Opportunity Analysis For Contactless and Biometric Enhancements for Physical Security

26 November 2003

DOCUMENT ACCEPTANCE

PREPARED BY: _____ DATE: 10/23/03
Richard W. Caldwell, CPP, DON eBusiness Operations Office, Commercial Partner

PREPARED BY: _____ DATE: 10/23/03
Larry Gale, SPAWAR Systems Center Charleston, Commercial Partner

ACCEPTED: _____ DATE: 10/23/03
Bonita Armstrong, DON eBusiness Operations Office, Director of Smartcard and CAC Group (Acting)

ACCEPTED: _____ DATE: 10/23/03
Larry Taylor, SPAWAR Systems Center Charleston, Biometrics Program Manager

*ACCEPTED: _____ DATE: 12/2/03
Col Shaevitz, US Pacific Command, Deputy Chief of Staff

* "The acceptance of this report by the USPACOM signatory does not constitute a commitment to any organization, including without limitation, federal or non-federal entities, contractually or otherwise, to a specific technology or course of action."

RECORD OF CHANGES

The following serves as a history of the change activity affecting this document:

Change Number	Date	Number Of Figure, Table Or Paragraph	A* M D	Title Or Brief Description
Draft 0.0		ALL	A	First draft
Draft 0.1	26 August 2003	Various	A/M /D	Detailed survey results added.
Draft 0.2	9 October 2003	Various	A/M /D	Final draft for comments
Final	21 November 2003	Various	A/M	Legal inclusions, J6 comments
Post-final	26 November 2003	Various	A/M	Additional comments

*__A__ - Added __M__ - Modified __D__ - Deleted

Table of Contents

1. Executive Summary 1
2. Project Description and Background 2
2.1. BUSINESS PROBLEM SATISFIED BY THE PILOT 2
2.2. PRIOR SYSTEM 3
2.3. DESCRIPTION OF PILOT SYSTEM 4
2.4. TECHNICAL ARCHITECTURE 7
2.4.1 Hardware Changes 8
2.4.2 Card Architecture 8
2.4.3 Enrollment Integration 9
2.4.4 Backend Application & Database 10
3. Project Goals, Objectives and Metrics 10
3.1. PROJECT GOALS AND OBJECTIVES 10
3.1.1. Dual Biometric Operational Test 10
3.1.2. Next-Generation CAC 10
3.2. PROJECT METRICS 11
3.2.1. User Acceptance 11
3.2.2. System Performance 11
3.2.3. Enhanced Security 11
3.3. ALIGNMENT OF PILOT AND ENTERPRISE GOALS 12
4. Analysis of Pilot Results 12
4.1. EVALUATION OF METRICS 12
4.1.1. User Acceptance 12
4.1.2. System Performance 13
4.1.3. Enhanced Security 14
4.2. QUALITATIVE ANALYSIS AND INTANGIBLE BENEFITS 15
4.3. PILOT COSTS 15
5. Pilot Lessons Learned 17
5.1. PROBLEMATIC POPULATION 17
5.2. PERSONNEL DATA 17
5.3. REVISITING BUSINESS PROCESSES 17
5.4. DISTRIBUTED ACCESS CONTROL 18
6. Future Opportunities and Next Steps 18
6.1. NECESSARY SYSTEM ENHANCEMENTS 18
6.2. ACTION PLAN FOR US PACOM 18
6.3. ENTERPRISE OPPORTUNITY 19
6.4. ENTERPRISE ACTION PLAN 19
6.4.1. Short-Term Actions 19
6.4.2. Long-Term Actions 19

List of Figures

FIGURE 1: EXISTING MAGNETIC STRIPE SYSTEM 3
FIGURE 2: PILOT FINGERPRINT AUTHENTICATION 6
FIGURE 3: PILOT HAND GEOMETRY AUTHENTICATION 7
FIGURE 4: PILOT TECHNICAL ARCHITECTURE 8
FIGURE 5: MIFARE CHIP DATA MAP 9
FIGURE 6: ESS SYSTEM REQUIREMENTS 10
FIGURE 7: GOAL ALIGNMENT TABLE 12

List of Appendices

APPENDIX A DETAILED BASIS FOR MEASUREMENT 21
APPENDIX B DETAILED USERS SURVEY RESULTS 28
APPENDIX C SYSTEM STATISTICS 41
APPENDIX D REFERENCES 45
APPENDIX E LIST OF ACRONYMS 46

1. Executive Summary

This report documents the results of an Opportunity Analysis (OA) performed utilizing a potential Common Access Card (CAC), Physical Access Control solution for U.S. Pacific Command (PACOM) pilot project conducted by the DON eBusiness Operations Office.

Department of Defense Directive 8190.3, dated 31 August 2003, clearly identifies the CAC as the primary token to be used in physical security. Extensive discussions, in various forums, have taken place between the physical security and CAC communities over how to best address this issue and whether additional technologies need to be added to the CAC. It has been the position of the DON eBusiness Office, the CAC needs a contactless capability and this technology must be integrated with biometrics to provide the much needed authentication piece that is missing from the majority of legacy systems currently in use. There are two challenges: to identify a contactless technology standard that can provide the critical interoperability with a broad variety of installed electronic security systems throughout DoD, and the costs associated with such a transition.

The Navy's Space and Naval Warfare Systems Center (SPAWARSYSCEN) Charleston demonstrated the use of contactless smart card technology in conjunction with multiple biometric modalities to enhance Access Control within the J6 spaces of PACOM. The operational demonstration was conducted as a pilot project under the joint sponsorship of the Department of Navy (DON) eBusiness Operations Office and SPAWAR Program Management Warfare (PMW) 161. During the pilot, SPAWARSYSCEN Charleston, with input and guidance from the DON eBusiness Operations Office, assessed and evaluated the contactless biometric technology in a range of security and identification environments. The software and hardware was installed within buildings 20 and 20E at PACOM.

The pilot was evaluated over a two-month period where user acceptance and system performance was analyzed. Out of the 300+ users, only two had difficulty enrolling biometrically and they were able to fully participate in the pilot. Users were generally pleased with the system with some mild concerns about the nature of how their biometric data was being used. Those concerns were resolved by explaining the biometric template resides on a contactless chip on the user's personal identification card and not in a database. Biometric awareness increased by 44% over the evaluation. Users were granted access 97% of the time with two or fewer attempts, aligning with their expectations. PACOM management was pleased with results of pilot and opted to continue maintaining portions of the access control system at the conclusion of the pilot. During the evaluation phase of the pilot, PACOM was in the process of articulating requirements for their new Headquarters building, the Nimitz-MacArthur Command Center, potentially looking at a contactless/biometric solution.

This pilot clearly demonstrated that biometrics on a Mifare embedded chip could meet most of the functional demands of the physical security community for door access control. This solution, if incorporated into the CAC, still does not address the color-coding, or similar method, that most commands require to visibly identify a person's clearance level/access for others to see. There are other contactless and biometric technologies maturing that should be evaluated. There are vulnerabilities that need to be investigated. The piloted solution advanced past the current capabilities of the CAC for physical security and is readily available. An action plan is included in this document (**SECTION 6.4**) that could assist the DoD Access Card Office in making a decision for the next-generation CAC.

2. Project Description and Background

2.1. Business Problem Satisfied by the Pilot

The DoD Common Access Card (CAC) was developed to address solutions to three business processes and are:

1. The standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel,
2. The principal token for logical access to DON computer networks and systems through PKI identity, e-mail, and encryption certificates, and
3. The principal card used to enable physical access to buildings and controlled spaces.

This pilot was designed in Spring 2003 to address concerns with the third business area. To date, the CAC supports multiple technologies for the physical access control community such as bar code, magnetic stripe and integrated smart chip. These technologies have not been adopted by commands currently issued CAC's for a number of reasons to include:

- The primary reason is a solution is not easily integrated with their legacy Electronic Security System (ESS). Commands who integrated the CAC into their ESS, for example using the magnetic stripe, quickly discovered that the repeated contact reduces the lifespan of the CAC and their card readers.

- Considering the cost differential between a CAC ($8.00-$10.00) and a common magnetic stripe card ($0.50), this was a cost deterrent.

- A third reason for not adopting the CAC into their ESS, was that it did not enhance the security in their access control CONOPS. Bar codes and magnetic stripes are widely used and are becoming easier to duplicate. Solutions with the integrated smart chip, though more secure, were only available if a PIN was used which adversely impacted throughput time.

- Another reason for not adopting the CAC into their ESS is the requirement for commands to have a visible indication of the person's clearance/access level. This issue has been and continues to be a significant concern to command security managers.

There exist a number of contactless technologies, which may be incorporated into a standard sized card. The contactless technologies would eliminate the requirement for direct contact between card and reader, thereby reducing the physical wear and tear imposed on the CAC and better accommodating the existing installed base across the DON. It was also decided that the use of biometrics could provide stronger user authentication. Since the CAC contains data storage areas, it is feasible to store a copy of an individual's biometric template for use in subsequent biometric verifications. A number of biometric product vendors have implemented products utilizing contactless card technology for the storage of biometric templates in just this manner.

The number of contactless standards presented another problem as to which one should be used. The industry leaders included a 125 KHz Proximity standard, and three 13.56 MHz

standards. The Proximity standard raised concerns about enterprise implementation in regards to a security feature commonly referred to as a facility code. ISO 14443 A and ISO 14443B were mature 13.56 MHz standards, though the short read range (less than 4 inches) could be a limitation in future security applications. ISO 15693 offered a 30 inch read range, but it was a newly adopted standard and was not readily available on the market coupled with biometrics. On 25 August 2003, NIST took a big step towards a government-wide standard by publishing the Government Smart Card; Interoperability Specification 2.1, which specifies that ISO 14443 part 1 through 4, is now the standard for contactless technology.

2.2. Prior System

PACOM utilized a magnetic card system, AMAG, to control access to their secured spaces. Some doors were secured using a physical lock and key.

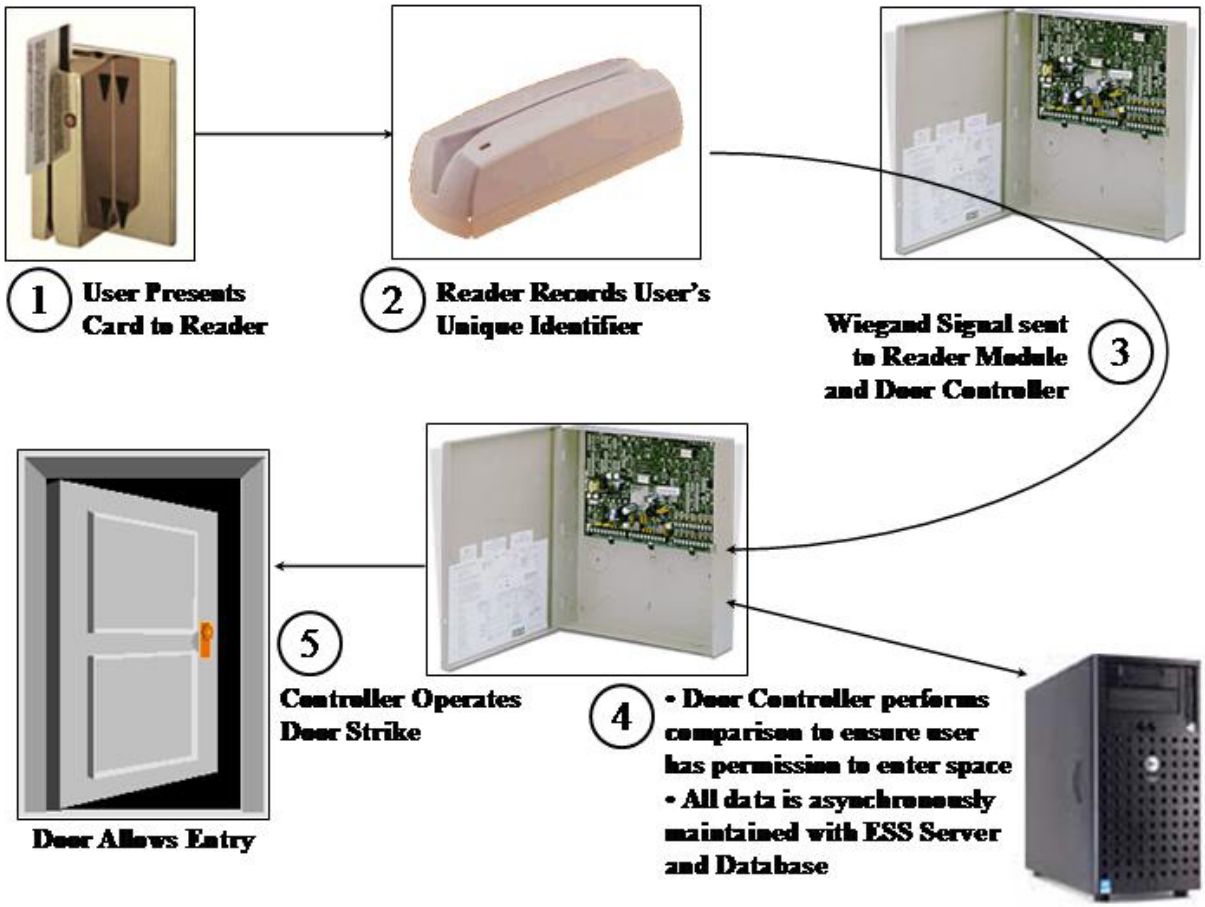


Figure 1: Existing Magnetic Stripe System

In the prior system, individuals were issued a magnetic card, which contained a unique identifier (Wiegand code). Users would swipe the magnetic card through the reader, which sent the encoded Wiegand string to the reader module and door controller. The door controller compared the received Wiegand string with the list of users authorized to access that door, and

if a match were found, the controller would then operate the door strike, allowing the door to be opened.

2.3. Description of Pilot System

PACOM was interested in exploring methods for increasing the security of their controlled spaces, particularly in light of the current construction of their new headquarters facility. Functional requirements for the pilot system were to provide biometric authentication of users attempting to access controlled spaces, and to utilize a contactless token for storage of the biometric templates.

SSC Charleston in conjunction with DON eBusiness CAC/Smart Card Group decided to address the authentication portion with both fingerprint and hand geometry biometrics. Hand geometry was selected exclusively for use at external doors, since the hand geometry reader units were available with a weather resistant enclosure, suitable for use in an outdoors setting. Fingerprint readers were used for the interior doors. The choice of a contactless technology was based upon prior experience, and utilized the Mifare (ISO 14443A) standard.

While the current CAC utilizes contact smart card technology, future iterations will probably also utilize a contactless technology as well. In the absence of a specification for the next generation CAC at the beginning of this project, and since modifications of the existing CAC card are not authorized, it was decided to utilize a separate, small contactless chip utilizing the Mifare standard for storage of both the finger and hand templates. A custom plastic sleeve was obtained which was used to hold the CAC, contactless chip, and a small color-coded tag with the users name, expiration date, and command affiliation. The tag was included in an attempt to mirror the command badge color for clearance/access visibility since the CAC does not have this feature. Mifare technology is supported by the selected fingerprint reader vendor (BioScrypt) and the hand geometry reader vendor (RSI). Some customization was required by those vendors in order to allow a single Mifare chip to contain both vendors' biometric templates.

