their user role type.

NISS is the primary collection instrument for DCSA oversight of the NISP and maintaining data associated with cleared facilities and their oversight. One goal of the NISS application is to continue to alleviate burden and eventually eliminate processes of Industry personnel manually

entering information into multiple forms and then DCSA personnel manually entering the information collected from these forms into a computer system. As the NISS continues to improve towards full operational capability, the intention is to stop collecting information from various forms and use NISS as the single authoritative source for collection and maintenance of this information. As a note, the Standard Form (SF) 328 Certificate Pertaining to Foreign Interest (Rev. 11/2018 OMB Control Number 0704-0579) is a digitized form within the NISS and aggregates into NISS. However, it is used for multiple purposes within the Government, and therefore NISS is not subsuming this collection. Therefore, the SF 328 burden is not included in the NISS burden estimate below.

3. Use of Information Technology

Information Technology is the sole use for the purposes of this collection as the NISS is a technological solution to support current DCSA business needs. Each year DCSA expects 11,671 electronic respondents for this collection, consisting of industry and government personnel participating in the NISP. This collection will be 100% electronic. For every cleared contractor facility, a NISS account will be needed to streamline a facility's entry and active participation in the NISP to facilitate work on classified contracts. The use of NISS automates several workflows and decreases duplication of manual effort for DCSA, Contractors, and Government Contracting Activities (GCA). Contractors are responsible for maintenance of their NISS accounts.

4. Non-duplication

NISS is the only system to collect information with regard to DCSA administration and implementation of the NISP. No other collection vehicles exist to gather this information.

5. Burden on Small Business

The collection of information does not have a significant impact on small businesses or other entities. DCSA is requesting the minimum amount of information necessary for evaluation to which the company has agreed to supply per the DD Form 441 Security Agreement. Based on contractor responses for those smaller businesses participating in the NISP, the system omits portions not relevant to their activities.

6. Less Frequent Collection

If this data is not collected, this will hinder DCSA's ability to accurately evaluate performance related to the administration and implementation of the NISP as outlined in E.O. 12829. The initial information collection will be completed over the course of approximately one year. The follow up information collections will not begin until after that time and will take place sporadically with a portion of respondents depending on the need for evaluation/assessment and/or monitoring/assisting.

7. Paperwork Reduction Act Guidelines

The proposed data collection activities are consistent with the guidelines set forth in 5 CFR 1320.6 (Controlling Paperwork Burden on the Public- General Information Collection Guidelines). There are no special circumstances affecting this collection.

8. Consultation and Public Comments

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice (FRN) for the collection published on Monday, October 19, 2020. The 60-Day FRN citation is 85 FR 66313.

No comments were received during the 60-Day Comment Period.

A 30-Day Federal Register Notice for the collection published on Wednesday, January 13, 2021. The 30-Day FRN citation is 86 FR 2652.

Part B: CONSULTATION

No additional consultation apart from soliciting public comments through the Federal Register was conducted for this submission.

9. Gifts or Payment

No payments or gifts will be provided to respondents.

10. Confidentiality

Information provided by the responding population are handled by DCSA as “For Official Use Only,” sensitive commercial information. Respondents are provided with sufficient information to be assured of their privacy, and clearly understand their privacy rights when accessing the system. The log-in screen to the system explicitly provides the Privacy Act Statement. A copy of the Privacy Act Statement has been provided with this package for OMB’s review.

A draft copy of the SORN, “National Industrial Security System (V10-01)”, has been provided with this package for OMB’s review.

A copy of the PIA, “Privacy Impact Assessment for the National Industrial Security System (NISS) Defense Counterintelligence and Security Service (DCSA)” has been provided with this package for OMB’s review.

Retention and purging of electronic and hard copy files are in compliance with guidelines identified in schedule NC1-446-81-2 Item 2, "Industrial Security Facility Case Files." Records Schedule: DAA-0446-2017-0001 was submitted to NARA and approved. A summary of the Records Schedule: DAA-0446-2017-0001 follows:

- Electronic Files will be included and maintained with the same retention as paper files including in the NISS.
- Hard Copy Printouts and Electronic Records
    - Retention Period: Destroy when no longer needed
    - Destroy two years after facility security clearance is terminated. Files with Foreign Ownership Control and Influence (FOCI) material will be retained for 15 years then destroyed in accordance with NC1-446-85-2, item 12.

- NISS tracks facility clearance information including facility clearance requests, facility verification requests and notifications that are sent when facility information changes. The system also provides standard and customized reports. The major components of the system are described below:

    - Facilities Management allows the user to search facilities, view their facilities, and generate standard and ad hoc reports. Provides the capability for Industrial Security personnel to input actions performed directly related to oversight of cleared contractors, and the time associated with those actions. Facility Clearance Request allows the user to search and submit clearance requests. A clearance request is submitted when a user agency, facility, or other entity requests a clearance for the facility and initiates the clearance process. Email notifications are sent to the requestors when the clearance is issued. Facility Verification Requests allows the user to search existing verification requests, submit verification requests, and view their verifications. A Facility Verification Request is submitted when a requestor (User agency or a facility) wishes to be notified when certain information about a facility changes. Notifications allow the user to view all their notifications for facilities they submitted verification requests for. User Management allows the user to update user information. The system also provides separate online user's manuals for the external and internal users.

