SUPPORTING STATEMENT - PART A

Navy Access Control System (NACS) and the U.S. Marine Corps Biometric and Automated Access Control System (BAACS) – 0703-0061

Summary of Changes from Previously Approved Collection:

- *The respondent labor burden and the cost to the federal government has increased since the previous approval. This is due to re-evaluating the wages of the respondent and the government workers processing the requests.*

1. Need for the Information Collection

In compliance with Section 3506(c)(2)(A) of the *Paperwork Reduction Act of 1995*, the Department of the Navy (DON), proposes renewal of a public information collection for the Information Technology (IT) collection system OMB Control Number 0703-0061, which includes the Navy Access Control System (NACS) and the U.S. Marine Corps Biometric Automated Access Control System (BAACS); The associated Form is SECNAV 5512/1 Department of the Navy Local Population ID Card/Base Access Pass Registration Form. The DON needs the information required by the proposed collection to adhere to the following statues or regulations that mandate or authorize the information collection:

a. 10 U.S.C. 113, Secretary of Defense: Title 10 establishes the Department of Defense as an executive department of the United States; The Secretary is the principal assistant to the President in all matters relating to the Department of Defense. Subject to the direction of the President and to this title, he has authority, direction, and control over the Department of Defense. Authorities d through h below are DOD authorities applicable to this collection.

b. 10 U.S.C. 5013, Secretary of the Navy. The Department of the Navy is separately organized under the Secretary of the Navy. The Department of the Navy operates under the authority, direction, and control of the Secretary of Defense. Subject to the authority, direction, and control of the Secretary of Defense and subject to the provisions of this title, the Secretary of the Navy is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Navy. Authority l below is a DON authority applicable to this collection.

c. 10 U.S.C. 5041, Headquarters, Marine Corps. Establishes a Headquarters, Marine Corps as the executive part of the Department of the Navy. The function of the Headquarters, Marine Corps, is to assist the Secretary of the Navy in carrying out his responsibilities. Except as otherwise specifically prescribed by law, the Headquarters, Marine Corps, shall be organized in such manner, and its members

shall perform such duties and have such titles, as the Secretary may prescribe. Authority k below is a USMC authority applicable to this collection.

d. In accordance with Public Law 110-181 Section 1089, the Office of the Undersecretary of Defense, Intelligence OUSD(I&S) developed and implemented Directive Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control mandated that Department of Defense DOD Physical Access Control Systems must support a DOD-wide and federally interoperable access control capability that can authenticate United States government physical access credentials and support access enrollment, authorization processes, and securely share information. The NACS and BAACS have been developed to support the DOD Defense Installation Access Control (DIAC) Identity Matching Engine for Security and Analysis (IMESA) that specify identity management web services that enable a conduit for information exchange between external authoritative databases and DON Physical Access Control Systems at the regional and installation levels.

e. OUSDI Directive-Type Memorandum (DTM) 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files establishes DoD policy for accessing Federal Bureau of Investigation (FBI) NCIC files through IMESA, provides for the use of NCIC information retrieved through IMESA for controlling entry to DoD installations and maintaining law and order on DoD installations; and provides for the use of NCIC information retrieved for crime prevention.

f. DOD Directive 1000.25, “DOD Personnel Identity Protection (PIP) Program,” July 2004, establishes policy for the implementation and operation of the PIP Program, to include use of DOD identity credentials and operation of DOD Physical Access Control Systems (PACS) that are used by DOD joint Services. The DON utilizes the NACS and the U.S. Marine Corps BAACS as its standard PACS systems at every U.S. Navy (USN) and U.S. Marine Corps (USMC) installation respectfully worldwide. NACS and BAACS are fully configurable force protection system that support physical access control mission. The DON is seeking authorization to issue identity credentials to those individuals needing physical access who are not otherwise credentialed under DOD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997. These credentials take the form of a Department of the Navy Local Population ID Card/Base Access Pass which is used as an installation pass only. It is important to note that Department of the Navy Local Population ID Card/Base Access Pass are issued only to those individuals who are not eligible for a CAC which is the DOD’s Personal Identity Verification (PIV) compliant credential, a DD Form 2, or a DD Form 1173 Uniformed Services Identification and Privilege card.

g. DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) Meet the requirements of references (d),(i), and Office of Management and Budget Memorandum 06-18 (reference (k)). Card

readers must be able to read and use the contactless-chip as prescribed in the National Information Security Technology (NIST) Special Publication (SP) 800-96 (reference (l)) and perform PIV card, certificates, and cardholder validation, and have the ability to provide rapid electronic authentication in accordance with references (d), (h), and (i) to federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System.

h. DoD 5200.08-R, Physical Security Program implements the policies and minimum standards for the physical security of DoD installations and resources, and implements general procedures that meet minimum Federal standards for controlling entry onto and exiting from military installations and the facilities within military installations. Access control is an integral and interoperable part of DoD installation physical security programs. Each installation commander/facility director must clearly define, consistent with DoD policy, the access control measures (tailored to local conditions) required to safeguard personnel, facilities, protect capabilities, and accomplish the mission.

i. DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos). The DON security personnel responsible for the physical access control mission at installation entry control points must have information concerning Persons and Organizations not affiliated with the DOD. The possession of a DOD or other credential, to include a Homeland Security Presidential Directive-12 PIV credential, is not sufficient alone to warrant authorizing entry. There are rules surrounding entry to access areas, to include days and times and under which force protection conditions an individual may enter an installation. The NACS and BAACS were developed for the collection and maintenance of this access authorization information, and for providing it to authorized DON security personnel and systems for decision-making purposes. The NACS and BAACS provide the capability to support tiered access control based on force protection condition and access control rules and capabilities across DON installations and/or regions.

j. E.O 9397 (SSN) Orders that the Social Security Board shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an account or the name and other identifying data pertaining to any account number of any such person. The SSN will be collected and used to determine the respondent's identity, and to perform a background check to determine the respondent's fitness to access a DOD installation.

k. Marine Corps Order 5530.14 Marine Corps Physical Security Program Manual prescribes policy, assigns responsibilities, and presents requirements that include the minimum security measures required for Level One, Level Two and

Level Three Restricted Areas, and specifies personal identification and access control systems to manage and control access of individual's (military, civil service, contractors, and official visitors) who require entry for reasons of official business, and render a service (vendors, delivery people).

l. OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program identifies the baseline security requirements for shore installations based on Required Operational Capability (ROC) and specifies personal identification and access control systems to manage and control access of Level One, Level Two and Level Three Restricted Areas.

2. Use of the Information

The respondents include non-DOD affiliated personnel requesting temporary or recurring, unescorted physical access to an installation (i.e., visitors, vendors, guests, non-DOD family members, or for DOD contractor personnel for less than six months).

The information collection is required to control physical access to DOD, DON or U.S. Marine Corps installations/units controlled information, installations, facilities, or areas over which the DOD, DON or U.S. Marine Corps has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./Coalition/allied government/ national security areas of responsibility and information; to issue badges, replace lost badges and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit of personnel.

Because this collection is being performed at over one hundred locations world-wide across the entire Navy and US Marine Corps Enterprise, the local installation commander is individually responsible for the registration process for his/her base including the vetting process for each registration, and thus, possesses the authority to introduce random access measures that alter or increase the frequency of the information collection based on security threat levels within the commanding officer's jurisdiction. Individual work flow and processes may differ. The general process follows: The respondents appear in person at the Navy or USMC Marine Corps Base Pass Office or Security Office. Bases typically have a signs posted at the base perimeter entry control points that guide the respondents to the Base Pass Office or Security Office. Additionally, respondents may be greeted by base security sentries posted at the base perimeter entry control points that provide verbal direction to the respondent.

The respondents enter the Base Pass Office or Security Office and are greeted by the Base's DON/USMC registrar who furnishes the SECNAV 5512/1 form to the respondent and instructs the respondent to complete the form by following the instructions that are included in page 3 of the form. When the form is complete, they return it to the registrar as to continue the registration process.