All employees requiring access to the secured spaces (Bldgs. 20 and 20E) were identified by the command, including military, government civilians, and contractor personnel. Users who did not already have a CAC were issued a CAC prior to commencement of the pilot. The command provided SSC Charleston personnel with a list of users and associated information prior to the pilot commencement in order to allow pre-printing of the color-coded tags with appropriate markings. Users whose data was not available prior to commencement were issued color-coded tags during the pilot enrollment period.

The Electronic Security System (ESS), which provides the backend functionality of mapping user identity to physical access privileges, was the Lenel On Guard system. Users were entered into the Lenel system database, and issued the contactless chip associated with their user identity. Access rights for that individual were setup via the Lenel software as indicated by PACOM systems administrators.

Once users were enrolled in the backend Lenel ESS, they were enrolled biometrically, using both fingerprint and hand geometry biometrics at the enrollment station. The biometric enrollments utilized the software from the respective biometric vendors (BioScrypt and RSI).

Both biometric templates were written to the user's contactless chip.

The following figure illustrates the steps required for a user to obtain access to a controlled space utilizing the pilot system.

1. The user attempting to gain access to the controlled space holds the contactless chip in the vicinity of the contactless reader.
2. The contactless reader reads the user's unique identifier (as a Wiegand string) and the user's enrolled biometric template from the contactless chip.
3. The user presents the appropriate biometric feature (i.e., the previously enrolled finger or hand) to the biometric reader.
4. The biometric reader compares the live scan biometric feature with the template retrieved from the contactless chip. If the two match at the appropriate statistical level, the biometric reader sends the user's unique identifier to the Lenel ESS, which utilizes its database to determine if the user is allowed access to the requested physical space. If the live scan and stored biometric template do not match, the Lenel system does not grant access. An appropriate error message is recorded in the Lenel system log, in order to identify which users were having problems with the system.
5. If the user is allowed access to the requested space, the door controller operates the door strike of the requested door, allowing it to be opened.

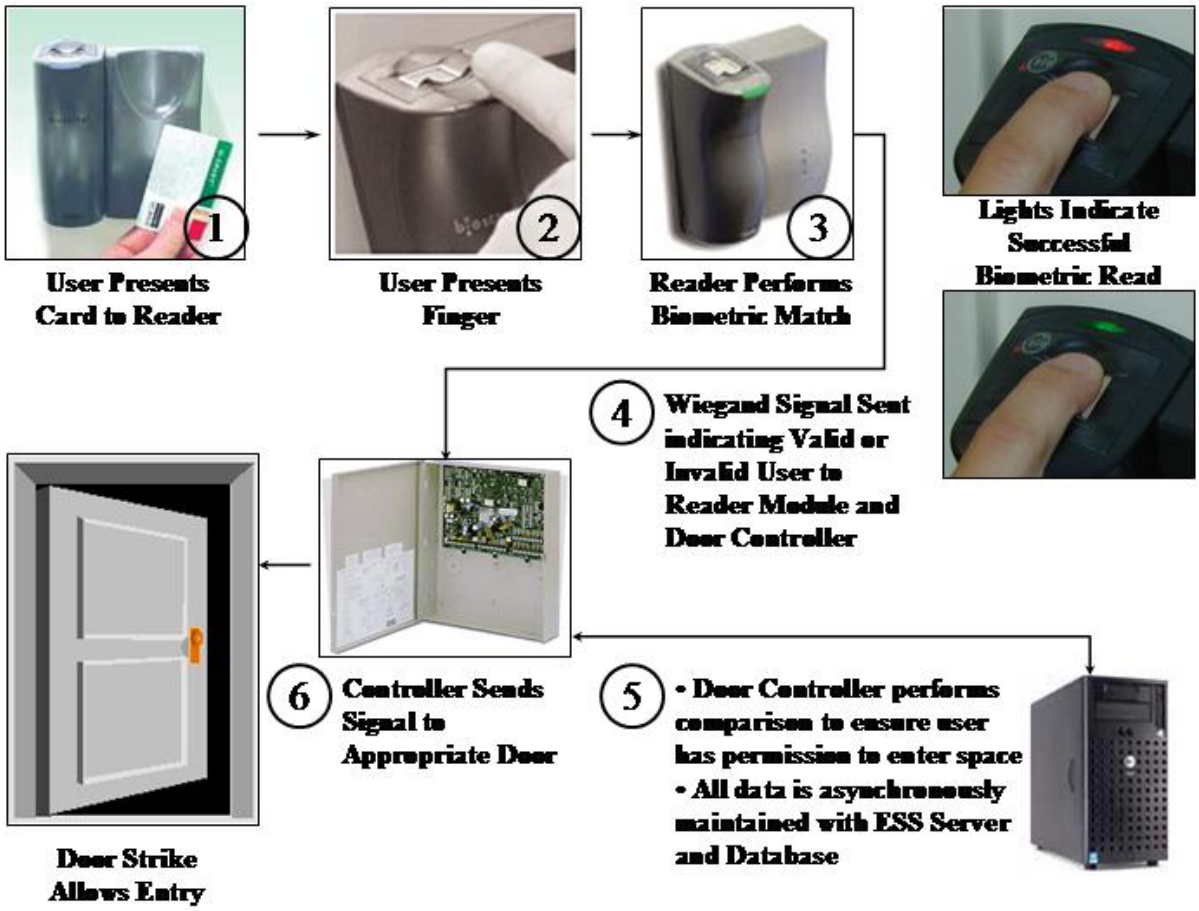


Figure 2: Pilot Fingerprint Authentication

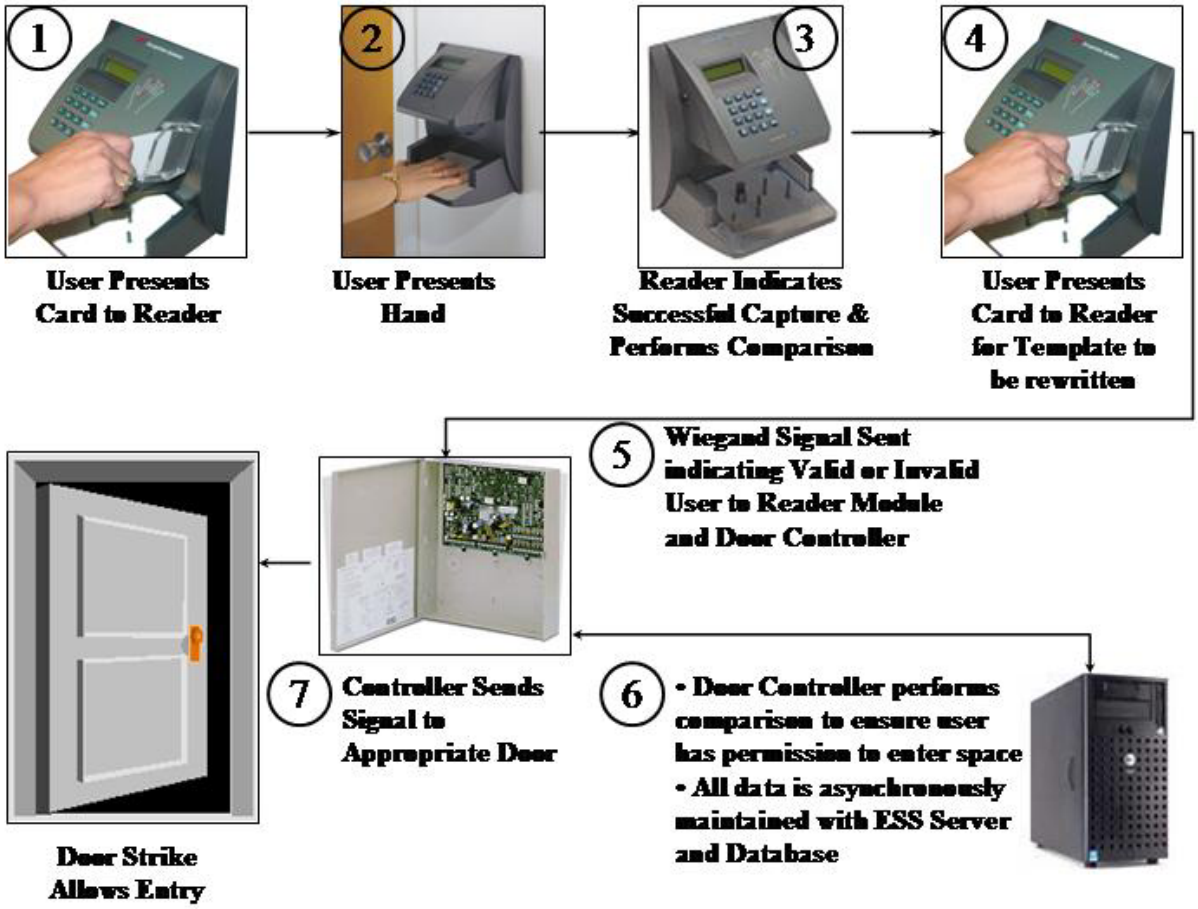


Figure 3: Pilot Hand Geometry Authentication

2.4. Technical Architecture

In the following figure, the pilot system is divided into 4 sections; each will be discussed separately identifying what technical aspects were added in order to implement the pilot system at US PACOM.

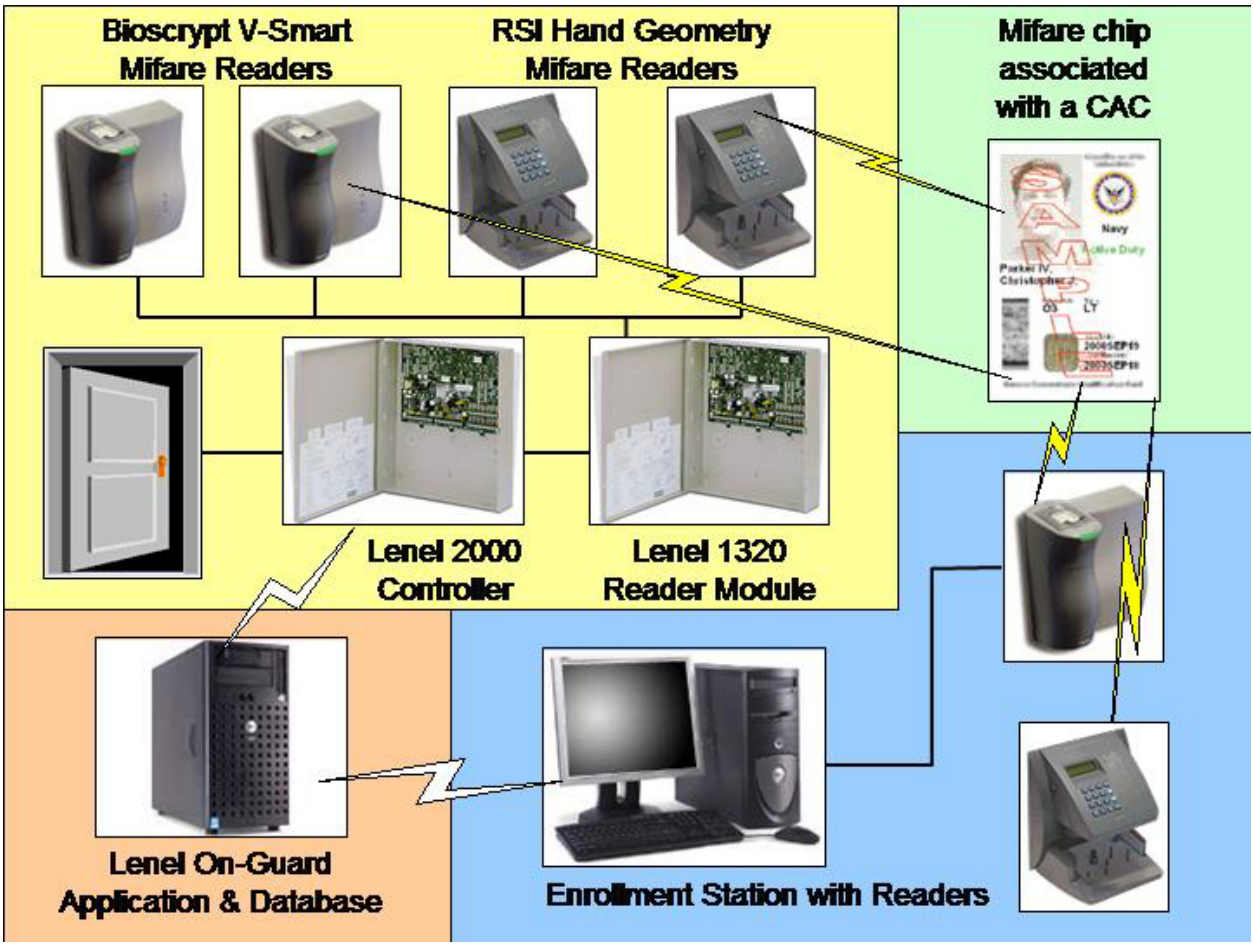


Figure 4: Pilot Technical Architecture

2.4.1 Hardware Changes

For the doors where the additional security was deemed necessary, readers were installed along with door strikes where needed. For exterior doors, the RSI hand geometry readers were installed. These units had a weatherized cover allowing them to be used in an outdoor setting. For interior doors, BioScrypt fingerprint readers were installed.

2.4.2 Card Architecture

The contactless chip incorporated Mifare technology, utilizing an antenna, which communicates with the reader using a 13.56 MHz signal. The Mifare chip has 1 kilobyte of space for the storage of data. This is sufficient storage space to contain a fingerprint template from the BioScrypt unit, as well as a hand geometry template from the RSI unit. By utilizing this architecture, it was not necessary for a user's templates to be stored on any central database; rather, the only copy of a user's biometric templates exists on a physical token, which is in that user's possession. Also, what is stored is not an image

of the user's biometric; rather a mathematical algorithm is stored. This algorithm, even if compromised cannot be used to reconstruct an image of the user's biometrics and still requires that a live scan be presented. This approach should alleviate many of the potential privacy concerns that users would have with respect to their biometric data.

The Mifare chip has 16 sectors numbered 0-15 and 4 blocks per sector numbered 0-3. (See **Figure 5**) The fourth block in every sector is unavailable for use by Bioscrypt or RSI, since this sector contains the access permissions used by the Mifare technology to control access to the data stored on the card. This makes it impossible for the RSI reader to read sectors containing BioScrypt data, and *vice versa*. Two templates were stored on each card, and the template required 352 bytes of storage (the templates are actually 348 bytes in size). These are indicated as blue for the primary template and magenta for the secondary template in **Figure 5.**

The black blocks are used by the manufacturer and were unavailable to be written to for customized uses. The dark green block (Sector0-Block1) is the layout block and Bioscrypt and RSI to specify layout of data on card such as where the templates are located use it. The red block (Sector8-Block1) is the administration table: it serves as a pointer to the Layout bock for the Bioscrypt Mifare reader. The green block (Sector0-Block2) stores user data, at this time only the User ID. The BioScrypt reader uses it to determine if the user has access to the space. The RSI reader uses sectors 2 and 3 for storing the hand geometry template. When a biometric access grants or deny occurs the reader sends a Wiegand string to the Lenel 1320 panel. For PACOM, the Wiegand string for a match contained the Facility Code stored on the reader and the User ID stored on the 14443 chip. For mismatches a configured Wiegand string stored on the reader was sent to the Lenel 1320 panel. The results were logged into the Lenel On Guard Database.

