SUPPORTING STATEMENT – PART A

NAVY ENABLER FRAMEWORK
(INCLUDES Navy Access Control Management System (NACMS)
And the U.S. Marine Corps Biometric and Automated Access Control System (BAACS)

A. JUSTIFICATION

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 a public information collection for the Information Technology (IT) collection system, Navy Enabler Framework, which includes the Navy Access Control Management System (NACMS) and the U.S. Marine Corps Biometric and 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; OMB Control Number 0703-TBD.

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. The Office of the Undersecretary of Defense, Intelligence OUSD(I) Directive Type Memorandum (DTM) 09-012 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 Enabler Framework including NACMS and and BAACS have been developed to support the DOD Defense Installation Access Control (DIAC) Identity Management Enterprise Services Architecture and fully supports the DIAC Interface Control Document Standards 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.

b. Section 1069 of Public Law 110-181, specifies standards required for entry to military installations in United States and tasks the Secretary of Defense (SECDEF) to develop access standards applicable to all military installations in the United States. The standards shall require screening standards appropriate to the type of installation involved, the security level, category of individuals authorized to visit the installation, and level of access to be granted including (A) protocols to determine

the fitness of the individual to enter an installation; and (B) standards and methods for verifying the identity of the individual The Enabler Framework including NACMS and Enabler Framework including NACMS and BAACS has been developed to support continuous vetting of individuals against authoritative data sources established and operated by the DOD, to determine the fitness of individuals .

c. 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 Navy Enabler Framework, which includes the NACMS 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. The Enabler Framework including NACMS 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.

d. Directive-Type Memorandum (DTM) 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance," December 1, 2008, updates the requirements for CAC eligibility. Specific populations are automatically eligible for a CAC based on their personnel category within the DOD. Examples include uniformed service personnel, DOD civilian employees, and specific categories of personnel assigned overseas in support of the Department. CAC eligibility for other populations, including DOD contractors, non-DOD federal civilians, state employees, and other non-DOD affiliates, is based on the DOD government sponsor's determination of the type and frequency of access required to DOD facilities or networks that will effectively support the mission. To be eligible for a CAC, the access requirement must meet one of the following criteria:

    i. The individual requires access to multiple DOD facilities or access to multiple non-DOD Federal facilities on behalf of the Department

on a recurring basis for a period of six months or more (this requirement is applicable to DOD contractors only).

ii. The individual requires both access to a DOD facility and access to DOD networks on site or remotely.

iii. The individual requires remote access to DOD networks that use only the CAC logon for user authentication.

These criteria are consistent with the August 2005 OMB Memorandum M-05-24 that directs credentialing standards generally apply to such categories unless they are short-term employees (less than six months), in which case the agency has discretion based on risk and other factors. The OMB guidance states that the application of the vetting and credentialing rules for contractors apply to "individual under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to which you would issue federal agency identity credentials, consistent with your existing security policies." The OMB guidance as written permits an agency to elect between either or both ("and/or") types of access as a prerequisite to sponsoring the issuance of DOD CAC to a contractor. This policy imposes greater security standards for DOD CAC issuance and thus enhances the safety of personnel and property on DON bases and installations. The policy is consistent with OMB's guidance that agencies issue credential's "consistent" with your existing security policies." Accordingly, contractors who do not require logical access are not eligible for Navy/USMC sponsorship to receive a DOD CAC. The Enabler Framework including NACMS and BAACS provides a secure and efficient means for non-DOD affiliated personnel requiring temporary or recurring unescorted physical access to an installation (i.e., visitors, vendors, guests, non-DOD family members or for DOD contractor personnel) to obtain a Department of the Navy Local Population ID Card/Base Access Pass and meets a bona-fide need that is not fulfilled by the HSPD-12 PIV credential policy or OMB Guidance.

e. DON security personnel responsible for the physical access control mission at installation entry control points must have information with which to identify authorized individuals. 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 Enabler Framework including NACMS and BAACS was 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 Enabler Framework including NACMS and BAACS provides the capability to support tiered access control based on force protection condition and access control rules and capabilities across DON installations and/or regions.

2. Use of the Information

The information collection requirement is necessary 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.

The respondents include non-DOD affiliated personnel requiring 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).