Respondents who provide their personal identifiable information are consenting to collection of information by their action of voluntarily offering their identity proofing documents, or fingerprints, irises, and facial profiles for biometric collection. Failure to provide requested information may result in denial of access to DOD installations, facilities, and buildings.

The respondent records their personal identifiable information on the SECNAV 5512/1 Department of the Navy Local Population ID Card/Base Access Pass Registration Form, and submits it to the DON/USMC registrar who verifies the information against list of acceptable Identity proofing documents listed on page 3 of the SECNAV 5512/1. The respondent only sees and completes the 5512/1 form. Respondents are not authorized to view the NACS or BAACS screens or enter any information in NACS or BAACS. Only the registrar enters the respondent's registration data into the NACS or the BAACS, which respectively serve as the registering Installation's/Base's Physical Access Control System where the data is stored for local physical access control requirements. Upon entry, this information is also securely transmitted and stored within the Department of Defense's authoritative data source (Identity Matching Engine for Security and Analysis (IMESA). The data is used to perform back ground checks to determine the fitness of non-DOD persons who are requesting access to DOD, DON or U.S. Marine Corps military installations. If a background check results in a finding that the respondent has not met the minimum criteria to determine fitness to access the base (that is listed on bottom of page 2 of the form), the DON/USMC registrar verbally conveys the determination of not fit to access the base to the respondent. If a background check results in a finding that the respondent is fit to access the base, the DON/USMC registrar will issue a Local Population ID Card or Base Access Pass to the respondent. Local Pop is printed on a PVC access card and a base pass is printed on paper.

Because the local installation policy may vary regarding requirements for the respondent to return the Local Population ID Card or Base Access Pass to the USN/USMC registrar after the respondent has completed their visit to the base, the USN/USMC registrar verbally communicates the local return policy at the time of issuance.

3. Use of Information Technology

The respondents complete the SECNAV 5512/1 paper form since they are not authorized to access DOD IT systems or networks, and therefore, electronic submission by the respondent is not a current option. Therefore, zero responses are collected electronically.

4. Non-duplication

NACS and BAACS are currently being used in CONUS and OCONUS for both installation level and facility level Physical Access Control. The significance of this is that each DON/USMC local installation commander is individually responsible for the registration process for his/her base including the vetting process for each registration.

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

5. Burden on Small Businesses

This information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

6. Less Frequent Collection

Collection is based on the respondent's need to access a DON installation. If the collection is not conducted or conducted less frequently, the DON would not have viable physical security measures to identify, control, and account for non-DOD personnel requiring temporary or recurring, unescorted physical access to an installation, nor the ability to register or screen to determine the fitness of the individual to enter an installation. Without the information collection, the DON cannot issue a Department of the Navy Local Population ID Card/Base Access Pass to eligible recipients who are seeking access to DON installations and facilities. The risk that the Department's overall security posture could be compromised would significantly increase. Additionally, without the capability to produce a Department of the Navy Local Population ID Card/Base Access Pass, disparate ID cards or base passes would proliferate, resulting in an additional burden for DON security offices such as life-cycle procurement, implementation, sustainment and training costs associated with disparate solutions.

7. Paperwork Reduction Act Guidelines

This collection of information does not require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice for the collection published on Wednesday, December 2, 2020. The 60-Day FRN citation is 85 FRN 77455.

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

A 30-Day Federal Register Notice for the collection published on Monday, March 1, 2021. The 60-Day FRN citation is 86 FRN 11959 .

Part B: CONSULTATION

No additional consultation apart from soliciting public comments through the 60-Day Federal Register Noticed was conducted for this submission.

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

A Privacy Act Statement (PAS) is provided at the top of the SECNAV 5512/1 form.

A System of Record Notice (SORN) is required. SORN DMDC 16, Identity Management Engine for Security and Analysis (IMESA); https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570757/dmdc-16-dod/.

SORN NM05512-2, Badge and Access Control System Records is also required. A copy of SORN NM05512-2 been provided with this package for OMB's review.

A Privacy Impact Assessment is required. A draft copy of the BAACS and NACS PIA has been provided with this package for OMB's review.