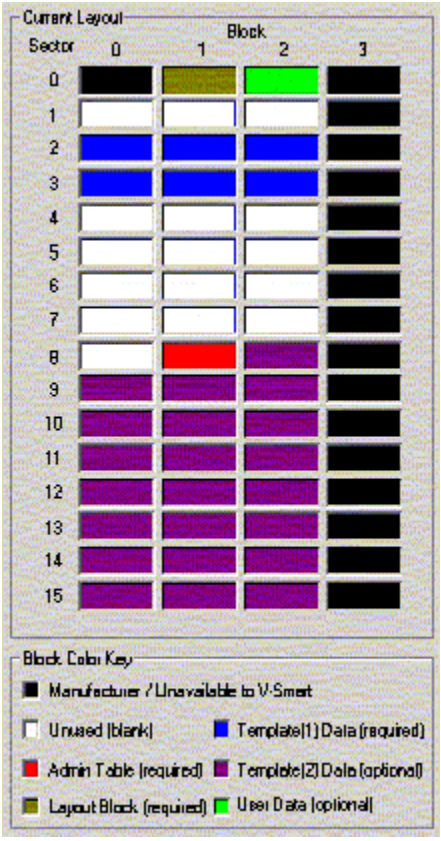


Figure 5: Mifare Chip Data Map

2.4.3 Enrollment Integration

Participants were enrolled into the ESS using the Lenel OnGuard badging system workstation. The badging system was hosted on a PC, running the Microsoft Windows 2000 Professional operating system, and containing 256 MB of RAM and 20 GB of disk storage. The badging software was part of the existing Lenel OnGuard system and the cards printed for the pilot conformed to the requested PACOM ID Configuration.

During enrollment via the Lenel badging workstation, the 26-bit Wiegand string comprised of the facility code and card number, was imported and assigned to personnel in the existing Lenel ESS database. This value is reported to the ESS when used at the existing proximity readers, which compares the user's permissions with the access requested at the reader's location. If the user is authorized, the backend sends a

command to the door strike, allowing the door to be opened

For biometric enrollment, the card was then taken to the biometric enrollment station. For the pilot, the same PC used for Lenel Badging had Bioscrypt VeriAdmin software (version 4.30) installed and a Bioscrypt V-Smart reader attached to the serial port of the enrollment station. The user had two fingerprint templates taken and stored to the card with their user profile as shown in the **Figure 5**. Once the user is enrolled biometrically, the card can be used at either of the existing proximity readers, or the biometric readers. When the user presents the card to a biometric reader, the templates are retrieved from the card, and a comparison is performed against a live scan from the user. The comparison threshold is set in two locations, one is specified for each V-Smart unit (used to heighten the matching requirements for more secure locations) and the other is defined at enrollment and stored on the Mifare chip (used to customize matching requirements for persons with poor biometric samples). Upon a match, the Wiegand data string associated with that user's profile is retrieved and transmitted to the ESS backend system, which compares the user's permissions with the access requested at the reader's location. If the user is authorized, the backend sends a command to the door strike, allowing the door to be opened.

2.4.4 Backend Application & Database

The backend ESS system does not distinguish between the currently installed ProxPro readers or the Biometric readers, because both send the same formatted Wiegand signal. There was no changes made to the ESS to biometrically enable the system: no additional modules or data fields were required. The workstation configuration used at PACOM can be found in the table below:

System Requirements	
Application	Lenel On-Guard Access Version 5.9
Operating System	Windows 2000
Memory Required	256 MB
Database	SQL Server 2000

Figure 6: ESS System Requirements

3. Project Goals, Objectives and Metrics

3.1. Project Goals and Objectives

3.1.1. Dual Biometric Operational Test

The immediate objective of this biometric pilot was to provide operational data for US PACOM to determine which technologies would provide the best-layered solution for the Nimitz-MacArthur Command Center HQ Building. The pilot would evaluate both fingerprint and hand geometry biometric technologies on a 1Kb MIFARE platform. This technology would be evaluated with an association with the CAC to determine how US PACOM personnel would respond using their CAC as the physical access token.

3.1.2. Next-Generation CAC

Beyond the immediate goal of improving access control, the larger objective is to provide operational data on contactless technology for consideration to be placed on the next generation of CAC's. Specifically, this pilot, by utilizing multiple biometric technologies would lay a foundation for configuration management for the contactless smart chip and how to incorporate multiple vendors' products on to the CAC in a non-proprietary manner.

3.2. Project Metrics

Three categories were devised to measure the success of the pilot in attaining the goals mentioned above. The majority of the metrics deal with intangibles, such as user's response to the using biometrics and how it enhanced security. By leveraging the existing infrastructure, some potential financial benefits can be realized, making a layered security approach economically feasible.

3.2.1. User Acceptance

The metrics for user acceptance were designed to measure overall satisfaction from end-users: ease of use in the operational environment; an increased knowledge of biometrics; and any increased feeling of security among users of the system. These metrics were captured using pre-pilot and post-pilot survey forms that were completed by users of the system, as well as through anecdotal reports from users and management and problem reporting forms filled out during the course of the pilot. Striking the right balance between level of security and inconvenience to the end user is a fine line that the pilot hoped to find through education and timely issue resolution. Goals for user acceptance were established with the perception that users would generally respond negatively to the system. For general user acceptance, the team set an ambitious goal that the majority of users would have a moderately positive response to the system in areas of ease of use and reliability. Recognizing the common user reaction that the use of biometrics as an invasion of privacy, the team set biometric awareness and response goals to increase positively one step on the survey's Liekert Scale. The overarching goal was for the users not to feel the system negatively impacted their ability to perform their duties.

3.2.2. System Performance

The metrics for system performance were designed to provide an assessment of how well the system performed during the pilot with respect to system stability, error rates in an operational setting, accuracy and speed of enrollment, and ease of administration of the system. These metrics were based primarily upon detailed review of all system logs, along with surveys of administrators of the system and other anecdotal reports. Goals for these specific metrics were established using the previous SSC Norfolk pilot as a baseline. Some specific goals for the system were: 95% system uptime, issue resolution within 1 day and that 90% of users would gain access on their first attempt and 95% on their second attempt. The other metrics were captured to gauge the ease of administration of the system and potential workload constraints the system would bring.

3.2.3. Enhanced Security

The metrics for enhanced security are a measurement of assurance that the individual attempting to use a card (token) for access is in fact the authorized owner of that card. These metrics were based primarily upon qualitative statements provided by managers

and administrators of the system. The obvious goal was for the on-site security managers to endorse the pilot as an asset in fulfilling their mission and use it as a model for the Nimitz-MacArthur Command Center HQ Building.

3.3. Alignment of Pilot and Enterprise Goals

The goal alignment table in **Figure 7** demonstrates how the enhanced capabilities offered by the CAC-PAC Norfolk system directly contribute to the satisfaction of enterprise goals and objectives.

Enterprise Goals & Objectives	Pilot-Enabled Capability	Key Performance Indicators
Use the CAC as the Physical Access Token	Contactless Technology	Evaluate 14443 A for inclusion on future CAC's
		Explore means to standardize how the contactless chip can be used across the enterprise.
Enhance Physical Access Control	Biometric Technology	Increased Biometric Awareness
		Increase User's feeling of security
		Provide Stronger User Authentication
Determine Cost and Time Effective Means to Enhance Security	Leverage Existing ESS	Minimize upgrade costs to backend systems
	Increase Security only where Required	Only upgrade where there is a security requirement, as opposed to reacting to technology constraints.

Figure 7: Goal Alignment Table

4. Analysis of Pilot Results

4.1. Evaluation of Metrics

This section presents an assessment of the quantitative success rates achieved in attaining the previously established goals of the project. A detailed description of each metric, the goal for which that metric is applicable, and the results obtained through quantitative analysis are provided. The metrics were obtained primarily from two sources: user responses to pre-pilot and post-pilot surveys and the error log in the ESS. A detailed description of the bases for measurement and results obtained are provided in **Appendix A** of this document. The system administrators and design engineers contributed to the qualitative and financial benefits of the pilot.

4.1.1. User Acceptance

As stated in **Section 3.2.1**, by adding an additional step to the entry process, and knowing the privacy concerns that individuals may have about their biometrics captured,

the team expected end-users to respond negatively to the pilot. However, the team also expected to balance the negative feelings with an increased sense of security and awareness of biometrics. User acceptance was measured using eleven different metrics: (1) general user satisfaction, (2) user perceptions of ease of use, (3) user perceptions of system reliability, (4) user perceptions of impact of system on their daily operations, (5) user perceptions of quality of training received, (6) increased user knowledge of biometrics, (7) improved user opinion of biometrics, (8) decreased perception of invasiveness of biometrics, (9) improved user opinion on use of biometrics for access control in their workspace, (10) improved user opinion on the use of the CAC as an entry token for physical access, and (11) improved user opinion on suitability and convenience of using the CAC in a plastic pouch for physical access.

The results were somewhat mixed. The general user satisfaction level, as measured by the post-pilot survey, was moderately positive, which satisfied the target criteria. Ease of use and reliability were dependent on the modality: the fingerprint readers were found to be moderately reliable and easy to use, which met the target criteria, but the hand geometry readers were evaluated on average as neutral or no opinion for both reliability and ease of use. User perceptions of impact on their daily operations were, on average, neutral/no opinion, which met our criteria. User perception of quality of training was somewhat satisfactory, which met our criteria. With respect on increased knowledge of biometrics, a very slight increase in average scores from pre-pilot to post-pilot was observed, but the increase was not significant enough to meet our target criteria. A similar small increase was observed in the user opinion of biometrics in general, and again, it was not significant to meet our target criteria.

The team had hoped that, with adequate training and experience using biometrics in this implementation, that users would show a decrease in their perception of the invasiveness of biometrics with respect to their personal privacy. In fact, there was a slight increase in the perceived invasiveness between pre- and post-pilot surveys. While not statistically significant, it still failed to meet our target criteria. However, there was a slight (one-half level) increase in user opinion on the use of biometrics for access control in their workspace. The increase did not meet the target of a full level of increase, but still is a measurably improved opinion.

The hoped-for improvement in user opinion with respect to the use of the CAC as an entry token for physical access was not realized. No change in score was reported between the pre- and post-pilot surveys. Finally, user opinion on the use of the CAC in a plastic pouch for physical access to secured spaces actually decreased slightly post-pilot. There are a number of comments provided by users addressing their concerns with the design and use of the plastic pouch in this manner.

For detailed survey results, please see **Appendix B: Detailed Users Survey Results**.

4.1.2. System Performance

This set of metrics provides an assessment of the actual performance of the pilot system and its components during the evaluation period. It is based primarily upon the system logs from the ESS, along with surveys of administrators. The specific metrics for system performance include (1) downtime, (2) issue resolution time, (3) increased

stability over time, (4) time to enroll and re-enroll, (5) failure to enroll, (6) quality of enrollment template obtained, (7) number of attempts required for successful enrollment (total of 12 individuals), (8) access granted rate on first attempt, (9) access granted rate on two or less attempts, (10) abandoned attempts, (11) administrative time required for system support, (12) ease of administration, and (13) ease of enrolling new users.

System metrics met or exceeded target criteria on every metric except one: time for re-enrollment of users who had difficulties. It took less than 10 minutes, on average, to re-enroll such problem users. The target was less than 5 minutes, so this did not meet the target. However, every other system performance target was met, or in many cases, exceeded.

For detailed system performance results, please see **Appendix C: System Statistics**.

4.1.3. Enhanced Security

The metrics for enhanced security provide an increased assurance that the individual attempting to use a card (token) for access is, in fact, the authorized owner of that card. The pilot was not intended to record the accuracy of the biometric devices in regards to False Acceptance Rates (FARs) and False Rejection Rates (FRRs); it was, rather, intended to measure the reactions of users to the use of biometric technology for physical access control, and to obtain data on how the technology functioned in a typical operational environment. User perceptions of security have already been discussed, in Section 4.1.1 above. However, it is important to assess the perception of security among the managers and administrators, as well as among the general user population. These metrics were based primarily upon qualitative statements provided by managers and administrators of the system.

USPACOM designated three individuals to be administrators for the system, thus making qualitative analysis based upon administrative surveys not statistically significant, but valuable nonetheless due to their first hand experiences with the system. An additional difficulty arose from an apparent element of confusion among users completing the on-line, web-based survey form. On the pre-pilot form, twelve (12) individuals described themselves as being administrators of the system. This is obviously incorrect, and so no differentiation was made between general users and self-proclaimed “administrators” in the analysis of the pre-pilot survey forms. The misconception was apparently cleared up by the completion of the project, and only two individuals completing the post-pilot survey described themselves as administrators. Both of these administrators found that the use of biometrics made the workplace significantly more secure, and declared that their participation in the pilot had an extremely positive impact on their opinions on the use of biometrics for access control in the workplace. They both also indicated that the use of biometrics made it much easier to do their jobs on a daily basis.

In a comparison of pre-pilot and post-pilot responses, managers and non-managers both displayed an improved opinion on the use of biometrics for access control in the workspace, but the degree of increase was significantly higher for managers than non-managers. Similarly, both groups displayed an increased level of agreement that the increased security provided by biometrics was worth the inconvenience of presenting the card (token) and finger or hand for access, with managers again showing a significantly

higher level of increase. With respect to opinions on the use of the CAC as an entry token, managers displayed a slight, non-significant increase, and non-managers a slight, non-significant decrease. Both groups had slightly decreased opinions on the use of the CAC in a plastic pouch as opposed to carrying multiple badges, but again, these decreases were so small as to be statistically insignificant.

Among both managers and non-managers, the most common response to the question "How has your participation in this pilot influenced your opinion on the use of biometrics for access control in your workplace" was "moderately positively". Both groups also responded to the question "how do you believe the use of biometrics in this pilot impacted the security of your workplace" with average responses between "neutral" and "moderately positively", with the latter being the most commonly provided response.

4.2. Qualitative Analysis and Intangible Benefits

In addition to the metrics described above, the PACOM Pilot produces several less quantifiable, yet significant benefits for both the customer and the enterprise. These include:

Integration of biometrics with existing ESS – The pilot demonstrated the ability to integrate a biometric authentication solution utilizing contactless technology into an existing enterprise legacy ESS. No large-scale replacement of legacy security infrastructure is required, which could lead to significant savings in future deployments. While this assertion cannot be made for all ESS's, the design laid out in this pilot makes it a promising prospect that would avoid additional cost associated with a full-scale upgrade.

Minimize Privacy Concerns – Through the education process, participants were made aware that their biometric templates were stored on their card rather than in a database. They were also instructed that the information on their card was a biometric template or a mathematical representation of their fingerprint, and it could not be reverse engineered to reconstruct their biometric information. These two design considerations alleviated most concerns about using biometric technology.

Validation of Security Access – By upgrading the J-6 spaces to biometric entry, management, for the first time, was able to set access privileges to those spaces when everyone was requested to enroll their biometric. The audit performed prior to biometrically enrolling persons allowed the security managers to revalidate who had access to the spaces and assured them of who was entering the spaces.

Scaled Upgrades – Management at PACOM was impressed on how a portion of the ESS could be upgraded to biometrics based on their security requirements. They plan to continue use part of the pilot system on Building 20E and selected doors of building 20. USPACOM plans to replace the RSI hand geometry readers on Building 20E with the Bioscypt fingerprint readers. USPACOM plans to leverage this study to research biometric options for other locations, possibly in their new headquarters building, which is currently under construction.