3. Use of Information Technology

Respondents are non-DOD members of the general public, businesses or other for profit and not-for-profit institutions who are seeking to access DOD, DON or U.S. Marine Corps installations/bases, facilities, or areas over which the DOD, DON or Marine Corps has security responsibilities. The respondents appear in person, record their personal identifiable information on the SECNAV 5512/1 Department of the Navy Local Population ID Card/Base Access Pass Registration Form, and submit it to the DON/USMC registrar who verifies the information against required I-9 Identity proofing documents. The registrar then enters the respondent's registration data into the Navy's Access Control Management System (NACMS) or the USMC's Biometric and Automated Access Control System (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 (Local Population Database). 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. Upon successful registration and background check, either a Local Population ID Card or Base Access Pass is issued to the respondent. Respondents who provide their personal identifiable information are consenting to collection of information by their action of voluntarily offering their I-9 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.

Enabler Framework including NACMS and BAACS is a centralized, rules-based access control and identity management system that:

- Supports the DoN physical security, force protection, identity management and access control missions by identifying and/or verifying an individual through the use of a database for designated populations for purposes of protecting U.S./Coalition/allied government/national security areas of responsibility and information.

- Provides personnel identification and verification capabilities during disaster scenarios or other catastrophic events.
- As a force protection program to protect DON assets, personnel, and physical property, and installation access, it detects fraudulent identification cards and security alerts in the form of Debarment, Suspension, Revocation, Be-on Lookout, or National Crime Information Center Wants/Warrants for individual persons.

The Enabler Framework including NACMS and BAACS is Federal Information Processing Standard (FIPS) -201 compliant. It is a networked client/server database system designed to easily verify the access authorization and fitness of personnel entering military installations and fully supports and reads HSPD-12 PIV credentials, barcode technology, photograph, and fingerprint biometric identification. FIPS-210 approved card readers verify captured data internally against the Enabler Framework including NACMS and BAACS database and externally against authoritative data sources such as the Defense Enrollment Eligibility Reporting System (DEERS) and/or the DOD Interoperability Layer Services (IoLS). It also is fully compatible with commercial off-the-shelf physical pccess control software packages.

The Enabler Framework including NACMS and BAACS system supports the DOD DIAC Interface Control Document Standard for web services required to perform all of the following tasks without requiring further customization or development:

- Fixed and Mobile Registration. The Registration workstation enables a Registrar to enter a person's information into the database either by:
  - Scanning a CAC which is the DOD's Personal Identity Verification (PIV) compliant credential
  - Scanning a DD Form 2, or a DD Form 1173 Uniformed Services Identification and Privilege card
  - Scanning a DON Local Population Identification Card/Base Access Pass
  - Or by manually typing information into data field boxes and the printing/creation of the Department of the Navy Local Population ID Card/Base Access Pass (installation passes).

  Registration supports validation by authorized personnel or sponsors to log their approval for pending registrations that require sponsorship. The system allows authorized Base Security officials to flag individual registration records with Security Alerts in the form of Debarment, Suspension, Revocation, Be-on Lookout, or National Crime Information Center Wants/Warrants. The mobile registration station provides flexibility by allowing the station to be moved from location to location to minimize impact to base and force operational capability.
- Entry Control Point. Fixed card readers and/or mobile hand-held card readers may be used for credential authentication at Entry Control Points to authenticate persons entering the installation or facilities. Entry Control Point workstations may be co-located at manned Entry Control Points to augment the monitor and display of physical access activity.

4. Non-duplication

There is no known information collection which duplicates this effort. Due to the sensitivity and statutory restrictions on recording and disclosure of some law enforcement data, that information is retained in separate authoritative law enforcement systems, such as National Crime Information Center (NCIC) or the DOD Criminal Justice Information Systems. Enabler Framework only stores a unique identifier reference record that is used by Base Security Officials to perform external criminal justice system record checks within the separate authoritative law enforcement system(s), therefore, the law enforcement data is not redundant in Enabler.