Records Retention and Disposition for SORN NM05512-2:
Badges and passes are destroyed three months after return to issuing office. Records of issuance are destroyed six months after new accountability system is established or one year after final disposition of each issuance record is entered in retention log or similar record, whichever is earlier. Visit request records are destroyed two years after final entry or two years after date of document, whichever is later. Collection forms, paper and/or plastic badges/passes are shredded or incinerated using DOD approved procedures. If any IT system or data storage media fails and must be replaced, the data storage component (e.g., disks/hard drives) is removed from the hardware and degaussed with DOD approved degaussing systems and are then mechanically shredded prior to disposal.

Records Retention and Disposition for SORN DMDC 16:
Records will be destroyed five (5) years after no access by all DoD Physical Access Control Systems (PACS) associated to that individual OR after all PACS have submitted a de-registration request for the individual.

11. Sensitive Questions

Social Security Numbers (SSN) are collected. The data collected as part of the enrollment into the NACS and BAACS is the basis for the Local Installation Commander making a decision to grant or deny access to his/her installation. An SSN Justification Memo has been provided with this package for OMB's review

12. Respondent Burden and its Labor Costs

Part A: Estimation of Respondent Burden

1) SECNAV 5512/1 form
   a) Number of Respondents: 4,900,000
   b) Number of Responses Per Respondent: 1
   c) Number of Total Annual Responses: 4,900,000
   d) Response Time: 10 minutes
   e) Respondent Burden Hours: 816,667

2) Total Submission Burden
   a) Total Number of Respondents: 4,900,000
   b) Total Number of Annual Responses: 4,900,000
   c) Total Respondent Burden Hours: 816,667

Part B: Labor Cost of Respondent Burden

1) SECNAV 5512/1 form
   a) Number of Total Annual Responses: 4,900,000
   b) Response Time: 10 minutes
   c) Respondent Hourly Wage: $27.20
   d) Labor Burden per Response: $4.53
   e) Total Labor Burden: $22,213,333

2) Overall Labor Burden
   a) Total Number of Annual Responses: 4,900,000
   b) Total Labor Burden: $22,213,333

The Respondent hourly wage was determined by using the Department of Labor Wage Website by using the 2020 average volunteer hourly rate of $27.20 per hour, according to Independent Sector; https://independentsector.org/value-of-volunteer-time-2020/.

13. Respondent Costs Other Than Burden Hour Costs

There are no annualized costs to respondents to complete this collection other than the labor burden costs addressed in Section 12 of this document.

14. Cost to the Federal Government

Part A: Labor Cost to the Federal Government

1) NACS / BAACS
   a) Number of Total Annual Responses: 4,900,000
   b) Processing Time per Response: 10 minutes
   c) Hourly Wage of Worker(s) Processing Responses: $32.02
   d) Cost to Process Each Response: varies: $5.44
   e) Total Cost to Process Responses: $26,672,660.00

2) Overall Labor Burden to Federal Government
   a) Total Number of Annual Responses: 4,900,000
   b) Total Labor Burden:$26,672,660.00

The hourly wage of worker was determined by using the Department of Labor Wage site GS pay schedule,, Grade 12, step 1: https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2021/GS_h.pdf.

Part B: Operational and Maintenance Costs

1) Cost Categories
   a) Equipment: $497,800
   b) Printing: $696,920
   c) Postage: $0
   d) Software Purchases: $298,680
   e) Licensing Costs: $497,800
   f) Other: $697,051

2) Total Operational and Maintenance Costs: $2,688,251

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government:$ 26.672,660.00

2) Total Operational and Maintenance Costs: $2,688,251

3) Total Cost to the Federal Government: $29,360,911.00

15. Reasons for Change in Burden

The respondent labor burden and the cost to the federal government has increased since the previous approval. This is due to re-evaluating the wages of the respondent and the government workers processing the requests.

16. Publication of Results

The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

We are not seeking approval to omit the display of the expiration date of the OMB approval on the collection instrument.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

We are not requesting any exemptions to the provisions stated in 5 CFR 1320.9.