4.3. Pilot Costs

Line Item	Total
Labor (Organic)	

Line Item	Total
Hardware	

SSC Charleston	$24,600.00
SSA Pacific Pearl City	
- Installation per IDP	$19,600.00
- Collect detailed records	$22,100.00
- On-site maintenance	$19,000.00
Subtotal Labor (Organic)	*$85,300.00*
Software	
Lenel On-Guard 32ESI Ver 5.10	$6,320.00
Lenel Bioscrypt Software SWG-1402	$3,295.00
Subtotal Software	*$9,615.00*
Other	
Travel	$5,200.00
Per Diem	$1,600.00
Subtotal Other	*$6,800.00*
Grand Total	**$155,000.00**

Lenel LNL-2000 Door Controllers (2)	$2,178.00
Lenel LNL-1320 Reader Modules	$2,508.00
RSI Contactless Hand Geometry Readers (5)	$10,000.00
Bioscrypt V-Smart Readers (10)	$9,650.00
RFID Tags (400)	$2,400.00
Door Strikes (10)	$4,290.00
Magnetic Lock	$631.00
Power Supplies (6)	$2,916.00
American Fibretek MT-0485-2 (2)	$1,176.00
American Fibretek PS-24 (2)	$32.00
12V DC Batteries (12)	$216.00
Misc Wire and Cabling	$200.00
Misc Supplies	$10,088.00
Equipment Testing	$6,000.00
Equipment Shipping	$1,000.00
Subtotal Hardware	*$53,285.00*

5. Pilot Lessons Learned

The lessons learned from this pilot were derived from the comments and responses provided by users of the system on the post-pilot survey forms, comments from administrators of the system, and written and oral communications from the PACOM management.

5.1. Problematic Population

With any biometric demonstration, there are portions of the population that are more problematic than others. PACOM provided a test bed where known issues had to be addressed from the very beginning. For example, it is widely accepted that the fingerprint ridges in Asian women are hard to detect with many biometric readers. Great care was given to the quality of the enrolled template and the matching threshold was lowered to accommodate this population. Other users were identified through close monitoring of biometric mismatches on a daily basis. One woman experienced problems convincing the fingerprint readers her presented biometric was from a live person due to poor circulation; this was resolved by her rubbing her hands together prior to presenting her finger. Another individual experienced problems because a lifetime of fishing had worn the some of the ridges on his fingers away: this problem was resolved by enrolling a thumb that presented a higher quality template.

LESSON: *Knowing the demographics and lifestyles of the user base can assist in planning for the exceptions to the rule.*

5.2. Personnel Data

Prior to executing the pilot, user information was going to be loaded into the Lenel database to shorten the enrollment time. This information consisted of common data elements such as name and rank. US PACOM also had a requirement for a color-coded tag to indicate the security clearance level and expiration dates. The goal was to have a pre-printed tag that the biometric data could be loaded on at the time of enrollment. The data was crucial in making the enrollment process as quick and inconvenient as possible. PACOM's personnel database proved to be an unreliable source for this information. Much of the data had to be manually collected. Needless to say, this was time consuming and nearly caused a delay in the pilot.

LESSON: *Data requirements, sources and integrity should be evaluated at the beginning of the pilot to ensure that all aspects are ready for when they are needed.*

5.3. Revisiting Business Processes

When evaluating the personnel database, it was discovered that there was a need to revisit their existing business processes and procedures. For example, it was discovered that many of the personnel in the database had moved to their next duty station early, but were still active personnel in the database. This highlighted that the exit procedure should be modified so that the personnel database was updated and the badges were properly collected and accounted for.

LESSON: *Data integrity issues when brought to light are opportunities to reengineer your business processes. Consistent data monitoring reveals potential problems before they multiply.*

5.4. Distributed Access Control

One interesting problem experienced during the initial pilot execution was assigning access levels to individuals. It was determined that the space owners should determine who should have access to their spaces and when they should have access. This was a strong paradigm shift: everyone with a badge had access. With this new control, space owners experimented with restrictions on everyone, except for their employees, then switching back to open access. It took two weeks before the access rights became stable. During this time period, many of the end users were confusing access denial with biometric mismatches. The confusion could have been minimized if the personnel database had more clearly defined the access roles from the beginning.

LESSON: *Distributing control may be the most effective means of controlling access to spaces, but there must be a framework in place that defines the access rules.*
Infrastructure Ownership.

6. Future Opportunities and Next Steps

The PACOM Biometric Enhancement Pilot fulfilled the expectations of both the eBusiness Office and HQ PACOM by attaining established project goals and providing data on the use of contactless biometric equipment to enhance physical security in an operational setting. Additionally, data provided during the post-pilot evaluation will allow decision-makers to determine appropriate operational implementation issues with respect to future expansion of these capabilities at PACOM.

6.1. Necessary System Enhancements

This pilot clearly demonstrated the functional ability to utilize contactless biometric technology for controlling access to secured spaces. Additionally, it demonstrated the relative ease with which such technology may be integrated with an existing enterprise security infrastructure, especially when there is already an Electronic Security System (ESS) in place at those spaces. One enhancement that would provide additional benefit to the administrators would be a function to modify the requirement for biometric verification as threat conditions change. PACOM system administrators will need to maintain an acceptable level of inventory of card stock for the enrollment of new users, and for the replacement of lost or damaged contactless cards.

6.2. Action Plan for US PACOM

The PACOM biometric enhancement pilot remains in use for controlling access to some of the J6 spaces: Building 20E and selected J6 spaces (3 doors) in building 20. As a result of this successful pilot, PACOM is investigating inclusion of biometric access, in select locations for their newly constructed PACOM headquarters building. Some of the other areas that PACOM expressed an interest in are as follows:

- Logical Access
- Gate Access Solution
- Egress

- Flesh out American Disabilities Act (ADA) requirements
- Articulate Biometric Requirement to ACO
- Explore Enterprise Licensing Arrangements for Lenel Software

"However, as noted on the signatory page, this paragraph does not constitute a commitment by USPACOM to any organization, including without limitation, federal or non-federal entities, contractually or otherwise, to a specific technology or course of action."

6.3. Enterprise Opportunity

This pilot demonstrated that biometrics on a MIFARE embedded chip could meet the functional demands of the physical security community for door access control. However, the next step may be caught in a circular loop: if the CAC is to fulfill its role as the physical security token for DoD, then it needs to incorporate the accepted technologies the ESS and physical security community uses for authentication. Likewise, if the physical security community wants to use the CAC as the physical security token, then it needs to clearly articulate what standards should be incorporated on the next-generation CAC. There is an enormous potential to reduce the number of physical security tokens used within DoD, but the cycle of requirements versus infrastructure must be resolved. The eBusiness Operations Office clearly believes that a major warfighting command such as PACOM will be instrumental in the requirements process.

6.4. Enterprise Action Plan

In order to resolve the cycle of current CAC architecture versus requirements for next-generation CAC, an action plan has been generated to inform the appropriate agencies on the results of this pilot, gather concurrence regarding requirements, properly evaluate all potential solution, and facilitate a decision.

6.4.1. Short-Term Actions

DON eBusiness Operations Office has taken for action:

1. Provide pilot results to DON CIO, CNO N34, Biometric Management Office (BMO) and DOD ACO.
2. Continue to provide guidance to other Navy and Marine Corps organizations in regards to using the CAC as a physical security token by informing them of existing policies, current technologies trends and potential solutions to meet their specific needs.

6.4.2. Long-Term Actions

To fully develop the end state solution, several organizations across the services must agree on a CAC configuration that supports the requirements of the physical security community.

1. Determine whether contactless technology will or will not be on the next generation CAC.
2. Ensure that the NIST Government Smart Card Interoperability Specification (GSC-IS 2.1) Appendix G will be the standard for contactless.
3. CNO N34, DON eBusiness Operations Office and DON CIO determine

recommended DON platform.

4. CNO N34 presents architecture requirements to Security Equipment Integration Working Group (SEIWG).
5. SEIWG makes recommendation to SCSCG regarding technology requirements for physical security community.
6. Senior Smart Card Coordinating Group (SCSCG) presents the DOD ACO with a configuration change request.
7. National Security Agency (NSA) to fully evaluate contactless security vulnerabilities, such as interception of contactless signals and key hacking.
8. Evaluate other technology solutions that meet the same function requirements.
9. DoD ACO to make contactless technology decision on the next-generation CAC.
10. SCSCG to determine space configuration on contactless chips, if necessary.
11. Define policies and deployment strategies that will encourage a transition to the next-generation CAC, as the DoD physical security token.
12. Define Issuance Strategy for next-generation CAC. (Currently under review).

Appendix A Detailed Basis for Measurement

The table below was taken from the PACOM BEPS Test Plan and Post Pilot results were added.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
1	**System Performance**					
2		Downtime	Lenel System Logs	Percentage of time that system is up and available to users.	95%+	**EXCEEDED GOAL:** The only downtime observed through an examination of system logs consisted of two brief interruptions to systems communications to individual readers. These were noted as a sequence of "Communications Lost" and "Communications Restored" messages. The total duration of these interruptions were 12 minutes, 24 seconds. The system was had was up 99.999% of the time.
3		Issue Resolution Time	Lenel System Logs	How long, from the time a problem is reported to the systems administrator (or recognized to exist by the systems administrator through examination of logs) until that problem is corrected.	1 day	**MET GOAL:** Issues were resolved satisfactorily in less than one day on average.
4		Increased stability over time	Lenel System Logs	Measured by looking at system uptime/availability within each discrete time period (week or month). The system uptime should improve from its initial baseline and eventually plateau at the acceptable level.	10% improvement	**EXCEEDED GOAL:** The system was fully available over 99.999% of the time, thus there was no significant change over time.
5		Time to Enroll	Admin Reports	Time from the beginning of an enrollment to the completion of a successful enrollment (on average).	*10 minutes* for initial enrollment	**EXCEEDED GOAL:** Systems administrators reported an average enrollment time of less than 5 minutes.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
					5 minutes for re-enrollments	**MISSED GOAL:** Systems administrators reported re-enrollments took less than 10 minutes on average: this was twice the goal due to re-enrollment normal involved troubleshooting the root problem with the individual.
6		Failure to Enroll	Admin Reports	Percentage of users for whom it is not possible to obtain a satisfactory enrollment of one or more biometric templates	Less than 2%	**MET GOAL:** For the population of 350, satisfactory biometric templates were eventually obtained for all but 6 participants (1.7%). An additional 12 individuals had biometric matching threshold lowered beyond the standard system setting.
7		Quality of Enrollment Template	Admin Reports	Quality scores reported by the biometric vendor software at time of initial enrollment. Because of vendor limitations, only the Bioscrypt fingerprint system reports a measurable score, so no RSI hand geometry equivalent metric will be available.	Average Quality score for Bioscrypt fingerprint image: three stars.	**EXCEEDED GOAL:** The average quality score for Bioscrypt fingerprint images was 3.5.
8		Number of attempts required for successful enrollment.	Admin Reports	This is a count of the number of attempts made for each user before an acceptable quality biometric template is obtained and verified.	3 or fewer (average across all users).	**EXCEEDED GOAL:** The average number of attempts to obtain an acceptable quality biometric was 2.
9		Access granted on first attempt	Lenel System Logs	How often did a user gain entry to the system with only a single presentation of his biometric characteristic?	90%	**EXCEEDED GOAL:** The rate of access on first try ranged from 85% to 99% on individual doors. The aggregate average across all doors was 92.33 %.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
10		Access granted with 2 or fewer attempts.	Lenel System Logs	How often did a user gain entry to the system with 2 or fewer presentations of his biometric characteristic? This will be determined through review of the Lenel system log files.	95%	**EXCEEDED GOAL:** The rate of user successful verifications with one or fewer retries ranged from 97.82% to 99%.
11		Average number of attempts required to gain access to the system.	Lenel System Logs	Average number of attempts for all users before a user was granted access to the system. This will be determined through review of the Lenel system log files.	2.5 or less (average)	**EXCEEDED GOAL:** The average number of attempts was less than 2, which exceeds the target criteria.
12		Abandoned attempts	Lenel System Logs	How often did a user attempt to gain access to the system, then abandon the attempt before being granted access? This will be derived through an examination of the Lenel system log files.	Decrease over time.	**EXCEEDED GOAL:** There were no significant instances of users abandoning efforts to access the system were noticed.
13		Administrative time required for systems support.	Admin Post-Survey	How many hours per week (average) did systems administrators have to spend on maintenance, support, and troubleshooting of the system, as reported on Administrator Post-Pilot Survey Form.	10 Hours or Less per week.	**MET GOAL:** Both administrators who completed the post-pilot survey indicated that they spent less than 10 hours per week on maintenance, support, and troubleshooting of the system.
14		Ease of Administration	Admin Post-Survey	How difficult did systems administrators find it to provide maintenance, support and troubleshooting of the system, as reported on Administrator Post-Pilot Survey Form.	Moderately Easy	**MET GOAL:** Both administrators who completed the post-pilot survey rated maintenance of the system as Moderately Easy.
15		Ease of Enrolling New Users	Admin Post-Survey	How difficult did systems administrators find it to enroll users into the system, as reported on Administrator Post-Pilot Survey Form.	Moderately Easy	**EXCEEDED GOAL:** Both administrators who completed the post-pilot survey rated the ease of enrolling users in the systems as Very Easy.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
16	**User Acceptance**					
17		General User Satisfaction	User Post-Survey	Average of User responses on the Post-Pilot Survey form to the question "What is your general level of satisfaction with the Pilot Project?"	Moderately Positive	**MET GOAL:** Question 7 on the survey, "Do you feel the increased security that biometrics provides is worth the inconvenience of presenting your card and presenting your finger or hand to the reader?" provides the metrics used. The average post-pilot response was 4.0, "Somewhat Agree", which equates to the target criterion of Moderately Positive.
18		User Perceptions of Ease of Use	User Post-Survey	Average of User responses on the Post-Pilot Survey form to the questions "How would you rate the ease of use of the Hand Geometry Readers?" and "How would you rate the ease of use of the Fingerprint Readers?"	Moderately Easy to Use	**MIXED RESULTS:** **MISSED GOAL:** The user responses were an average of 3.0, or "Neutral/No Opinion" for ease of use of the Hand Geometry readers, which did not meet the target criterion. **MET GOAL:** user responses were an average of 4.0, which is "Moderately Easy", for the Fingerprint readers, which met the target criterion.
19		User Perceptions of System Reliability	User Post-Survey	Average of User responses on the Post-Pilot Survey form to the questions "How would you rate the reliability of the Hand Geometry Readers?" and "How would you rate the reliability of the Fingerprint Readers?"	Moderately Reliable	**MIXED RESULTS:** **MISSED GOAL:** The user responses were an average of 3.7 (Neutral to Moderately Reliable) for the Hand Geometry readers' reliability, which did not meet the target criterion. **MET GOAL:** The user responses were an average of 4.0 (Moderately Reliable) for the fingerprint readers' reliability, which met the target criterion.
20		User Perceptions of Impact of system on their daily operations.	User Post-Survey	Average of User responses on the Post-Pilot Survey form to the question "What impact did the use of biometrics have on your	No Impact or No Opinion.	**MET GOAL:** The average user response to this question was 3.2, or Neutral/No Opinion. This meets the target criteria.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
				daily operations?”.		
21		User Perceptions of Quality of Training	User Post-Survey	Average of User responses on the Post-Pilot Survey form to the question “How would you rate the quality of training and orientation provided to you at the beginning of this pilot?”	Somewhat Satisfactory	**MET GOAL:** Average user response was 4.2, Somewhat Satisfactory. This meets the target criterion.
22		Increased user knowledge of biometrics	User Pre-Survey and Post-Survey	Increase in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question “How would you describe your current level of knowledge about biometrics?”	Average Increase of one level.	**MISSED GOAL:** The average increased from 2.5 (midway between “Somewhat Knowledgeable” to “Moderately Knowledgeable”) to 2.7. This was not as significant an increase as was targeted.
23		Improved User Opinion of biometrics in general	User Pre-Survey and Post-Survey	Increase in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question “What is your opinion, in general, of biometrics?”	Average Increase of one level.	**MISSED GOAL:** The average increased from 3.4 to 3.8, which is less than the target criteria.
24		Decreased perception of invasiveness of biometrics.	User Pre-Survey and Post-Survey	Improvement in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question “To what degree to you consider biometrics to be an invasion of your personal privacy?”	Average improvement of one level.	**MISSED GOAL:** The average increased from 3.3 to 3.4; a small increase, but we had hoped to see a decrease in perceived level of invasiveness, so the target criteria were not satisfied.
25		Improved User Opinion on the use of biometrics for access control in their workspace.	User Pre-Survey and Post-Survey	Improvement in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question “What is your opinion on the use of biometrics for access control in your workplace?”	Average improvement of one level.	**MISSED GOAL:** The average increased from 3.6 (on the positive side of the “Neutral/No Opinion” value) to 4.1 (“Somewhat Agree”). Numerically, not as strong an increase as we had targeted, but still a measurably positive improvement.