CAC, DD Form 2 and DD Form 1173 identification cards are produced through the DEERS Real Time Automated Personnel and Identification System (RAPIDS). DEERS RAPIDs and Enabler complement one another in that the credentials issued by RAPIDS can be registered into the Enabler Framework, then scanned and authenticated for physical access into an installation. The systems serve very different purposes, have different users and are physically located at different places on an installation. The architectures are radically different and would require significant effort and funding to develop the capability to accommodate the differing purposes and connection requirements. DEERS is the DOD repository for all individuals who are or have been either directly employed by the DOD or who are entitled to DOD benefits, and is the authoritative data source for identity of those personnel. RAPIDS interfaces directly with the DEERS for the sole purpose of creating or updating DOD personnel information or verifying benefits. There is a single connection between a RAPIDS station and DEERS. Enabler Framework including NACMS and BAACS is a database containing information used for physical access permissions, which has multiple connections to each site's registration workstation(s), security office(s), and entry control point(s) to support numerous interactions of many types.

DEERS RAPIDS is funded centrally; Enabler Framework including NACMS and BAACS is a combination of centrally funded and customer-purchased and funded. The significance of this is that each DON/USMC local installation commander is individually responsible for his/her base's records and access permissions. In DEERS, the responsibility for the accuracy and quality of the records forwarded for inclusion in the database is held at the Service level. A key feature of the Enabler Framework including NACMS and BAACS system is the ability to catch lost or stolen cards, and to ensure that personnel entering a site have permission to access the site. As previously stated, possession of a credential, whether PIV or not, does not in and of itself allow an individual access to a base. Enabler Framework including NACMS and BAACS provides a significant capability to ensure that only the right people enter a site, positively affecting the force protection posture. Enabler Framework including NACMS and BAACS is currently being used in CONUS and OCONUS; and these DOD installations rely on it for installation Physical Access Control. Similarly, RAPIDS is the repository for data supporting benefits and privileges eligibility for the DOD enterprise. Both systems have critical mission-specific purposes that are complementary. However, merging the two systems is not practical or feasible.

It is important to note that for any respondent that undergoes the information collection process, that their information will be retained in the system for a period of time authorized by the Systems of Records Notice. If their DON/USMC Local Population ID Card/Base Access Pass expires, the record retention date has not been reached and the individual returns to seek further access, the registration renewal process will leverage their information retained in the system and the burden per renewal response will be less (i.e. the person will be processed more expeditiously).

5. Burden on Small Business

Collection of this information does not involve small businesses or small entities. If individual respondents are employed by a small business, they are subject to the same access screening standards specified by the DON local installation commander regardless of their race, gender or affiliation.

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

Special circumstances that would require respondents to report information to the agency more often than quarterly include:

a. If the DOD or DON as a whole or if an individual DON installation elevated or heightened their force protection conditions, regardless of the reason, the local installation commander may introduce random access measures that alter or increase the frequency of the information collection. An example would be if a breach in security occurred as a result of a counterfeit DON Local Population ID Card/Base Pass, then the local commanding officer may issue orders to revoke issued cards and require re-issuance.

b. The local commanding officer has discretion over specifying the period of validity for any Local Population ID Cards/Base Access Passes that are issued under his/her jurisdiction.

There are no special circumstances that would require respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it.

There are no special circumstances that would require respondents to submit more than an original and two copies of an individual document.

There are no special circumstances that would require respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records, for more than three years.

There are no special circumstances in connection with a statistical survey that is not designed to produce valid and reliable results that can be generalized to the universe of study.

There are no special circumstances requiring the use of a statistical data classification that has not been reviewed and approved by the Office of Management and Budget.

There are no special circumstances that includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or requiring respondents to submit proprietary trade secrets, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

8. Consultation and Public Comments

a. An agency 60-day Federal Register Notice was published in Volume 78 FR 59344, Pages 59344 -59345, on September 26, 2013. No public comments were received. A 30-day Federal Register Notice was published in Volume 79 FR 11424 on February 28, 2014. This is currently still open for comment.

b. No consultations with persons outside the sponsoring agency regarding availability of requested information, frequency of collection, clarity of instructions, etc., were performed. Future consultation with respondents, or their representatives, are planned to be performed at least every 3 years, regardless if the information collection does not change.

9. Gifts or Payment

No payments will be made to respondents for this information collection.