    - Select data from the following documents are entered into NISS from Industrial Security Case Files (physical and electronic files):

        - Sponsorship Letter

        - DD Form 254, Contract Security Classification Specification

        - DD Form 441, Department of Defense Security Agreement

        - DD Form 441-1, Appendage to the Department of Defense Security Agreement

        - List of Key Management Personnel (KMP)

        - SF 328, Certificate Pertaining to Foreign Interest

    - NISS contains the following types of information:

- Facility Overview
    - Overview
    - FCL Information
    - Addresses
    - KMP
    - Contacts
    - Prior Names and Alias
- Business Information
    - General Business Information
    - Legal Structure
    - Government Customers and Programs
    - Classified Subcontractors
    - SAM
    - CSI
- Foreign Ownership Control and Influence (FOCI) & International
    - Adjudication
    - Foreign Visits
    - Foreign Travel
    - Foreign Government Information
    - Exports
    - Foreign Sales and Subsidiaries
    - Freight Forwarding Countries
- Safeguarding & Information System (IS)

- Safeguarding
- General Safeguarding
- COMSEC
- Safeguarding Off-Sites
- Safeguarding Notes
- IS General Information Form

▪ Actions & Documentation

- Sponsorship Submissions
- Telephonic Surveys
- Briefings
- Facility Profile Documents

11. Sensitive Questions

Social Security Numbers are collected. An SSN Justification Memo is provided with this package for review. No other questions considered sensitive are collected.

12. Respondent Burden, and its Labor Costs

Note: There has been no modification to the Total Annual Responses or Response Time burden. The only modification below is to represent the updated average Respondent Hourly Wage based on 2020 rates compared to the 2017 rates used with the initial approval.

Part A: ESTIMATION OF RESPONDENT BURDEN

1) Collection Instrument
   National Industry Security System (NISS)
   a) Number of Respondents: 11,671
   b) Responses per Respondent: 1
   c) Number of Total Annual Responses: 11,671
   d) Response Time: 1 hour
   e) Respondent Burden Hours: 11,671

2) Total Submission Burden
   a) Total Number of Respondents: 11,671
   b) Total Number of Annual Responses: 11,671

c) Total Respondent Burden Hours: 11,671

Part B: LABOR COST OF RESPONDENT BURDEN

1) Collection Instrument
   National Industry Security System (NISS)
   a) Number of Total Annual Responses: 11,671
   b) Response Time: 1 hour
   c) Respondent Hourly Wage: $37.70
   d) Labor Burden per Response: $37.70
   e) Total Labor Burden: $439,996.70

2) Overall Labor Burden
   a) Total Number of Annual Responses: 11,671
   b) Total Labor Burden: $439,997

Respondent Hourly Wage of $37.70 is based on an approximate salary of a GS-13, Step 1 https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/20Tables/html/GS_h.aspx

13. Respondent Costs Other Than Burden Hour Costs

There is no cost associated with these tools for the respondent. Access to the system and respondent account requires an email address and Internet access, tools which cleared contractor facilities already have in place and/or have procedures in place to otherwise access online activities.

14. Cost to the Federal Government

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument
   National Industry Security System (NISS)
   a) Number of Total Annual Responses: 11,671
   b) Processing Time per Response: 1 hour
   c) Hourly Wage of Workers Processing Responses: $37.70
   d) Cost to Process Each Response: $37.70
   e) Total Cost to Process Responses: $439,996.70

2) Overall Labor Burden to the Federal Government
   a) Total Number of Annual Responses: 11,671
   b) Total Labor Burden: $439,996.70

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Total Operational and Maintenance Cost: $3,182,321

The FY2020 annual O&M cost of $3,182,321 includes system sustainment (data center hardware, MilCloud, supporting personnel) and system licensing. There are no administrative costs (printing, mailing, distributing and reviewing) since all action is taken through this automated information collection system.

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: $439,996.70

2) Total Operational and Maintenance Costs: $3,183,321

3) Total Cost to the Federal Government: $3,622,318

15. Reasons for Change in Burden

This is a renewal of an existing, approved OMB collection. There are two small changes in burden estimate. The estimated average hourly wage of respondents and workers has been increased to reflect 2020 figures, rather than the 2017 figures used in the prior submittal. The estimated Operational and Maintenance cost has also been lowered. The result of these two changes is an increase in Respondent Labor Burden but a net decrease in Total Cost to the Federal Government.

16. Publication of Results

The information collected will not be published. The data collection is primarily evaluated by DCSA to administer and implement the NISP, pursuant to Executive Order 12829. Congressional reports are provided on an annual basis with the total number of cleared facilities within the NISP, aggregate security vulnerability assessment ratings, and information system accreditation timelines.

17. Non-Display of OMB Expiration Date

Approval is not sought for avoiding display of the expiration date for OMB approval of the information collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

This submission describing data collection requests no exceptions to the Certificate for Paperwork Reduction Act (5 CFR 1320.9).