#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
26		Improved User Opinion on the use of the CAC as an entry token for physical access.	User Pre-Survey and Post-Survey	Improvement in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question "What is your opinion on the use of the CAC as an entry token for physical access to secured spaces?"	Average improvement of one level.	**MISSED GOAL:** The average remained unchanged at 3.6, so the target criteria were not satisfied.
27		Improved User Opinion on the suitability and convenience of using the CAC in a plastic pouch for physical access.	User Pre-Survey and Post-Survey	Improvement in average values reported by users on Post-Pilot Survey form over values reported on Pre-Pilot Survey form to the question "What is your opinion on the suitability and convenience of using the CAC in a plastic pouch for physical access to secured spaces?"	Average improvement of one level.	**MISSED GOAL:** The average decreased from 3.7 to 3.5. This was a small decrease, but clearly a move in the opposite direction from what was hoped for. The target criteria were not satisfied.
28	**Cost Benefit**	Overall				
29		Cost of enhancing a system with biometrics.	SSC Charleston Actual Cost Reports	Cost differential involved in deploying the biometric solutions compared to a non-biometric installation of an electronic security system (ESS).	Less than 10% differential.	
30		Cost of Consolidating Technology to the CAC.	SSC Charleston Actual Cost Reports	Cost savings if biometrics and contactless technologies existed on the CAC vs. requiring a separate contactless biometric token and pouch.		
31		Impact to Security Operations and Maintenance Costs.	SSC Charleston Actual Cost Reports	This will measure the costs of deploying and maintaining a contactless biometric security system.		
32	**Security Enhancement**	Overall	Rolled up Summary			
33		Increased	User Pre-Survey	Improvement in average values	Average	**MISSED GOAL:** The average

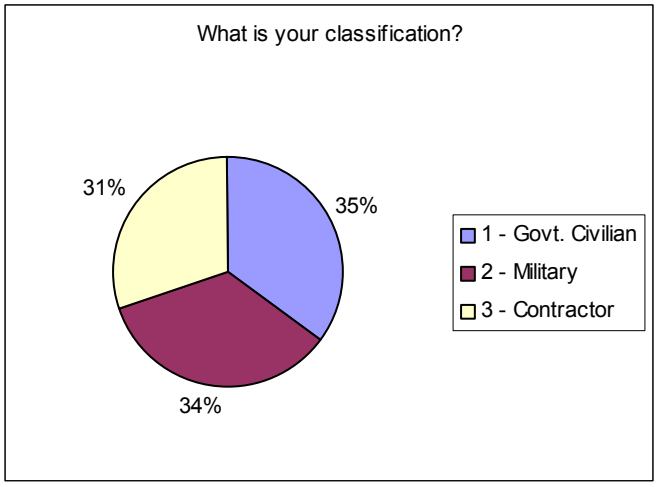
#	Metric Group	Metric	Data Source	Calculation Method	Goal	Observed Result
		perception of security and safety by users.	and Post-Survey	reported by users on Post-Pilot Survey form over values reported on the Pre-Pilot Survey form to the question "What is your perception of the current level of security in your workplace?"	improvement of one level.	increased from 3.3 (Neutral/No Opinion) to 3.9 (just below Moderately Secure). Not quite a one level improvement, so the target criteria were not met.
34		Reduction of Fraud and Theft	PACOM OPS Report	Reduced incidents of fraud or theft within the controlled spaces during the pilot as compared to incidents occurring before the pilot.		
35		Quality of System	PACOM OPS Report	US PACOM will provide a qualitative statement regarding how the pilot enhanced security.		

Appendix B Detailed Users Survey Results

Below are the survey questions, along with the relative percentage for each question among respondents. The left column contains the pre-pilot survey results; the right column contains the post-pilot survey results.