10. Confidentiality

This information collection does not ask the respondent to submit proprietary, trade secret, or confidential information to the DOD or DON. The SECNAV 5512/1 Department of the Navy

Local Population ID Card/Base Access Pass Registration Form is stamped For Official Use Only (FOUO). The respondent's personal identifiable information that they record on the SECNAV 5512/1 form and that the DON registrar enters into the system will be protected per the Privacy Act of 1974 (Public Law 93-579). Respondents are asked to read a Privacy Act Statement prior to providing the requested information. A System of Records Notice (SORN NM05512-2 *Badge and Access Control System Records* Federal Register /Vol. 75, No. 87 /Thursday, May 6, 2010 /Notices; http://dpclo.defense.gov/privacy/SORNs/component/navy/NM05512-2.html) is established for this collection. A DOD Privacy Impact Assessment has been completed and approved. The following are links to the PIAs.

These protection measures safeguard the access to Enabler Framework including NACMS and BAACS to authorized users only.

11. Sensitive Questions

This information collection does not include any questions such as sexual behavior and attitudes, religious beliefs, or other matters that are commonly considered private. For identity verification purposes, the following information is being requested:

- Gender – The gender of the individual is requested for demographic and identity proofing purposes only. Gender is not a factor in determination of access eligibility.

- Social Security Number (SSN) – The data collected as part of the enrollment into the Enabler Framework including NACMS and BAACS solution is the basis for the Local Installation Commander making a decision to grant or deny access to his/her installation. This access control decision will include the completion of a query of the NCIC database as a separate process external to Enabler Framework. This query is completed based on submittal of the First and Last Name, Date of Birth and SSN as primary query fields.

OMB has required that every Federal Agency develop and implement a plan to reduce the unnecessary use of the SSN. To meet this requirement, DOD issued Directive Type Memorandum (DTM) 07-015 which focuses on reducing SSN use in DOD. This DTM mandates that SSNs should not be used in DOD unless there is a specific legal/legislative requirement for using the SSN. Also, the SSN Reduction Plan provides for a comprehensive review of new and existing DOD forms and systems where SSNs are currently used or proposed. To comply with DOD policy, the Department of the Navy has submitted Memorandums signed/approved by U.S. Navy and U.S. Marine Corps Flag/SES level authority to OMB that contains the justification for use of the SSN.

12. Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden

The burden estimate was determined as follows:

Step 1: Combined the total number of U.S. Navy and U.S. Marine Corps bases to get 131 bases;
Step 2: Estimate the number of days per year that a given base will support registration (365 minus 102 weekend days minus 10 holidays);
Step 3: Estimate the average number of daily respondents per base. Note that the daily average factors in special events, such as change of command ceremonies, graduation ceremonies, large conferences, deployments, deployment returns, and air shows/fleet week;
Step 4: Calculate the Total Annual Respondents by multiplying the total number of bases by the estimated number of days per year by the average number of daily respondents per base. Round up to the nearest hundred thousand;

Total number of bases	131
Estimated number of days per year when registration is supported	253
Average number of daily respondents per base	147
Total Average Annual Respondents	4,900,000
Estimate 25% of respondents will be repeat visitors who renew their registration	1,225,000

The collection consists of more than a single instrument of collection; i.e., a paper form and an electronic record. The burden estimates for each instrument, an aggregated total burden was determined as follows:

Step 1: Estimate the percentage of responses collected electronically;
Step 2: Estimate the percentage of responses collected on paper form;
Step 3: Estimate the average burden per electronic response. Burden was estimated by observation of less than ten respondents;
Step 4: Estimate the average burden per paper form response. Burden was estimated by observation of less than ten respondents;
Step 5: Add the estimates of average burden per electronic response and the average burden per paper form response to get the aggregate average burden per response;
Step 6: Calculate the Total Annual Hours Requested by multiplying the Number of Respondents by the Aggregate Average burden per response and divide that by 60 (minutes per hour)

Percentage of these responses collected on paper form	100%
Average burden per paper form response	5 minutes

Total Annual Hours requested	408,333
Current OMB Inventory	0
Difference	+408,333

b. Labor Cost of Respondent Burden

The following is an estimate of annualized cost to respondents of only the burden hours imposed by the collection. Capital, start-up, contracting out, or operations and maintenance costs are not included. Respondent costs other then burden hour costs are shown in Item 13 of the Supporting Statement.