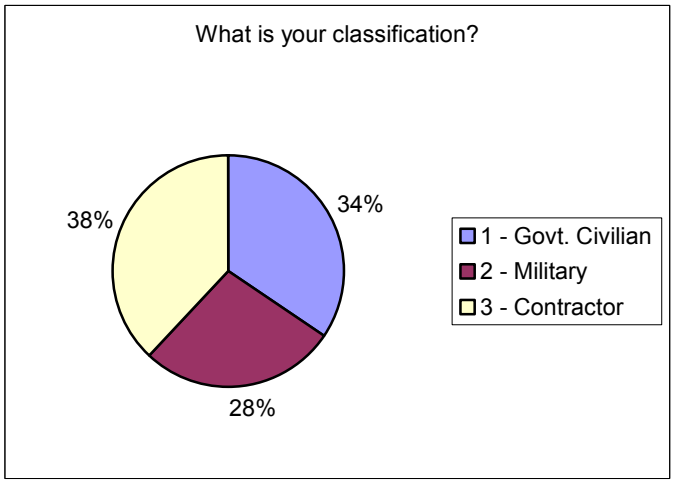
PRE-PILOT SURVEY

Question 1

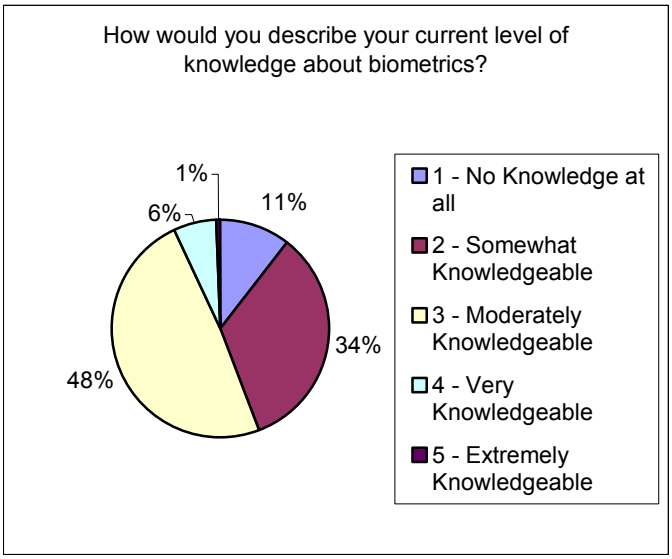


POST-PILOT SURVEY

Question 1

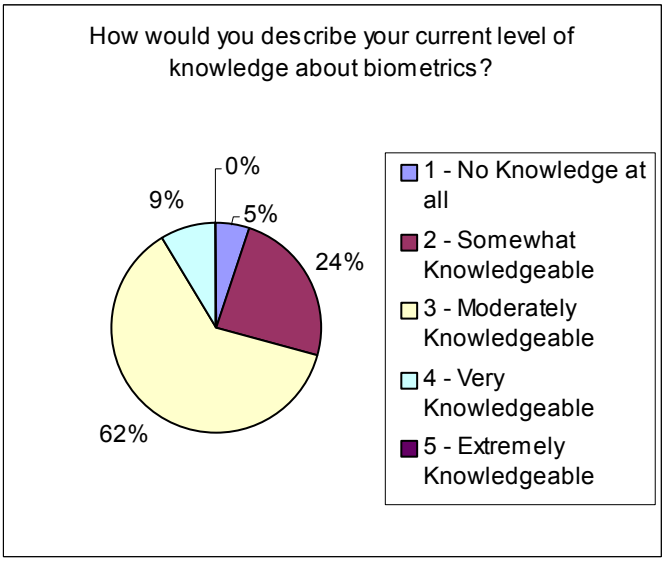


Question 2



Average: 2.5

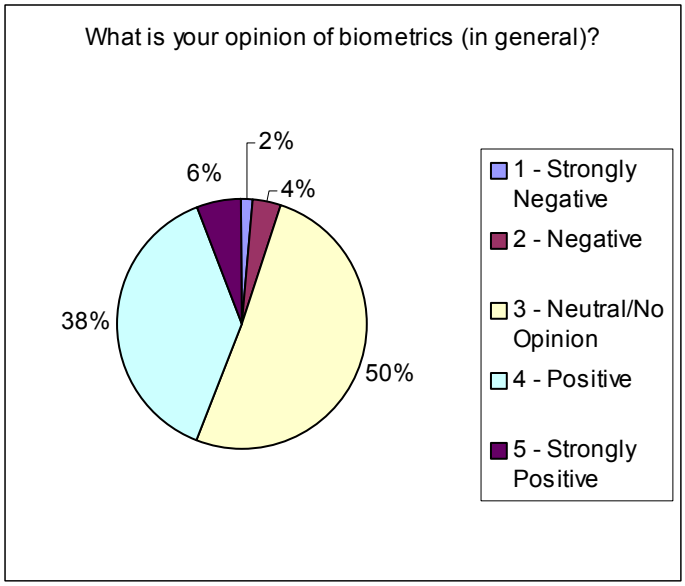
Question 2



Average: 2.7

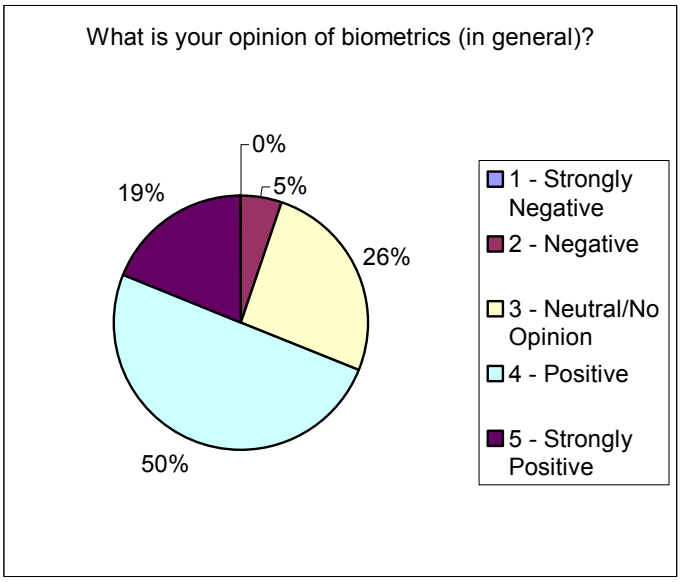
PRE-PILOT SURVEY **POST-PILOT SURVEY**

Question 3



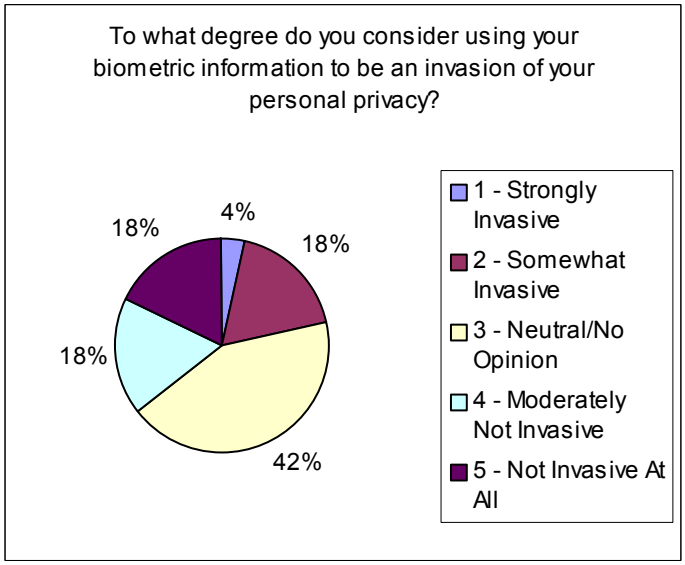
Average: 3.4

Question 3



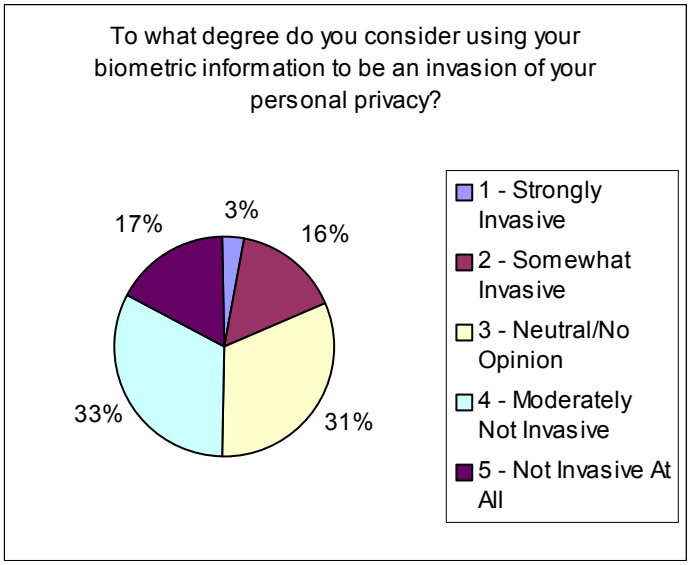
Average: 3.8

Question 4



Average: 3.3

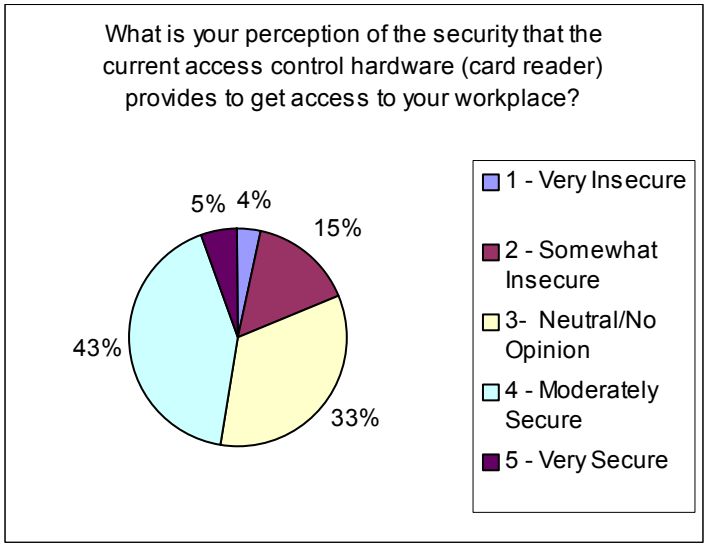
Question 4



Average: 3.4

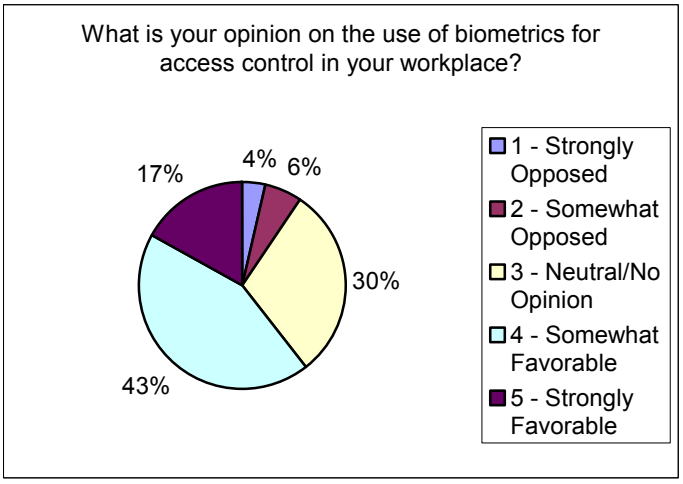
PRE-PILOT SURVEY

Question 5



Average: 3.3

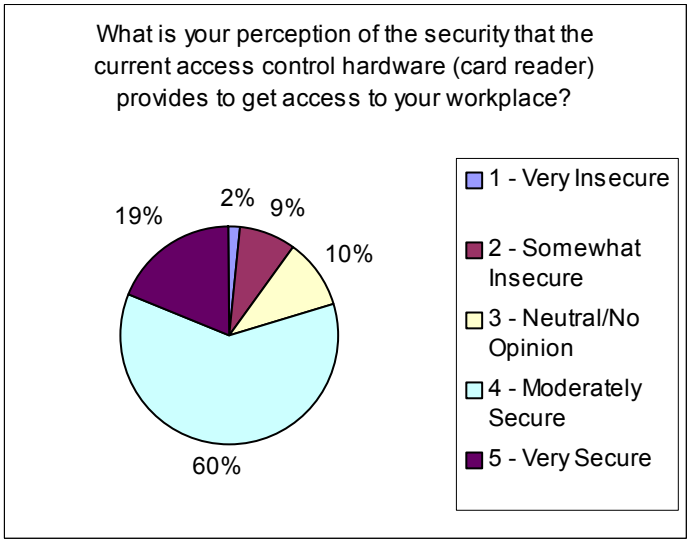
Question 6



Average: 3.6

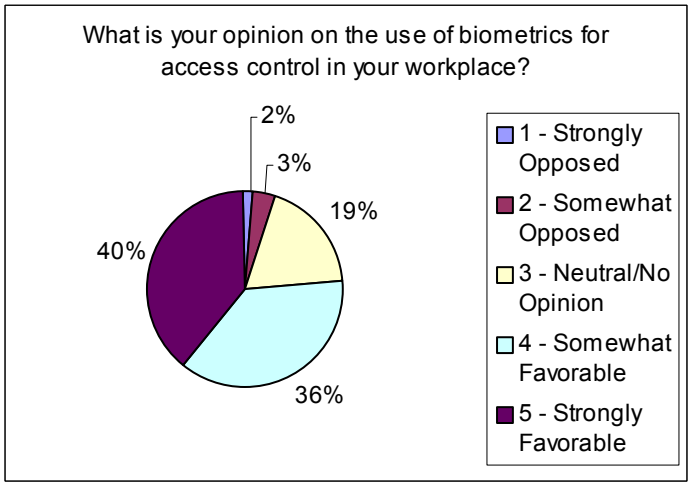
POST-PILOT SURVEY

Question 5



Average: 3.9

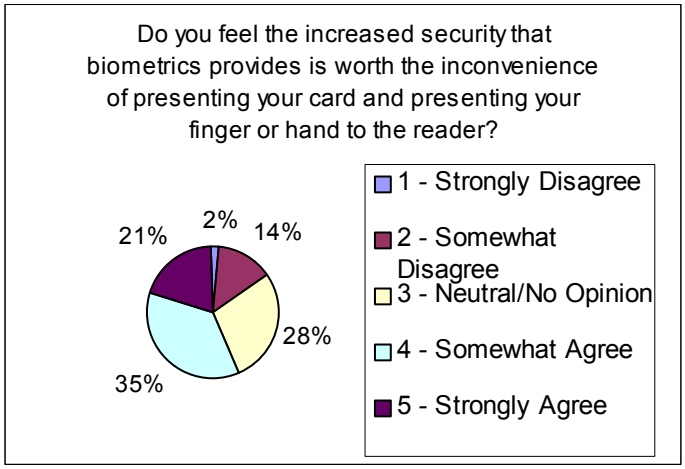
Question 6



Average: 4.1

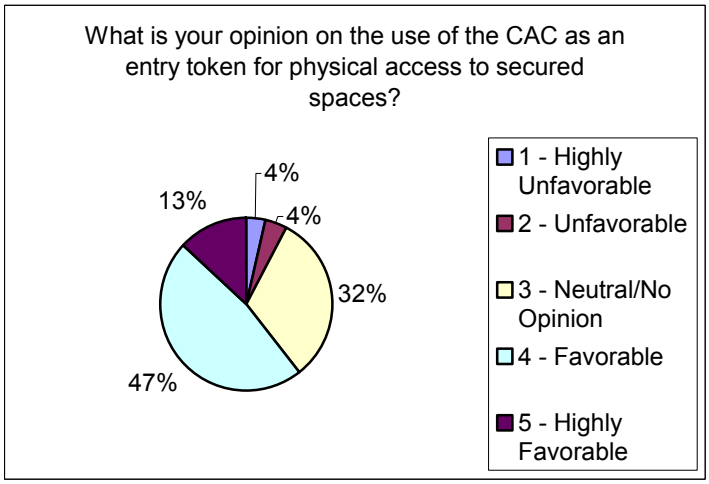
PRE-PILOT SURVEY

Question 7



Average: 3.6

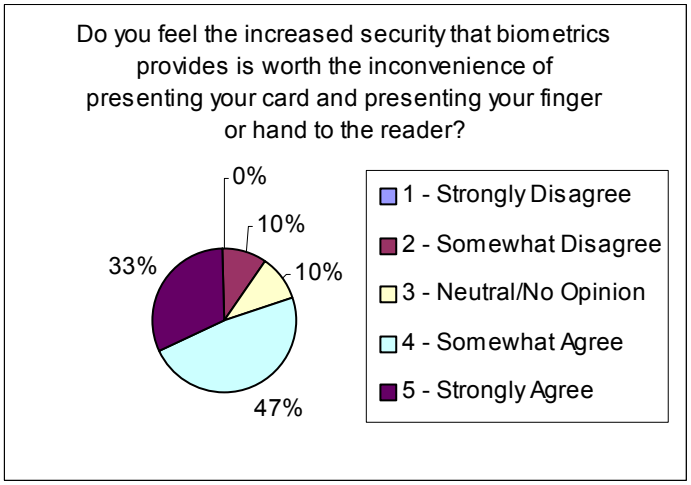
Question 8



Average: 3.6

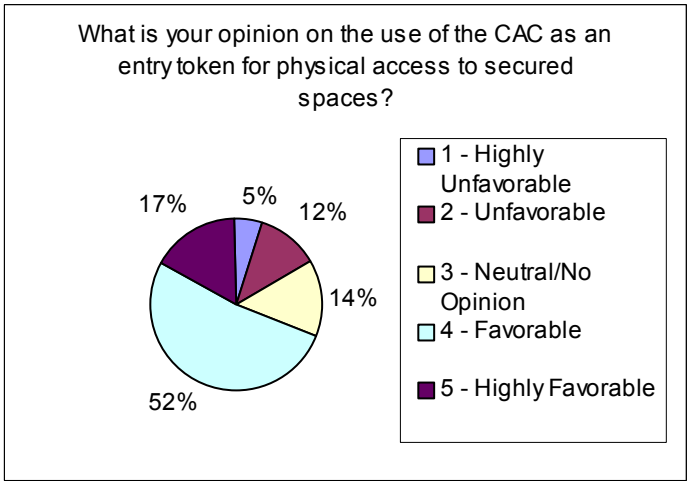
POST-PILOT SURVEY

Question 7



Average: 4.0

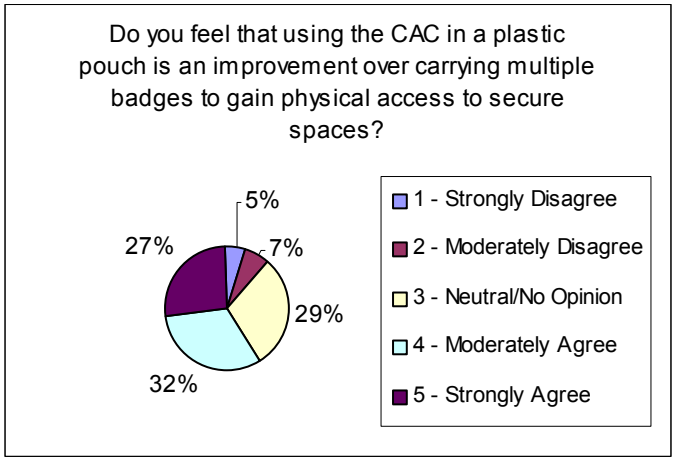
Question 8



Average: 3.6

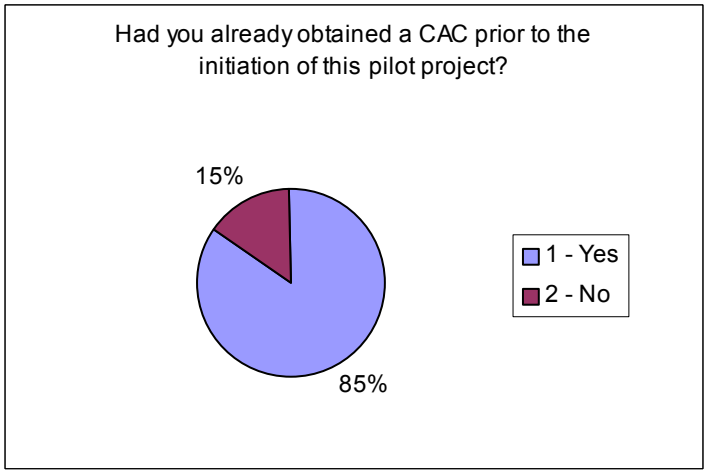
PRE-PILOT SURVEY

Question 9



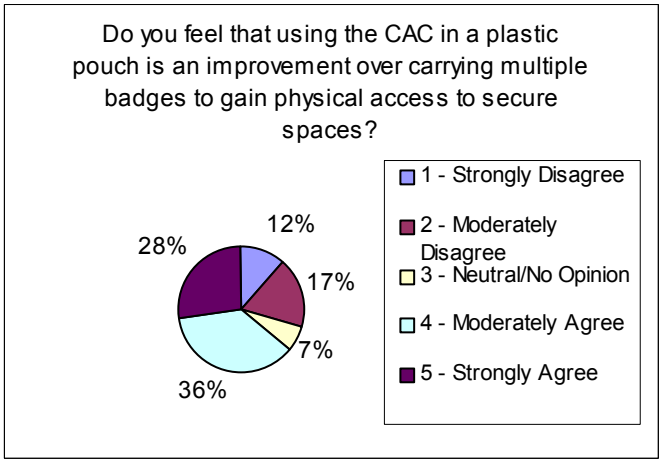
Average: 3.7

Question 10



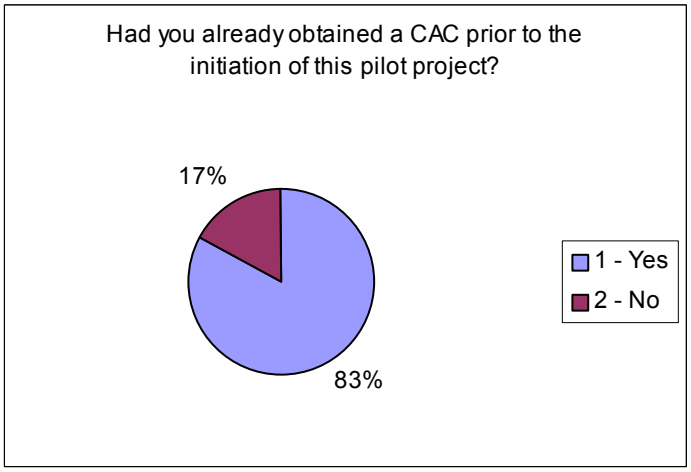
POST-PILOT SURVEY

Question 9



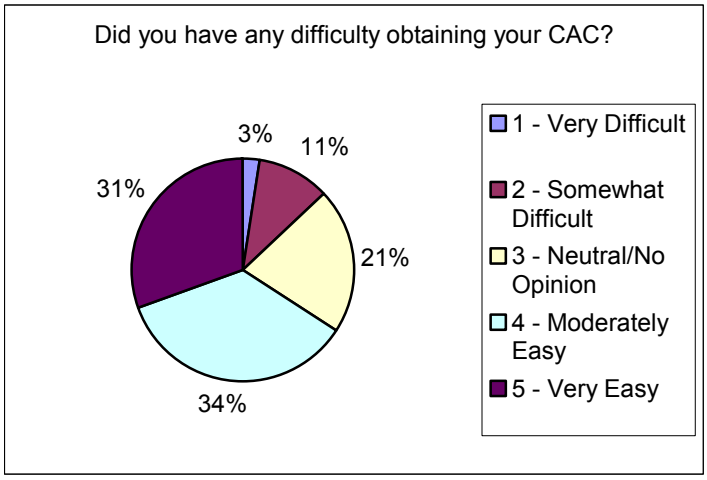
Average: 3.5

Question 10



PRE-PILOT SURVEY

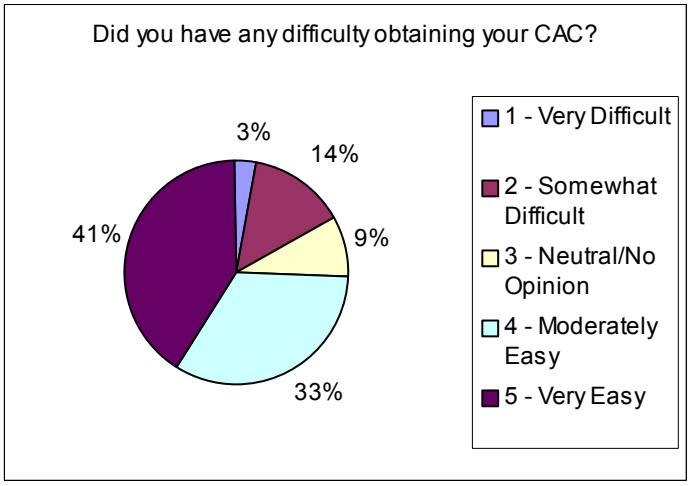
Question 11



Average: 3.8

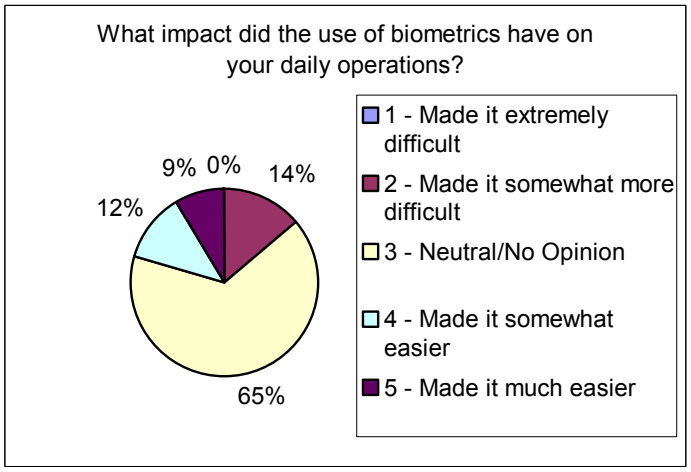
POST-PILOT SURVEY

Question 11



Average: 3.9

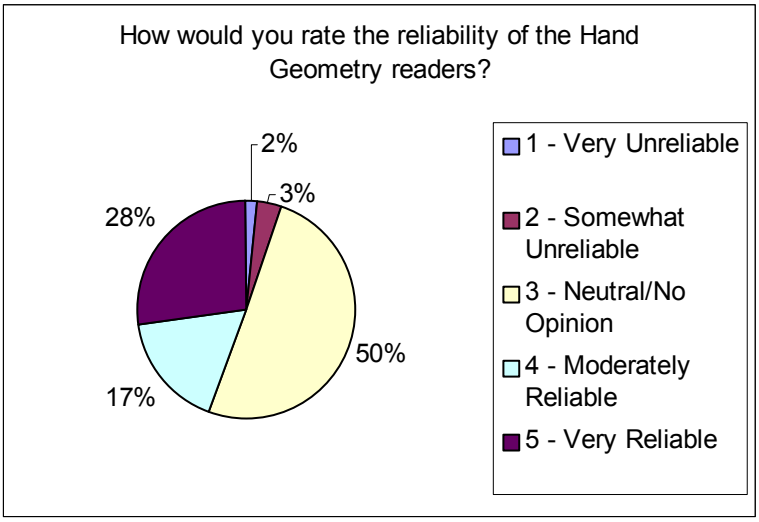
Question 12



Average: 3.2

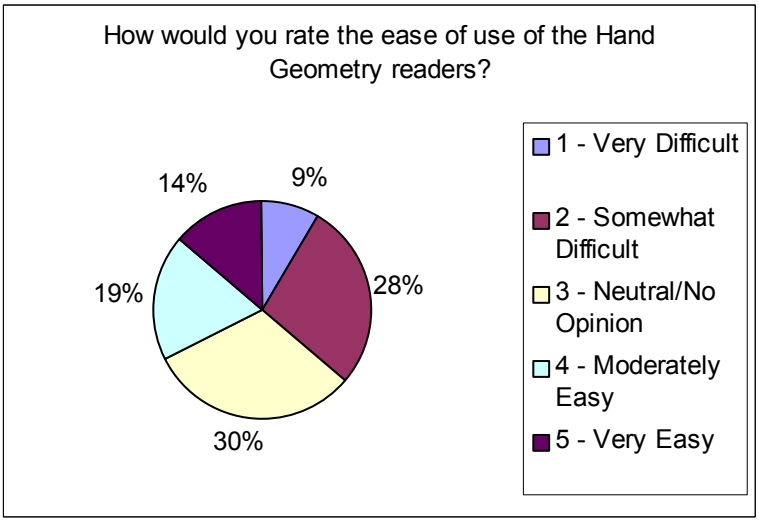
POST-PILOT SURVEY

Question 13



Average: 3.7

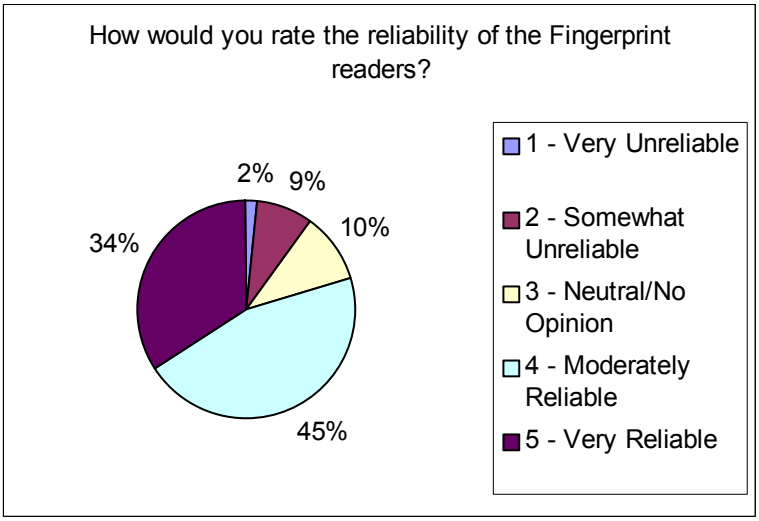
Question 14



Average: 3.0

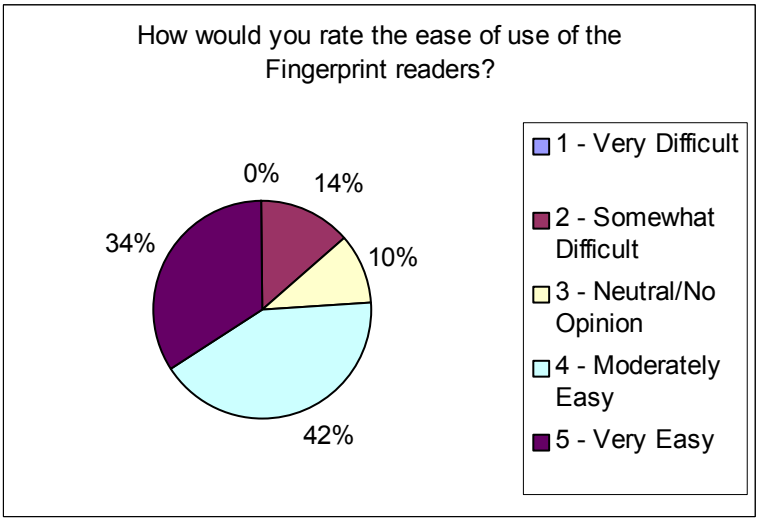
POST-PILOT SURVEY

Question 15



Average: 4.0

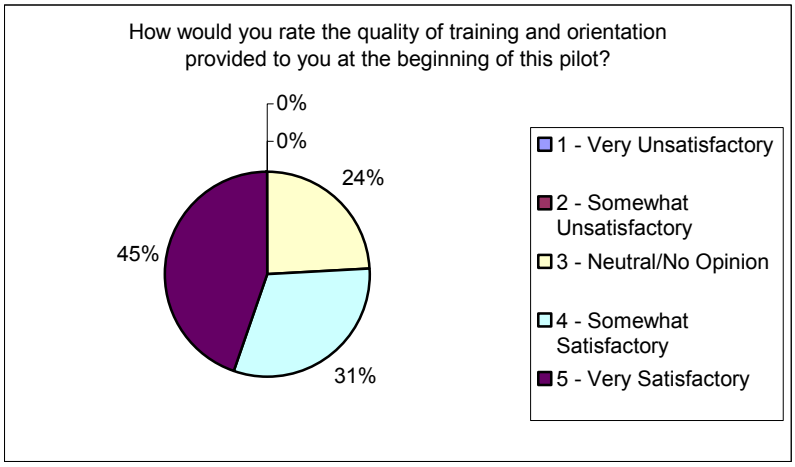
Question 16



Average: 4.0

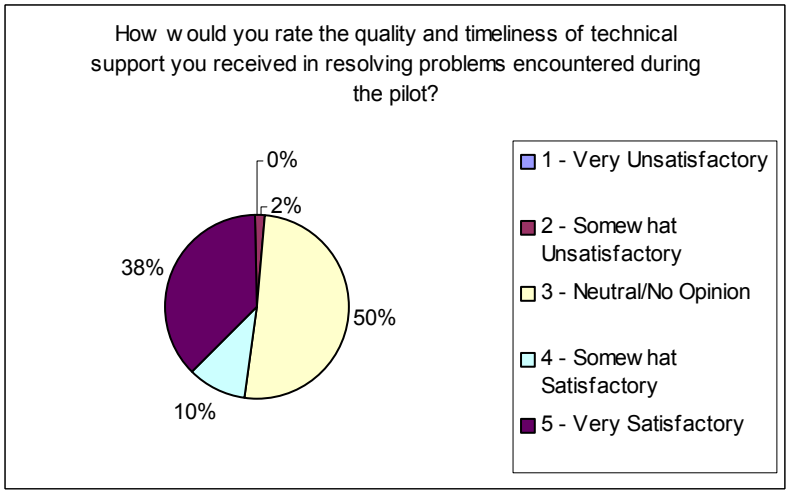
POST-PILOT SURVEY

Question 17



Average: 4.2

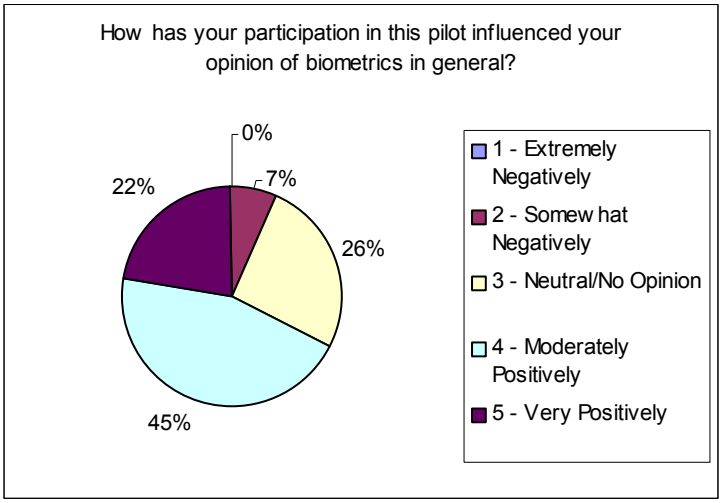
Question 18



Average: 3.8

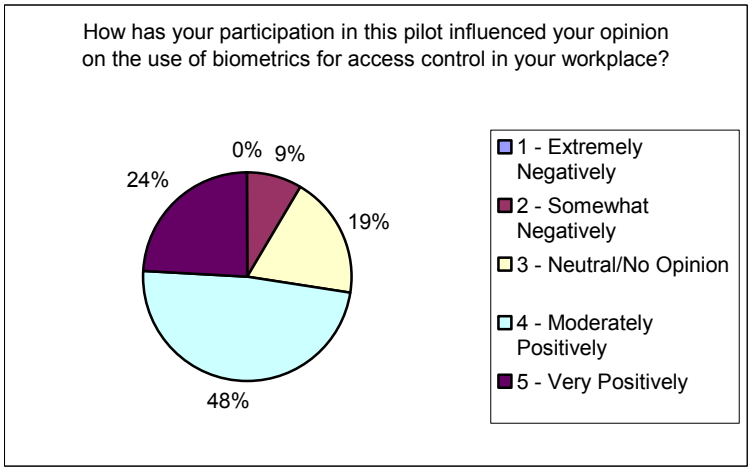
POST-PILOT SURVEY

Question 19



Average: 3.8

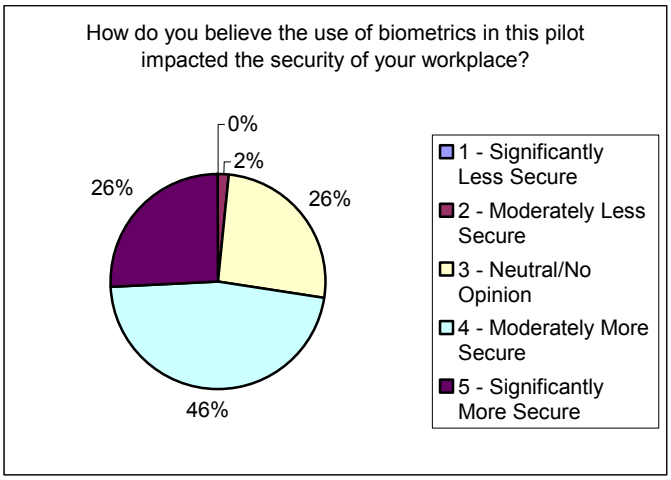
Question 20



Average: 3.9

POST-PILOT SURVEY

Question 21



Average: 4.0

Manager vs. Non-Manager responses

The following table provides a breakdown of average (arithmetic mean) responses to the pre-pilot and post-pilot surveys, broken down to compare and contrast the responses of managers and non-managers among the respondents.

PACOM Survey Analysis: Manager vs. Non-Manager

Question #		Pre-Pilot Manager	Non-Manager	Post-Pilot Manager	Non-Manager
1	What is your classification?	[1]	[1]	[1]	[1]
2	How would you describe your current level of knowledge about biometrics?	2.67	2.39	2.78	2.71
3	What is your opinion of biometrics (in general)?	3.43	3.43	3.89	3.77
4	To what degree do you consider using your biometric information to be an invasion of your personal privacy?	3.25	3.31	3.48	3.42
5	What is your perception of the security that the current access control hardware (card reader) provides to get access to your workplace?	3.34	3.27	3.67	4.03

6	What is your opinion on the use of biometrics for access control in your workplace?	3.57	3.71	4.22	3.97
7	Do you feel the increased security that biometrics provides is worth the inconvenience of presenting your card and presenting your finger or hand to the reader?	3.53	3.65	4.11	3.94
8	What is your opinion on the use of the CAC as an entry token for physical access to secured spaces?	3.6	3.64	3.7	3.58
9	Do you feel that using the CAC in a plastic pouch is an improvement over carrying multiple badges to gain physical access to secure spaces?	3.67	3.71	3.59	3.42
10	Had you already obtained a CAC prior to the initiation of this pilot project?	[2]	[2]	[2]	[2]
11	Did you have any difficulty obtaining your CAC?	3.82	3.79	4.07	3.84
12	What impact did the use of biometrics have on your daily operations?	[3]	[3]	3.22	3.1
13	How would you rate the reliability of the Hand Geometry readers?	[3]	[3]	3.52	3.77
14	How would you rate the ease of use of the Hand Geometry readers?	[3]	[3]	3.22	2.84
15	How would you rate the reliability of the Fingerprint readers?	[3]	[3]	4.11	3.94
16	How would you rate the ease of use of the Fingerprint readers?	[3]	[3]	4.04	3.9
17	How would you rate the quality of training and orientation provided to you at the beginning of this pilot?	[3]	[3]	4.26	4.16
18	How would you rate the quality and timeliness of technical support you received in resolving problems encountered during the pilot?	[3]	[3]	3.74	3.94

19	How has your participation in this pilot influenced your opinion of biometrics in general?	[3]	[3]	4	3.68
20	How has your participation in this pilot influenced your opinion on the use of biometrics for access control in your workplace?	[3]	[3]	4.04	3.74
21	How do you believe the use of biometrics in this pilot impacted the security of your workplace?	[3]	[3]	4.11	3.84
22	As an administrator of the system, how would you rate the ease of enrolling users in the system?	[3]	[3]	5	5
23	How has your participation in this pilot influenced your opinion of biometrics in general?	[3]	[3]	3	4
24	How has your participation in this pilot influenced your opinion on the use of biometrics for access control in your workplace?	[3]	[3]	5	5
25	How do you believe the use of biometrics in this pilot impacted the security of your workplace?	[3]	[3]	4	4

Notes: [1] Breakdown of military, civilian government, and contractors. No statistical significance to the breakdown of those groups.