Annualized Cost to Respondents				
Respondent Categories	% of Respondents	% of Total Respondents	Hourly Loaded Rate (+25%)[1]	Cost to Respondents
Non-paid	25%	1,225,000	$ 0	$ 0
Low Pay – Min. Wage $7.25	25%	1,225,000	$ 9.06	$ 11,098,500
Median Pay – All Occupations[2]	40%	1,960,000	$ 16.71	$ 32,751,600
Median Pay – General & Operations Managers[3]	10%	490,000	$ 45.88	$ 22,481,200

[1] An estimate of 25% as the cost of fringe benefits was taken from a review of two papers available from the U.S. Bureau of Labor Statistics website; 1) Report on the American Workforce, U.S. Department of Labor, Elaine L. Chao, Secretary, 2001, and, 2) "The Growth of fringe benefits: implications for social security" by Yung-Ping Chen."

[2] U.S. Department of Labor Bureau of Labor Statistics 2012 Median Hourly Wage for all Occupations

[3] U.S. Department of Labor Bureau of Labor Statistics 2012 Median Hourly Wage for General and Operations Managers

Totals	100%	4,900,000	–	$ 66,331,300

13. Respondent Costs Other Than Burden Hour Costs

a. Total Capital and Start-up Cost. The Respondents will not incur capital or start-up costs as a result of this information collection. Respondents will not incur costs to purchase equipment or services as a result of this information collection.

b. Operation and Maintenance Cost. Respondents will not incur operation and maintenance costs as a result of this information collection.

14. Cost to the Federal Government

The annualized costs incurred by the federal government in collecting and processing the information collected, and explanation of the methods used in determining these estimates follow:

The capital startup costs was determined as follows:

Step 1: Estimated the application hardware and software, licensing, configuration, database build-out, engineering design, installation, training, and overhead costs to be $273,353 per base or $35,809,248 for 131 bases.
Step 2: Because the entire capability will be fielded across all 131 bases over a five year period (5 year funding cycle), the estimated annualized cost of start-up in the first year is approximately $7,161,850 ($35,809,248 divided by 5). There would be a 3.5% escalation in this annualized cost for each additional year until fully deployed.

Capital Startup Cost to Federal Government			
Description	Cost per Base	Total Costs for all Bases	Annualized Cost in First Year
Application hardware and software, licensing, configuration, database build-out, engineering design, installation, training, and overhead costs	$273,353	$35,809,248	$7,161,850
Subtotal	$273,353	$35,809,248	$7,161,850

The O&M cost associated with equipment maintenance was determined as follows:

Step 1: Estimated the per base equipment cost to include all electronics hardware/systems/subsystems, software licensing and printing supplies to be $101,362.

Step 2: Estimated the equipment maintenance cost to be 15% of $101,362 or $15,204 per base or $1,991,757 for 131 bases;
Step 3: Estimated the Contracting Fees for Equipment Maintenance Services to be 10% of $15,204 or $1,520 per base or $199,176 for 131 bases;
Step 4: Estimated the Government Contracting Oversight/Management to be 25% of $15,204 or $3,801 per base or $497,939 for 131 bases;
Step 5: Estimated the subtotal O&M equipment maintenance cost to be $20,526 per base ($15,204 plus $1,520 plus $3,801) or $2,688,872 for 131 bases;
Step 6: Because the entire capability will be fielded across all 131 bases over a five year period (5 year funding cycle), the estimated annualized cost of O&M equipment maintenance in the first year is approximately $537,774 ($2,688,872 divided by 5). There would be a 3.5% escalation in this annualized O&M cost for each additional out year.

O&M Equipment Maintenance Cost to Federal Government

Description	Cost per Base	Total Costs for all Bases	Annualized Cost in First Year
Equipment Maintenance Cost (15% of $101,362)	$15,204	$1,991,763	$398,351
Contracting Fees for Equipment Maintenance Services (10% of $15,204)	$1,520	$199,176	$39,835
Government Contracting Oversight/Management (25% of $15,204)	$3,801	$497,939	$99,588
Subtotal	$20,526	$2,688,872	$537,774

The Operations and Maintenance (O&M) cost associated with manpower/labor (staff to collect, enter, process, produce cards/passes and maintain records) was determined as follows:

Step 1: Obtained the hourly base rate for a contracted Pass & ID/Registration Clerk from the U.S. Department of Labor Register of Wage Determinations for the District of Columbia (01113 - General Clerk III (2005-2103, Rev. 13, 06/19/2013 is $18.74 base pay per hour);
Step 2: Estimate the loaded per hour rate to be $23.43. Multiplied the base pay per hour ($18.74) by 25% to get the cost of Fringe Benefit of $4.69, and then added that to the base pay per hour;
Step 3: Estimate the number of hours worked per year per clerk to be 1920 hours per year. Estimate was based on a maximum of 2080 hours per year minus 80 hours for paid leave minus 80 hours for federal holidays;
Step 3: Estimate the Annual Full Time Equivalent cost for single clerk to be $44,976 per year;
Step 4: Estimate the percentage of bases that require a single FTE clerk to be 30% of 131 bases or 39 bases. Estimate the percentage of bases that require two FTE clerks to be 50% of 131 bases or 66 bases. Estimate the percentage of bases that require three FTE clerks to be 20% of 131 bases or 26 bases;

Step 5: Estimate the Total Number of clerks required for all bases to be 249 clerks. Estimate was based on 1 clerk multiplied by 39 bases (39 clerks), plus 2 clerks multiplied by 66 bases (132 clerks), plus 3 clerks multiplied by 26 bases (78 clerks).
Step 6: Estimate the Total Labor Cost for all clerks/bases to be $11,199,024. Estimate was based on the Annual Full Time Equivalent cost for single clerk to be $44,976 per year multiplied by 249 clerks;
Step 7: Estimated the cost to contract out manpower/labor services to be 10% of $11,199,024 or $1,119,902 for 131 bases;
Step 8: Estimated the Government Contracting Oversight/Management to be 25% of $11,199,024 or $2,799,756 for 131 bases;
Step 9: Estimated the subtotal O&M Manpower/Labor Cost to be $15,118,682 for 131 bases;
Step 10: Because the entire capability will be fielded across all 131 bases over a five year period (5 year funding cycle), the estimated annualized cost of O&M Manpower in the first year is approximately $3,023,736 ($15,118,682 divided by 5). There would be a 3.5% escalation in this annualized O&M cost for each additional out year.
Note Assumes existing base Security Office DOD civilian or military personnel will oversee day-to-day management of Pass & Identification clerks, so no labor cost for clerk management is included.

O&M Manpower/Labor Cost to Federal Government			
Wage Determination Category Code 01113 - General Clerk III (2005-2103, Rev. 13, 06/19/2013 base hourly rate)	1920	$18.74	$35,981
Fringe Benefit Load @ 25%	1920	$4.69	$8,995
Subtotal Loaded per hour rate and Annual FTE cost for a single clerk		$23.43	$44,976
Number of bases/clerks:			
30% of 131 bases require one FTE clerk	39	1	39
50% of 131 bases require two FTE clerks	66	2	132
20% of 131 bases require three FTE clerks	26	3	78
Subtotal number of clerks required for all bases			249
Subtotal labor Cost for all clerks/bases			$11,199,024
Contracting Fees for Pass & ID Clerk Services (10% of $11,199,024)			$1,119,902
Government Contracting Oversight/Management (25% of $11,199,024)			$2,799,756
Subtotal O&M Manpower/Labor Cost (for 131 bases)			$15,118,682
Subtotal O&M Manpower/Labor Cost per year (annualized cost per year over five years)			$3,023,736

ANNUALIZED COST TO GOVERNMENT

Cost Description	Cost per Base	Total Costs for all Bases	Annualized Cost in First Year
Subtotal Capital/startup Costs	$273,353	$35,809,248	$7,161,850
O&M Equipment Maintenance Costs	$20,526	$2,688,872	$537,774
O&M Manpower/Labor Costs	varies	$15,118,682	$3,023,736
Subtotal O&M Annual Costs	varies	$17,807,554	$3,561,511
Total Costs	varies	$53,616,802	$10,723,360

15. Reasons for Change in Burden

This is an initial request for OMB Control Number. There is no decrease in burden at this time.

16. Publication of Results

The results of collection of this information will not be published for statistical use outside of the DOD. On occasion, the DON may report statistics to the DON program office. An example would be daily, weekly or monthly total respondents processed by base/installation presented in tabular format in a presentation.

17. Non-Display of OMB Expiration Date

There are no requests to omit display of the expiration date of OMB approval on the instrument of collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

There are no requests for exceptions to the certification statement.