[2] Breakdown of how many had CAC prior to pilot initiation. No statistical significance to that breakdown.

[3] Question only provided in post-pilot survey form.

Appendix C System Statistics

This section summarizes the performance of the system across the life of the pilot. Data was extracted from the Lenel ESS log files, and was imported into a MySQL database on a Linux system for data analysis. A number of custom Perl programs were developed to analyze the data in a variety of ways.

The first chart below (**Chart 1**) summarizes how many attempts were required by users to gain access upon presentation of their token and live scan biometric. In this chart, the data is shown across time, to observe if there was any significant change in the performance of the system over time. Zero retries means the user obtained a biometric match upon the first presentation of the token and biometric feature for comparison. The entry rate for users exceeded 90% on the first attempt over the entire life of the pilot. This exceeded the goal established at the beginning of the pilot.

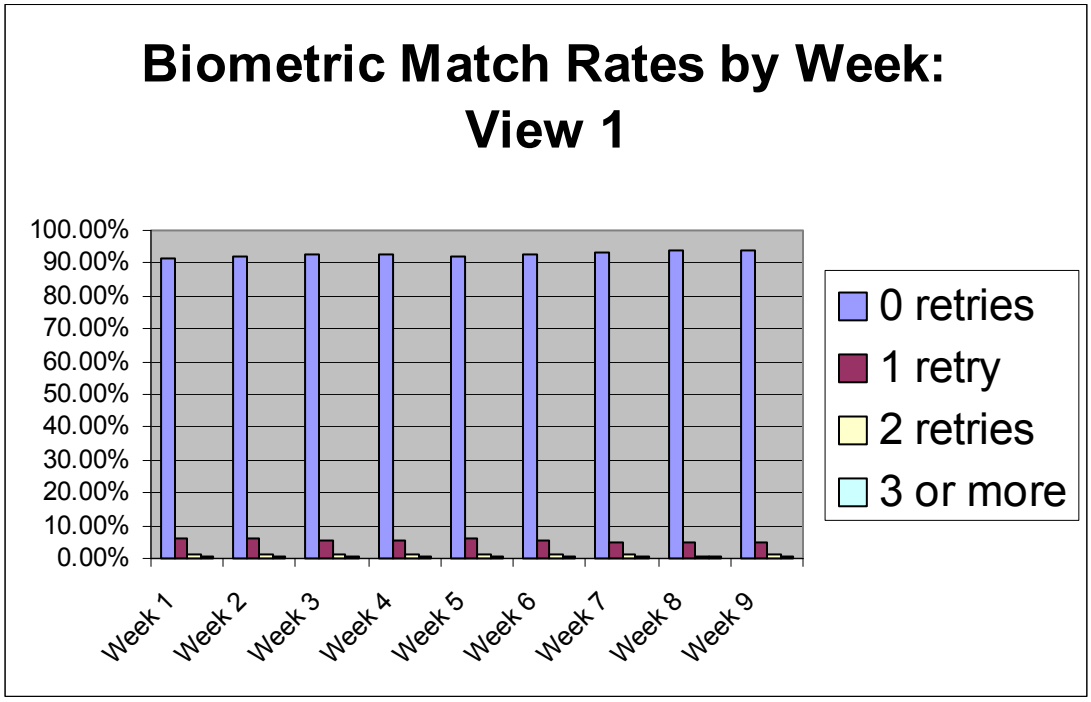


Chart 1

Based upon past pilot projects involving biometrics, a common pattern has been observed: users may be careless in the placement of their finger or hand, causing them to fail to obtain a biometric match on the first attempt. However, the users typically realize what they're doing wrong, correct the position of their finger or hand, and obtain a quality scan (and match) upon their second attempt. For this reason, one metric of system performance is the percentage of users obtaining a biometric match (and

therefore, access to the facility) with 2 or fewer attempts. The chart below (**Chart 2**) provides the summarization of the data collected when viewed by that criterion. This chart also presents the data across time, to observe if there was any significant change in the performance of the system over the life of the pilot.

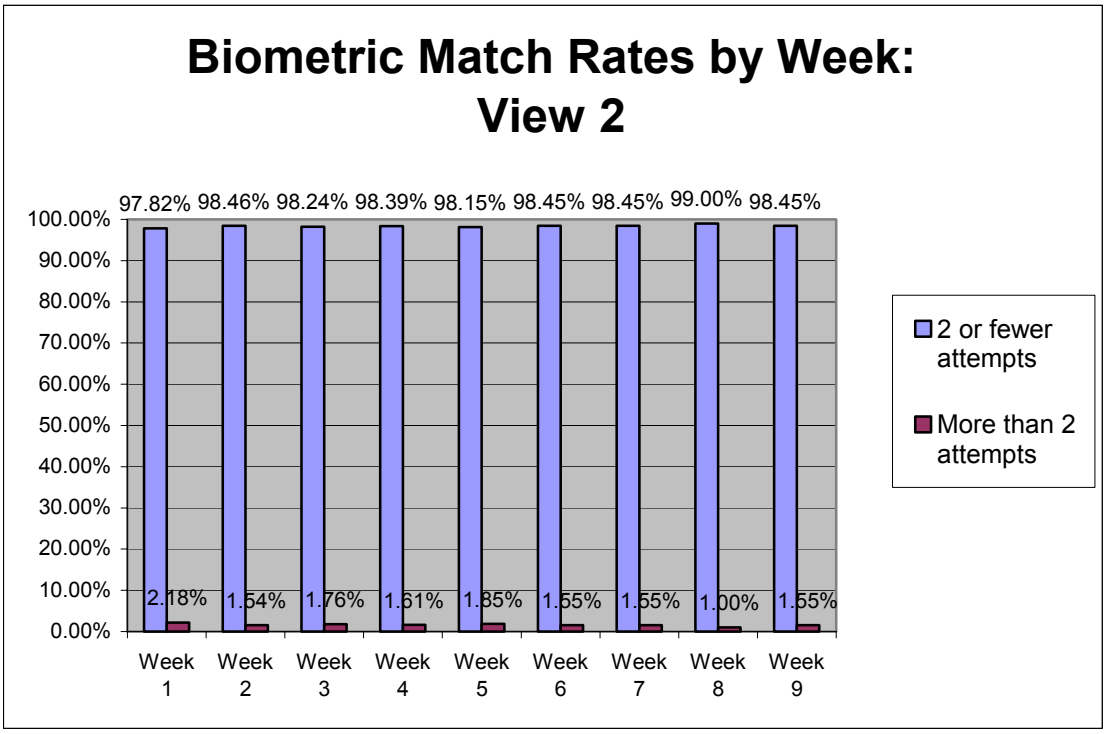


Chart 2

Another area of interest was the performance of the biometric readers located at each door. The user access rates were broken out by reader, and the results for each door were summarized. The rates observed ranged from a low of 85% (at door 103) to a high of 98.5% at the exterior side door. The following chart (**Chart 3**) summarizes the observed rates for each door/reader.

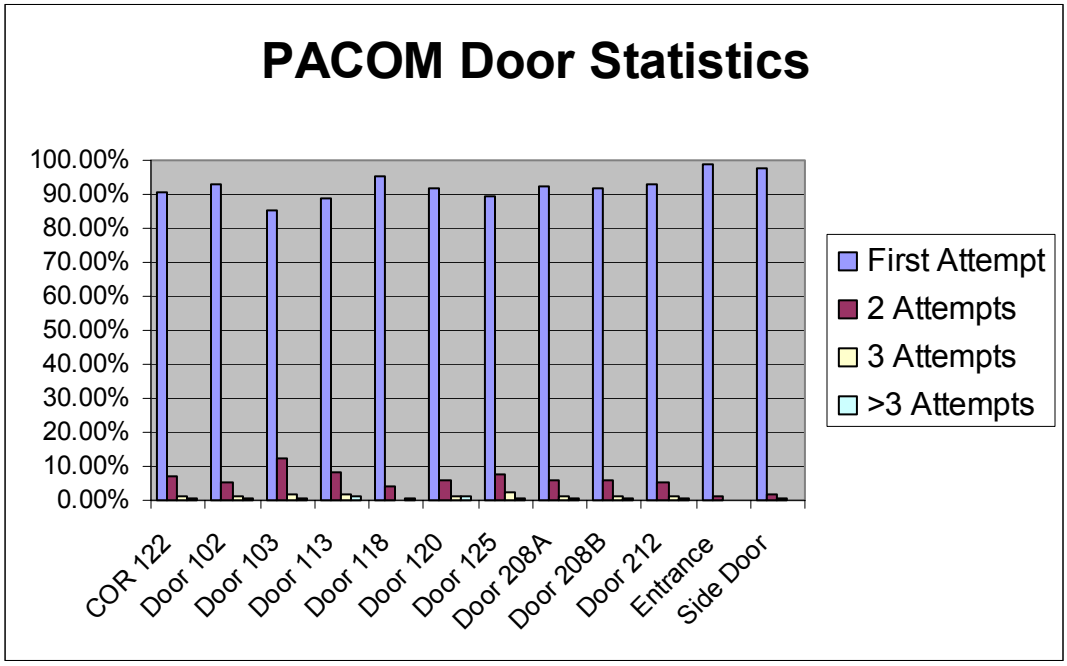


Chart 3

During the course of the pilot, the Lenel ESS logs were monitored in order to observe individuals who experienced excessively high rejection rates. Some of these were determined anecdotally to have been due to poor fingerprint template quality, and were subsequently improved through re-enrollment of the biometric template. In other cases, individuals had particularly poor fingerprint ridges, or poor circulation in the extremities. In the first situation, individual thresholds were reduced to accommodate that individual, and in the second situation, the individual learned to rub the finger vigorously to "warm it up" before placing it on the reader. The following chart (**Chart 4**) shows error rates of a few of the users experiencing the highest error rates. Note the general decrease in error rates for those individuals that followed the corrective measures described above.

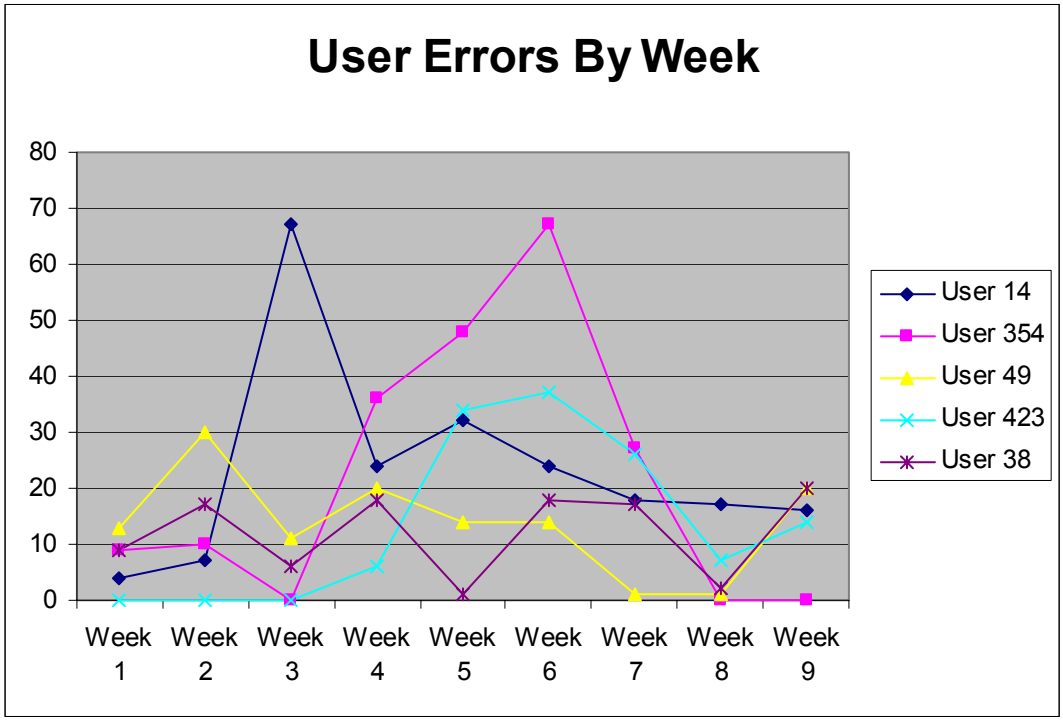

User Errors By Week
80
70
60
50
40
30
20
10
0
Week 1
Week 2
Week 3
Week 4
Week 5
Week 6
Week 7
Week 8
Week 9
User 14
User 354
User 49
User 423
User 38

Chart 4

Appendix D References

These references were relied upon when compiling this Opportunity Analysis:

- Common Access Card Biometric Enhancements for Physical Security Project Charter, Version 1.4 (06 JAN 2003)
- U.S. Pacific Command Biometric Enhancements for Physical Security Test Plan, SSC Charleston (28 JAN 2003)

Helpful references on Security Guidance; Technology Reports, Other Research efforts:

1. Infineon Technologies. Security and Chip IC's SLE66CL160S Short Product Information 05.00, July 1999.

2. Philips Semiconductors, MIFARE Identification products. http://www-us.semiconductors.philips.com/identification/products/mifare/ (2001).

3. Lenel On-Guard. http://www.lenel.com/onguard/access.htm

4. Bioscrypt V20 Biometric Smart Card Reader. http://www.bioscrypt.com/products/vsmart.shtml

5. Smart Card Alliance. *Contactless Technology for Secure Physical Access: Technology and Standards Choices* dated October 2002. www.smartcardalliance.org.

6. Smart Card Alliance, Smart *Cards and Biometrics White Paper*, May 2002.

7. NIST Inter-Agency Report 6887: Government Smart Card Interoperability Specification (v2.0). *Briefing for M1-Biometrics*, August 22, 2002.

8. NIST Inter-Agency Report 6887 Government Smart Card Interoperability Specification (v2.0*), Presentation for: INCITS, B10.1 1C Cards with contacts, and B10.5 Contactless IC Cards*, August 14, 2002.

Appendix E List of Acronyms

Acronym	Definition
ACO	Access Card Office
BMS	Balanced Magnetic Switch
CAC	Common Access Card
CIO	Chief Information Officer / Chief Information Office
CNO	Chief of Naval Operations
CONOPS	Concept of Operations
DoD	Department of Defense
DON	Department of Navy
eBUSOPSOFF	DON eBusiness Operations Office
ESS	Electronic Security System
FAR	False Acceptance Rate
FRR	False Rejection Rate
GB	Gigabyte
HID	Hughes Identification Devices originally, now HID Corporation
ID	Identification
ISO	International Standards Organization
Kb	Kilobyte
KHz	Kilo Hertz
MB	Megabyte
MHz	Mega Hertz
NSA	National Security Agency
OA	Opportunity Analysis
PAC	Physical Access Control
PC	Personal Computer
PIN	Personal Identification Number
RAM	Random Access Memory
REX/PIR	Request to Exist / Passive Infrared Detector
SA	System Administrator
SCSCG	Smart Card Senior Coordinating Group
SEIWG	Security Equipment Integration Working Group
SIPRNET	Secure Internet Protocol Network
SPAWAR	Space & Naval Warfare Systems Command
SSC	SPAWAR Systems Center